aws

Guida per l'utente

Amazon Elastic Compute Cloud

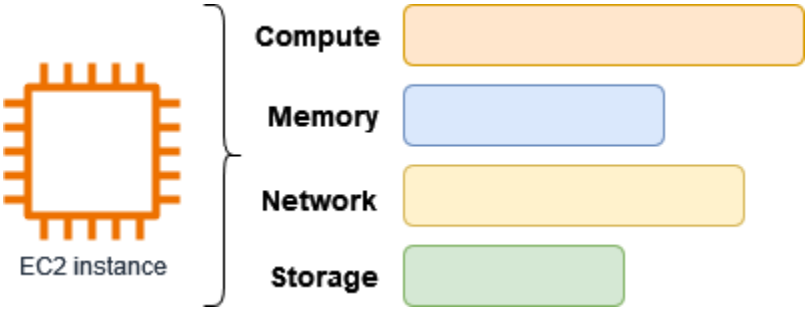
Amazon Elastic Compute Cloud: Guida per l'utente

Table of Contents

Che cosa è Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) fornisce capacità di calcolo scalabile on demand nel cloud Amazon Web Services (AWS). L'utilizzo di Amazon EC2 riduce i costi hardware in modo da poter sviluppare e implementare applicazioni più velocemente. Puoi utilizzare Amazon EC2 per avviare il numero di server virtuali necessari, configurare la sicurezza e i servizi di rete, nonché gestire l'archiviazione. Puoi aggiungere capacità (aumento) per gestire attività a uso intensivo di calcolo, come processi mensili o annuali o picchi nel traffico del sito Web. Quando l'utilizzo diminuisce, puoi ridurre nuovamente la capacità (riduzione).

Un'istanza EC2 è un server virtuale nel cloud. AWS Quando avvii un'istanza EC2, il tipo di istanza specificato determina l'hardware disponibile per l'istanza. Ogni tipo di istanza offre un diverso equilibrio di risorse di calcolo, memoria, rete e archiviazione. Per ulteriori informazioni, consulta la Amazon EC2 Instance Types Guide.



Caratteristiche di Amazon EC2

Amazon EC2 offre le seguenti funzionalità di alto livello:

Istanze

Server virtuali.

Amazon Machine Images (AMI)

Modelli preconfigurati per le istanze contenenti i pacchetti di bit necessari per il server (compresi il sistema operativo e il software aggiuntivo).

Tipi di istanza

Varie configurazioni di CPU, memoria, archiviazione, capacità di rete e hardware grafico per le istanze.

Volumi Amazon EBS

Volumi di archiviazione persistente per i dati tramite Amazon Elastic Block Store (Amazon EBS).

Volumi di archivio dell'istanza

Volumi di archiviazione per i dati temporanei che verranno eliminati quando l'istanza viene arrestata, ibernata o terminata.

Key pairs (Coppie di chiavi)

Informazioni di accesso sicure per le tue istanze. AWS archivia la chiave pubblica e l'utente archivia la chiave privata in un luogo sicuro.

Gruppi di sicurezza

Un firewall virtuale che consente di specificare i protocolli, le porte e gli intervalli IP di origine che possono raggiungere le istanze e gli intervalli IP di destinazione a cui le istanze possono connettersi.

Amazon EC2 supporta l'elaborazione, l'archiviazione e la trasmissione di dati di carte di credito da parte di un esercente o di un provider di servizi, oltre a essere conforme allo standard Payment Card Industry Data Security Standard (PCI DSS). Per ulteriori informazioni su PCI DSS, incluso come richiedere una copia del PCI AWS Compliance Package, vedere PCI DSS Level 1.

Servizi correlati

Servizi da usare con Amazon EC2

Puoi usarne altre Servizi AWS con le istanze che distribuisci utilizzando Amazon EC2.

Dimensionamento automatico Amazon EC2

Assicura di disporre del numero corretto di istanze Amazon EC2 disponibili per gestire il carico dell'applicazione.

AWS Backup

Automatizza il backup delle istanze Amazon EC2 e dei volumi Amazon EBS ad esse collegati.

Amazon CloudWatch

Monitora le istanze e i volumi Amazon EBS.

Elastic Load Balancing

Distribuisci automaticamente il traffico delle applicazioni in ingresso tra più istanze.

Amazon GuardDuty

Rileva l'uso potenzialmente non autorizzato o dannoso delle istanze EC2.

EC2 Image Builder

Automatizza la creazione, la gestione e l'implementazione di immagini up-to-date server, sicure e personalizzate.

AWS Launch Wizard

Dimensiona, configura e distribuisci AWS risorse per applicazioni di terze parti senza dover identificare e fornire manualmente le singole AWS risorse.

AWS Systems Manager

Esegui operazioni su larga scala sulle istanze EC2 con questa soluzione di gestione sicura end-to-end.

Servizi di elaborazione aggiuntivi

Puoi avviare istanze utilizzando un altro servizio di AWS elaborazione anziché Amazon EC2.

Amazon Lightsail

Crea siti Web o applicazioni Web utilizzando Amazon Lightsail, una piattaforma cloud che fornisce le risorse necessarie per implementare rapidamente il tuo progetto a un prezzo mensile basso e prevedibile. Per confrontare Amazon EC2 e Lightsail, consulta Amazon Lightsail o Amazon EC2.

Amazon Elastic Container Service (Amazon ECS)

Implementa, gestisci e dimensiona le applicazioni containerizzate su un cluster di istanze EC2. Per ulteriori informazioni, consulta Scelta di un servizio container. AWS

Amazon Elastic Kubernetes Service (Amazon EKS)

Esegui le tue applicazioni Kubernetes su AWS. Per ulteriori informazioni, vedere Scelta di un servizio AWS container.

Accesso a Amazon EC2

È possibile creare e gestire le istanze Amazon EC2 utilizzando le seguenti interfacce:

Console Amazon EC2

Una semplice interfaccia Web per creare e gestire istanze e risorse Amazon EC2. Se hai registrato un AWS account, puoi accedere alla console Amazon EC2 accedendo AWS Management Console e selezionando EC2 dalla home page della console.

AWS Command Line Interface

Consente di interagire con i AWS servizi utilizzando i comandi nella shell della riga di comando. È supportata su Windows, Mac e Linux. Per ulteriori informazioni sulla AWS CLI , consulta la Guida per l'utente di AWS Command Line Interface. Puoi trovare i comandi di Amazon EC2 nella Documentazione di riferimento ai comandi di AWS CLI.

AWS CloudFormation

Amazon EC2 supporta la creazione di risorse utilizzando AWS CloudFormation. Crei un modello, in formato JSON o YAML, che descrive AWS le tue risorse e fornisce e configura AWS CloudFormation tali risorse per te. Puoi riutilizzare i CloudFormation modelli per fornire le stesse risorse più volte, nella stessa regione e account o in più aree e account. Per ulteriori informazioni sui tipi di risorse supportati e sulle proprietà di Amazon EC2, consulta la sezione Riferimento al tipo di risorsa EC2 nella Guida per l'utente di AWS CloudFormation .

AWS SDK

Se preferisci creare applicazioni utilizzando API specifiche per una lingua anziché inviare una richiesta tramite HTTP o HTTPS, AWS fornisce librerie, codice di esempio, tutorial e altre risorse per gli sviluppatori di software. Le librerie offrono funzioni di base per automatizzare attività quali la firma crittografica delle richieste, la ripetizione delle richieste e la gestione delle risposte agli errori, semplificando le attività iniziali. Per ulteriori informazioni, consulta Strumenti per creare su AWS.

AWS Tools for PowerShell

Un insieme di PowerShell moduli che si basano sulle funzionalità esposte da. AWS SDK for .NET Gli strumenti PowerShell consentono di eseguire operazioni di script sulle AWS risorse dalla PowerShell riga di comando. Per iniziare, consulta la AWS Tools for Windows PowerShell Guida per l'utente di . Puoi trovare i cmdlet per Amazon EC2 nella Documentazione di riferimento di AWS Tools for PowerShell Cmdlet.

API della query

Amazon EC2 fornisce un'API di query. Queste richieste sono richieste HTTP o HTTPS che utilizzano i verbi HTTP GET o POST e un parametro di query denominato `Action`. Per ulteriori informazioni sulle operazioni dell'API per Amazon EC2, consulta la sezione relativa alle operazioni della Amazon EC2 API Reference.

Prezzi delle Amazon EC2

Amazon EC2 offre le seguenti opzioni di prezzo:

Piano gratuito

È possibile iniziare a utilizzare Amazon EC2 gratuitamente. Per esplorare le opzioni del piano gratuito, consulta Piano gratuito di AWS.

Istanze on demand

Pagamenti per le istanze utilizzate al secondo, con un minimo di 60 secondi, senza impegni a lungo termine o pagamenti anticipati.

Savings Plans

Puoi ridurre i costi di Amazon EC2 e svolgere una serie di attività, in USD per ora, per un periodo di uno o tre anni.

Reserved Instances

Puoi ridurre i costi Amazon EC2 utilizzando un'istanza specifica per una configurazione di istanza specifica, incluso il tipo di istanza e la regione, per un periodo di uno o tre anni.

Spot Instances

Consente di richiedere istanze EC2 inutilizzate, in grado di ridurre i costi di Amazon EC2 in modo significativo.

Host dedicati

Riduci i costi utilizzando un server EC2 fisico completamente dedicato al tuo uso, on demand o nell'ambito di un Savings Plan. Puoi utilizzare le licenze software esistenti legate al server e ottenere assistenza per soddisfare i requisiti di conformità.

Prenotazione della capacità on demand

Prenota capacità di calcolo per le istanze EC2 per qualsiasi durata in una determinata zona di disponibilità.

Fatturazione al secondo

Rimuove dalla fattura il costo dei minuti e dei secondi inutilizzati.

Per un elenco completo delle tariffe e dei prezzi specifici per Amazon EC2 e per ulteriori informazioni sui modelli di acquisto, consulta la sezione Prezzi di Amazon EC2.

Stime, fatturazione e ottimizzazione dei costi

Per creare stime per i tuoi casi AWS d'uso, usa il AWS Pricing Calculator.

Per stimare il costo della trasformazione dei carichi di lavoro Microsoft in un'architettura moderna che utilizza servizi open source e nativi del cloud distribuiti su AWS, usa il Modernization AWS Calculator for Microsoft Workloads.

Per vedere la tua fattura, vai sul Pannello di controllo di gestione dei costi e della fatturazione nella console AWS Billing and Cost Management. La fattura contiene collegamenti per passare ai report di utilizzo, che consentono di visualizzare i dettagli della fattura. Per ulteriori informazioni sulla fatturazione AWS dell'account, consulta la Guida per l'utente di AWS Billing and Cost Management.

In caso di domande relative alla AWS fatturazione, agli account e agli eventi, contatta l' AWS assistenza.

Per calcolare il costo di un ambiente con provisioning di esempio, consultare Centro benefici economici Cloud. Quando si calcola il costo di un ambiente con provisioning, ricordare di includere costi accidentali come l'archiviazione snapshot per i volumi EBS.

È possibile ottimizzare i costi, la sicurezza e le prestazioni del proprio AWS ambiente utilizzando AWS Trusted Advisor.

Puoi utilizzarlo AWS Cost Explorer per analizzare il costo e l'utilizzo delle tue istanze EC2. Puoi visualizzare i dati relativi agli ultimi 13 mesi e prevedere quanto probabilmente spenderai per i prossimi 12 mesi. Per ulteriori informazioni, consulta la sezione Analisi dei costi AWS Cost Explorer nella Guida per l'AWS Cost Management utente.

Risorse

- Caratteristiche di Amazon EC2
- AWS Re: post
- AWS Skill Builder
- AWS Support
- Tutorial pratici
- Web hosting
- Windows attivo AWS

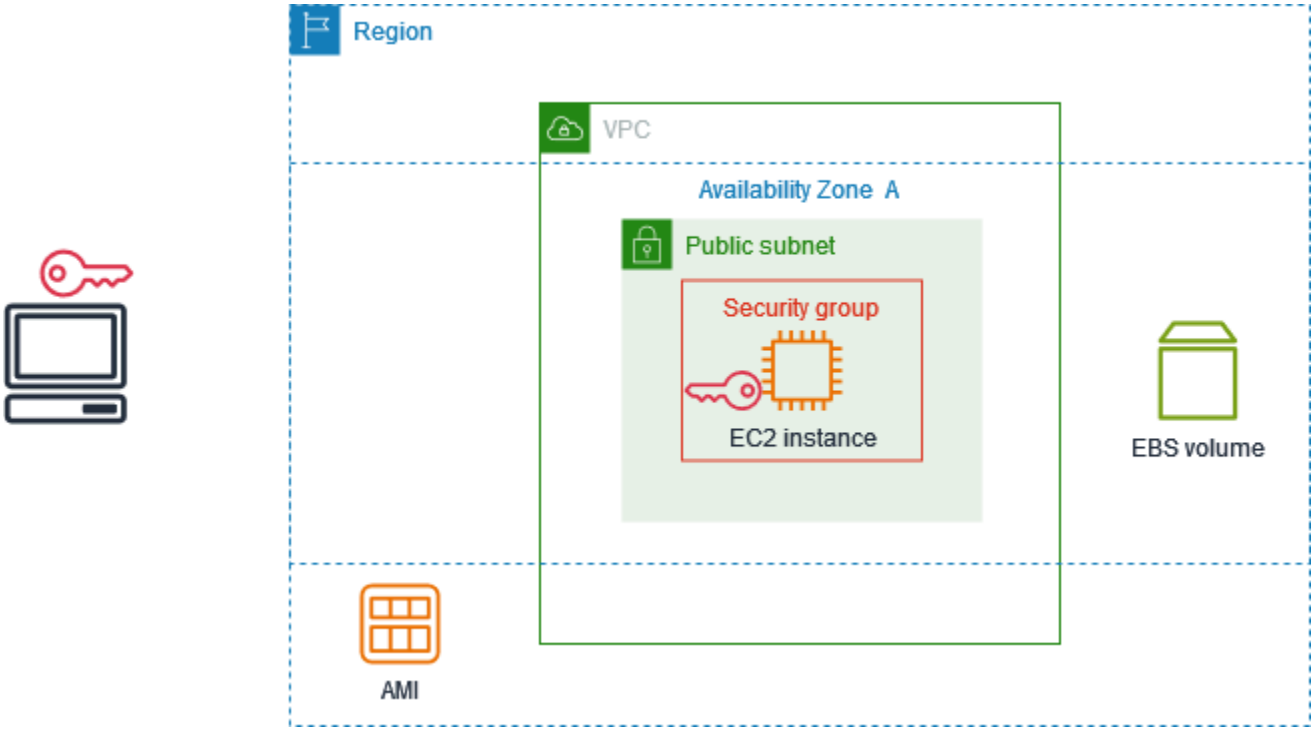
Nozioni di base su Amazon EC2

Utilizza questo tutorial per iniziare a usare Amazon Elastic Compute Cloud (Amazon EC2). Imparerai come avviare e connetterti a un'istanza EC2. Un'istanza è un server virtuale nel AWS cloud. Con Amazon EC2, puoi installare e configurare il sistema operativo e le applicazioni eseguiti sull'istanza.

Panoramica

Il diagramma seguente mostra i componenti chiave che utilizzerai in questo tutorial:

- Un'immagine: un modello che contiene il software da eseguire sull'istanza, ad esempio il sistema operativo.
- Una key pair: un set di credenziali di sicurezza che usi per dimostrare la tua identità quando ti connetti alla tua istanza. La chiave pubblica si trova sulla tua istanza e la chiave privata è sul tuo computer.
- Una rete: un cloud privato virtuale (VPC) è una rete virtuale dedicata a te. Account AWS Per aiutarti a iniziare rapidamente, il tuo account include un VPC predefinito in ogni VPC predefinito e ogni Regione AWS VPC predefinito ha una sottorete predefinita in ogni zona di disponibilità.
- Un gruppo di sicurezza: funge da firewall virtuale per controllare il traffico in entrata e in uscita.
- Un volume EBS: è necessario un volume root per l'immagine. Facoltativamente, puoi aggiungere volumi di dati.



Costo di questo tutorial

Quando ti registri AWS, puoi iniziare a usare Amazon EC2 utilizzando il. Piano gratuito di AWS Se hai creato il tuo account Account AWS meno di 12 mesi fa e non hai ancora superato i vantaggi del piano gratuito per Amazon EC2, completare questo tutorial non ti costerà nulla, perché ti aiutiamo a selezionare le opzioni che rientrano nei vantaggi del piano gratuito. In caso contrario, ti verranno addebitati i costi di utilizzo standard di Amazon EC2 dal momento in cui avvii l'istanza fino alla sua interruzione (ovvero l'attività finale di questo tutorial), anche se l'istanza rimane inattiva.

Per istruzioni su come determinare se sei idoneo al piano gratuito, consulta. the section called “Monitoraggio dell'utilizzo del piano gratuito”

Attività

- Fase 1: avvio di un'istanza
- Fase 2. connessione all'istanza
- Fase 3. pulizia di un'istanza
- Passaggi successivi

Fase 1: avvio di un'istanza

Puoi avviare un'istanza EC2 utilizzando la AWS Management Console procedura descritta nella procedura seguente. La finalità di questo tutorial è aiutarti ad avviare in modo semplice e rapido la prima istanza. Pertanto, non verranno descritte tutte le possibili opzioni.

Per avviare un'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore dello schermo, viene visualizzata la versione corrente Regione AWS , ad esempio l'Ohio. Puoi utilizzare la regione selezionata o, facoltativamente, selezionare una regione più vicina a te.
3. Dalla dashboard della console EC2, nel riquadro Launch instance, scegli Launch instance.
4. In Name and tags (Nome e tag), per Name (Nome), inserisci un nome descrittivo per l'istanza.
5. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), esegui la seguente operazione:
   a. Scegli Quick Start, quindi scegli il sistema operativo (OS) per la tua istanza. Per la tua prima istanza Linux, ti consigliamo di scegliere Amazon Linux.
   b. Da Amazon Machine Image (AMI), seleziona un AMI contrassegnato come idoneo al piano gratuito.
6. In Tipo di istanza, per Tipo di istanza **`t2.micro`**, scegli quale è idonea per il piano gratuito. Nelle regioni in cui non `t2.micro` è disponibile, `t3.micro` è idoneo al piano gratuito.
7. In Key pair (login), per Key pair name, scegli una coppia di chiavi esistente o scegli Crea nuova coppia di chiavi per creare la tua prima coppia di chiavi.

   > ⚠ Warning
   >
   > Se scegli Proceed without a key pair (scelta non consigliata), non sarai in grado di connetterti alla tua istanza utilizzando i metodi descritti in questo tutorial.

8. In Impostazioni di rete, nota che abbiamo selezionato il tuo VPC predefinito, selezionato l'opzione per utilizzare la sottorete predefinita in una zona di disponibilità che abbiamo scelto per te e configurato un gruppo di sicurezza con una regola che consente le connessioni alla tua istanza da qualsiasi luogo. Come prima istanza, ti consigliamo di utilizzare le impostazioni predefinite. Altrimenti, puoi aggiornare le impostazioni di rete come segue:

- (Facoltativo) Per utilizzare una sottorete predefinita specifica, scegliete Modifica, quindi scegliete una sottorete.
- (Facoltativo) Per utilizzare un VPC diverso, scegli Modifica, quindi scegli un VPC esistente. Se il VPC non è configurato per l'accesso pubblico a Internet, non potrai connetterti alla tua istanza.
- (Facoltativo) Per limitare il traffico di connessione in entrata a una rete specifica, scegli Personalizzato anziché Anywhere e inserisci il blocco CIDR per la tua rete.
- (Facoltativo) Per utilizzare un gruppo di sicurezza diverso, scegli Seleziona gruppo di sicurezza esistente e scegli un gruppo di sicurezza esistente. Se il gruppo di sicurezza non dispone di una regola che consenta il traffico di connessione dalla rete, non sarai in grado di connetterti alla tua istanza. Per un'istanza Linux, devi consentire il traffico SSH. Per un'istanza Windows, è necessario consentire il traffico RDP.

9. In Configura archiviazione, nota che abbiamo configurato un volume root ma nessun volume di dati. Questo è sufficiente per scopi di test.
10. Analizza un riepilogo della configurazione dell'istanza nel pannello Summary (Riepilogo) e, quando è tutto pronto, scegli Launch instance (Avvia istanza).
11. Se il lancio ha esito positivo, scegli l'ID dell'istanza dalla notifica di successo per aprire la pagina Istanze e monitorare lo stato dell'avvio.
12. Seleziona la casella per l'istanza. Lo stato iniziale dell'istanza è`pending`. Dopo l'avvio di dell'istanza, il suo stato diventa `running`. Scegli la scheda Stato e allarmi. Dopo aver superato i controlli di stato, l'istanza è pronta a ricevere le richieste di connessione.

Fase 2. connessione all'istanza

La procedura da utilizzare dipende dal sistema operativo dell'istanza. Se non riesci a collegarti all'istanza, consulta Risolvi i problemi di connessione alla tua istanza Linux per ricevere assistenza.

Istanze Linux

Puoi connetterti alla tua istanza Linux usando qualsiasi client SSH. Se utilizzi Windows sul tuo computer, apri un terminale ed esegui il `ssh` comando per verificare che sia installato un client SSH. Se il comando non viene trovato, installa OpenSSH per Windows.

Per connettersi all'istanza tramite SSH

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza quindi scegli Connect (Connetti).
4. Nella pagina Connect to instance, scegli la scheda client SSH.
5. (Facoltativo) Se hai creato una coppia di chiavi all'avvio dell'istanza e hai scaricato la chiave privata (file.pem) su un computer che esegue Linux o macOS, esegui il chmod comando example per impostare le autorizzazioni per la tua chiave privata.
6. Copia il comando SSH di esempio. Di seguito è riportato un esempio, dove *key-pair-name*.pem è il nome del file di chiave privata, *ec2-user* è il nome utente associato all'immagine e la stringa dopo il simbolo @ è il nome DNS pubblico dell'istanza.

```
ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
```

7. In una finestra di terminale sul tuo computer, esegui il ssh comando salvato nel passaggio precedente. Se il file della chiave privata non si trova nella directory corrente, è necessario specificare il percorso completo del file della chiave in questo comando.

   Di seguito è riportata una risposta di esempio:

```
The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
 (198-51-100-1)' can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

8. (Facoltativo) Verificate che l'impronta digitale nell'avviso di sicurezza corrisponda all'impronta digitale dell'istanza contenuta nell'output della console quando avviate un'istanza per la prima volta. Per ottenere l'output della console, scegli Azioni, Monitoraggio e risoluzione dei problemi, Ottieni registro di sistema. Se le impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco. man-in-the-middle Se invece corrispondono, passare alla fase successiva.
9. Specificare (sì **yes**.

   Di seguito è riportata una risposta di esempio:

```
Warning: Permanently added 'ec2-198-51-100-1.us-
east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

Istanze Windows

Per connetterti a un'istanza di Windows, devi recuperare la password iniziale dell'amministratore e utilizzare questa password quando ti connetti all'istanza tramite Remote Desktop. Dopo l'avvio dell'istanza, dovrai attendere alcuni minuti prima che la password sia disponibile.

Il nome utente predefinito per l'account Administrator dipende dalla lingua del sistema operativo (OS) contenuto nell'AMI. Per verificare il nome utente corretto, identifica la lingua del sistema operativo dell'AMI, quindi scegli il nome utente corrispondente. Ad esempio, per un sistema operativo inglese, il nome utente è`Administrator`, per un sistema operativo francese è `Administrateur` e per un sistema operativo portoghese è`Administrador`. Se una versione linguistica del sistema operativo non ha un nome utente nella stessa lingua, scegli il nome utente`Administrator (Other)`. Per ulteriori informazioni, vedere Nomi localizzati per l'account amministratore in Windows in Microsoft TechNet Wiki.

Se l'istanza è stata aggiunta a un dominio, è possibile connettersi all'istanza utilizzando le credenziali di dominio definite in AWS Directory Service. Nella schermata di accesso a Desktop remoto, anziché utilizzare il nome del computer locale e la password generata, utilizzare il nome utente completo per l'amministratore (ad esempio, **`corp.example.com\Admin`**) e la password per questo account.

Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta the section called “Il desktop remoto non può connettersi al computer remoto”.

Per connetterti alla tua istanza Windows utilizzando un client RDP

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza quindi scegli Connect (Connetti).
4. Nella pagina Connect to instance, scegli la scheda Client RDP.
5. Per Nome utente, scegli il nome utente predefinito per l'account amministratore. Il nome utente scelto deve corrispondere alla lingua del sistema operativo (OS) contenuto nell'AMI che hai usato per avviare l'istanza. Se non esiste un nome utente nella stessa lingua del sistema operativo, scegli Amministratore (Altro).
6. Scegli Ottieni password.
7. Nella pagina Ottieni la password di Windows, procedi come segue:

a. Scegli Carica file di chiave privata e vai al file di chiave privata (`.pem`) che hai specificato all'avvio dell'istanza. Selezionare il file e scegliere Open (Apri) per copiare l'intero contenuto del file in questa finestra.

b. Scegli Decrittografa la password. La pagina Ottieni la password di Windows si chiude e la password di amministratore predefinita per l'istanza viene visualizzata in Password, sostituendo il collegamento Ottieni password mostrato in precedenza.

c. Copia la password e salvala in un posto sicuro. Questa password ti servirà per connetterti all'istanza.

8. Seleziona Download remote desktop file (Scarica file per desktop remoto). Al termine del download del file, scegli Cancel (Annulla) per tornare alla pagina Instances (Istanze). Vai alla directory dei download e apri il file RDP.
9. Potrebbe essere visualizzato un avviso che informa che l'identità di chi ha pubblicato la connessione remota non è nota. Scegli Connect (Connetti) per collegarti all'istanza.
10. Per impostazione predefinita è selezionato l'account amministratore. Incolla la password che hai copiato in precedenza, quindi scegli OK.
11. Data la natura dei certificati autofirmati, è possibile che venga visualizzato un avviso relativo all'impossibilità di autenticare il certificato di sicurezza. Esegui una di queste operazioni:
    - Se ritieni attendibile il certificato, scegli Sì per connetterti alla tua istanza.
    - [Windows] Prima di procedere, confronta l'impronta digitale del certificato con il valore nel registro di sistema per confermare l'identità del computer remoto. Scegli Visualizza certificato, quindi scegli Thumbprint dalla scheda Dettagli. Confronta questo valore con quello di **`RDPCERTIFICATE-THUMBPRINT`** Azioni, Monitoraggio e risoluzione dei problemi, Get system log.
    - [Mac OS X] Prima di procedere, confronta l'impronta digitale del certificato con il valore nel registro di sistema per confermare l'identità del computer remoto. Scegliete Mostra certificato, espandete Dettagli e scegliete SHA1 Fingerprints. Confronta questo valore con il valore di **`RDPCERTIFICATE-THUMBPRINT`** in Azioni, Monitor e risoluzione dei problemi, Get system log.

Fase 3. pulizia di un'istanza

Dopo aver creato l'istanza per questo tutorial, è consigliabile eseguire la pulizia mediante l'interruzione dell'istanza. Per eseguire altre operazioni con questa istanza prima di eseguire la pulizia, consulta Passaggi successivi.

> **Important**
>
> L'interruzione di un'istanza ne comporta l'eliminazione. Non è possibile riconnettersi a un'istanza dopo averla interrotta.

Smetterai di incorrere in addebiti per l'istanza o l'utilizzo che rientrano nei limiti del piano gratuito non appena lo stato dell'istanza passerà a o. `shutting down` `terminated` Per conservare l'istanza per un periodo successivo, ma senza incorrere in addebiti o utilizzi che influiscano sui limiti del piano gratuito, puoi interrompere l'istanza ora e riavviarla in un secondo momento. Per ulteriori informazioni, consulta Arresta e avvia le istanze Amazon EC2.

Per terminare l'istanza

1. Nel riquadro di navigazione, seleziona Instances (Istanze). Nell'elenco delle istanze, selezionare l'istanza.
2. Scegli Instance state (Stato istanza), Terminate instance (Termina istanza).
3. Quando viene richiesta la conferma, seleziona Terminate (Interrompi).

   Amazon EC2 arresta e termina l'istanza. Dopo averla terminata, l'istanza rimane visibile sulla console per un breve periodo di tempo, quindi la voce verrà eliminata automaticamente. L'utente non può rimuovere l'istanza terminata dal display della console.

Passaggi successivi

Dopo aver avviato l'istanza, potresti voler esplorare i seguenti passaggi successivi:

- Scopri come monitorare l'utilizzo del piano gratuito di Amazon EC2 utilizzando la console. Per ulteriori informazioni, consulta the section called “Monitoraggio dell'utilizzo del piano gratuito”.
- Configura un CloudWatch allarme per avvisarti se il tuo utilizzo supera il piano gratuito. Per ulteriori informazioni, consulta Monitoraggio dell' Piano gratuito di AWS utilizzo nella Guida per l'AWS Billing utente.
- Installa un volume EBS. Per ulteriori informazioni, consulta Creare un volume Amazon EBS nella Guida per l'utente di Amazon EBS.
- Scopri come gestire in remoto l'istanza EC2 utilizzando il comando Run. Per ulteriori informazioni, consulta Run Command AWS Systems Manager nella Guida per l'utente AWS Systems Manager .

- Scopri le opzioni di acquisto delle istanze. Per ulteriori informazioni, consulta Opzioni di acquisto delle istanze.
- Ottieni i dati sui tipi di istanze. Per ulteriori informazioni, consulta Ottenimento delle raccomandazioni per i tipi di istanza per un nuovo carico di lavoro.

Best practice per Amazon EC2

Per ottenere il massimo vantaggio da Amazon EC2, ti consigliamo di eseguire le best practice seguenti.

Sicurezza

- Gestisci l'accesso a AWS risorse e API utilizzando la federazione delle identità con un provider di identità e ruoli IAM quando possibile. Per ulteriori informazioni, consulta Creazione di policy IAM nella Guida per l'utente di IAM.
- Implementa regole meno permissive per il gruppo di sicurezza. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza.
- Applica patch, aggiorna e proteggi con regolarità il sistema e le applicazioni nell'istanza. Per ulteriori informazioni, consulta Gestione degli aggiornamenti. Per linee guida specifiche per i sistemi operativi Windows, consultaProcedure consigliate di sicurezza per le istanze Windows.
- Utilizza Amazon Inspector per individuare e scansionare automaticamente le istanze Amazon EC2 alla ricerca di vulnerabilità software ed esposizione alla rete non intenzionale. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon Inspector.
- Usa AWS Security Hub i controlli per monitorare le tue risorse Amazon EC2 rispetto alle best practice e agli standard di sicurezza. Per ulteriori informazioni sull'utilizzo di Security Hub, consulta Controlli Amazon Elastic Compute Cloud nella Guida per l'utente di AWS Security Hub .

Archiviazione

- Valuta le implicazioni del tipo di dispositivo root per quanto riguarda la persistenza, il backup e il ripristino dei dati. Per ulteriori informazioni, consulta Archiviazione del dispositivo root.
- Utilizza volumi Amazon EBS distinti per il sistema operativo e per i dati. Assicurati che il volume contenente i dati sia persistente dopo l'interruzione dell'istanza. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.
- Utilizza l'instance store disponibile per l'istanza per archiviare i dati temporanei. Ricorda che i dati archiviati nell'instance store vengono eliminati quando arresti o interrompi l'istanza. Se utilizzi un instance store per lo storage dei database, assicurati di disporre di un cluster con un fattore di replica che garantisca la tolleranza ai guasti.
- Crittografare volumi e snapshot EBS. Per ulteriori informazioni, consulta la crittografia di Amazon EBS nella Guida per l'utente di Amazon EBS.

Gestione delle risorse

- Utilizza i metadati dell'istanza e i tag di risorsa personalizzati per monitorare e identificare le risorse AWS . Per ulteriori informazioni, consulta Utilizzo dei metadati delle istanze e Tagging delle risorse Amazon EC2..
- Visualizza le restrizioni correnti valide per Amazon EC2. Pianifica le richieste di incremento dei limiti con un certo anticipo rispetto a quando ne avrai effettivamente bisogno. Per ulteriori informazioni, consulta Service Quotas di Amazon EC2.
- Utilizzala AWS Trusted Advisor per ispezionare il tuo AWS ambiente e poi formulare raccomandazioni quando esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza. Per ulteriori informazioni, consulta AWS Trusted Advisor nella Guida per l'utente di AWS Support .

Backup e ripristino

- Esegui regolarmente il backup dei volumi EBS utilizzando gli snapshot Amazon EBS e crea un' Amazon Machine Image (AMI) dall'istanza per salvare la configurazione come modello per l'avvio delle istanze future. Per ulteriori informazioni sui AWS servizi che aiutano a raggiungere questo caso d'uso, consulta AWS BackupAmazon Data Lifecycle Manager.
- Distribuisci i componenti di importanza critica dell'applicazione in più zone di disponibilità e replica i dati di conseguenza.
- Progetta le applicazioni in modo che siano in grado di gestire l'indirizzamento IP dinamico quando l'istanza viene riavviata. Per ulteriori informazioni, consulta Indirizzamento IP per le istanze Amazon EC2.
- Esegui il monitoraggio degli eventi e rispondi agli eventi. Per ulteriori informazioni, consulta Monitoraggio di Amazon EC2.
- Assicurati di essere preparato a gestire situazioni di failover. Come soluzione di base puoi collegare manualmente un'interfaccia di rete o un indirizzo IP elastico a un'istanza di sostituzione. Per ulteriori informazioni, consulta Interfacce di rete elastiche. Per una soluzione automatizzata, puoi utilizzare Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Guida per l'utente di Amazon EC2 Auto Scaling.
- Esegui regolarmente dei test del processo di recupero di istanze e volumi Amazon EBS per garantire che i dati e i servizi vengano ripristinati correttamente.

Reti

- Imposta il valore time-to-live (TTL) per le tue applicazioni su 255, per IPv4 e IPv6. Se si utilizza un valore inferiore, esiste il rischio che il TTL scada mentre il traffico dell'applicazione è in transito, causando problemi di raggiungibilità per le istanze.

Amazon Machine Images (AMI)

Un'Amazon Machine Image (AMI) è un'immagine fornita da AWS che fornisce le informazioni necessarie per avviare un'istanza. Devi specificare un'AMI quando avvii un'istanza. Puoi avviare più istanze da un'unica AMI quando devi disporre di più istanze con la stessa configurazione. Puoi utilizzare AMI diverse per avviare istanze quando devi disporre di istanze con configurazioni diverse.

Un'AMI include i seguenti elementi:

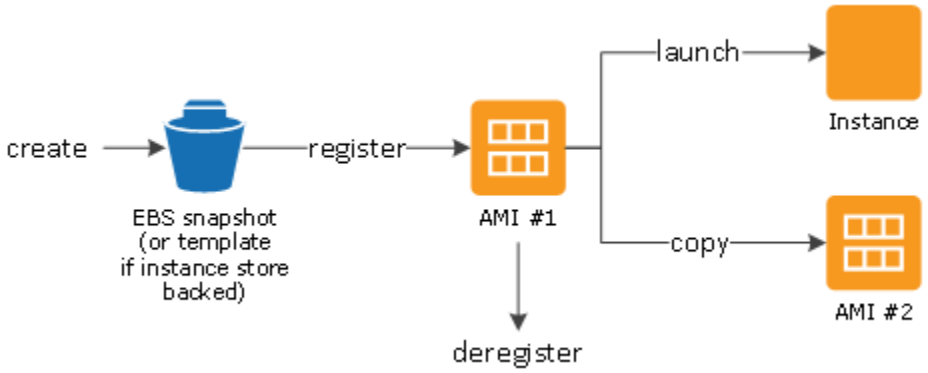
- Una o più istantanee di Amazon Elastic Block Store (Amazon EBS) o, per le AMI, un modello instance-store-backed per il volume root dell'istanza (ad esempio, un sistema operativo, un server delle applicazioni e applicazioni).
- Autorizzazioni di avvio che controllano quali AWS account possono utilizzare l'AMI per avviare le istanze.
- Una mappatura dei dispositivi a blocchi che specifica i volumi da collegare all'istanza quando questa viene avviata

Argomenti dell'Amazon Machine Image (AMI)

- Comprendere le informazioni di fatturazione AMI
- Quote di AMI

Utilizzare un'AMI

Nel seguente diagramma viene riepilogato il ciclo di vita dell'AMI. Dopo aver creato e registrato un'AMI, puoi utilizzarla per avviare nuove istanze. Puoi avviare istanze anche da un'AMI se il relativo proprietario ti concede i permessi di avvio. Puoi copiare un AMI all'interno della stessa AWS regione o in AWS regioni diverse. Quando un'AMI non è più necessaria, puoi annullare la relativa registrazione.



Puoi cercare un'AMI che soddisfi i criteri specifici dell'istanza desiderata. Puoi cercare le AMI fornite dalla comunità AWS o le AMI fornite dalla community. Per ulteriori informazioni, consulta Tipi di AMI e Trovare una AMI.

Dopo aver avviato un'istanza da un'AMI, puoi stabilire una connessione. Quando sei connesso a un'istanza, puoi utilizzarla come useresti qualsiasi altro server. Per ulteriori informazioni su avvio, connessione e utilizzo dell'istanza, consulta Nozioni di base su Amazon EC2.

Creare un'AMI

È possibile avviare un'istanza da un'AMI esistente, personalizzare l'istanza (ad esempio, installare software sull'istanza) e quindi salvare questa configurazione aggiornata come AMI personalizzata. Le istanze avviate da questa nuova AMI personalizzata includono le personalizzazioni apportate durante la creazione dell'AMI stessa.

Il dispositivo di archiviazione root dell'istanza determina il processo da seguire per creare un'AMI. Il volume root di un'istanza è un volume Amazon Elastic Block Store (Amazon EBS) o un volume

instance store. Per ulteriori informazioni sui volumi dispositivo root, consulta Volumi root per le tue istanze Amazon EC2.

- Per creare un'AMI Amazon EBS-backed, consulta Crea un'AMI supportata da Amazon EBS.
- Per creare un'AMI supportata da instance store, consulta Creazione di un'AMI Linux supportata da un instance store.

Per semplificare la suddivisione in categorie e la gestione delle AMI, puoi assegnare tag personalizzati. Per ulteriori informazioni, consulta Tagging delle risorse Amazon EC2..

Comprare, condividere e vendere AMI

Dopo aver creato un'AMI, puoi mantenerla privata in modo che solo tu possa usarla oppure puoi condividerla con un elenco di AWS account specificato. Puoi inoltre rendere pubblica un'AMI personalizzata in modo da consentirne l'uso da parte della community. La creazione di un'AMI sicura, protetta e utilizzabile per l'uso pubblico è un processo molto semplice se segui alcune semplici linee guida. Per ulteriori informazioni su come creare e utilizzare le AMI condivise, consulta AMI condivise.

Puoi acquistare AMI da terze parti, comprese le AMI fornite assieme ai contratti di servizio di organizzazioni quali Red Hat. Puoi anche creare AMI e venderle ad altri utenti Amazon EC2. Per ulteriori informazioni sull'acquisto o sulla vendita di AMI, consulta AMI a pagamento.

Annullare la registrazione dell'AMI

Puoi annullare la registrazione di un'AMI quando hai terminato di utilizzarla. Dopo aver annullato la registrazione di un'AMI, non puoi più utilizzarla per avviare nuove istanze. Le istanze esistenti avviate dall'AMI non saranno interessate da questa operazione. Per ulteriori informazioni, consulta Annullare la registrazione (eliminare) un AMI.

Amazon Linux 2023 e Amazon Linux 2

L'ultima versione di Amazon Linux, AL2023, è ottimizzata per Amazon EC2 e viene fornita senza costi aggiuntivi agli utenti di Amazon EC2. Le funzionalità di AL2023 includono una cadenza di rilascio delle versioni prevedibile, aggiornamenti frequenti e supporto a lungo termine.

Per ulteriori informazioni sulle funzionalità di AL2023 e sull'avvio di un'AMI AL2023, consulta:

- AL2023 Caratteristiche
- Nozioni di base su AL2023

Amazon Linux 2 (AL2) fornisce un ambiente di esecuzione stabile, sicuro e ad alte prestazioni per le applicazioni in esecuzione su Amazon EC2. Per ulteriori informazioni su Amazon Linux 2, consulta Amazon Linux 2 su Amazon EC2 nella Amazon Linux 2 User Guide.

> **Note**
>
> L'AMI Amazon Linux ha raggiunto il 31 end-of-life dicembre 2023 e non riceverà aggiornamenti di sicurezza o correzioni di bug a partire dal 1° gennaio 2024. Per ulteriori informazioni sull'AMI Amazon Linux end-of-life e sul supporto di manutenzione, consulta il post di blog Update on Amazon Linux AMI end-of-life. Ti consigliamo di aggiornare le applicazioni ad AL2023, che include il supporto a lungo termine fino al 2028.

AMI Windows

AWS fornisce un set di AMI disponibili pubblicamente che contengono configurazioni software specifiche per la piattaforma Windows. Puoi cominciare rapidamente a sviluppare e distribuire le applicazioni con Amazon EC2 usando queste AMI. Scegli innanzitutto l'AMI che soddisfa i tuoi specifici requisiti, quindi utilizza tale AMI per avviare un'istanza. Recupera la password dell'account amministratore e quindi accedi all'istanza utilizzando la connessione al desktop remoto, mediante la stessa procedura utilizzata con qualsiasi altro server Windows. Per ulteriori informazioni sulle AMI AWS Windows, consulta il riferimento alle AMI AWS Windows.

Quando si avvia un'istanza da un'AMI di Windows, il dispositivo principale per l'istanza di Windows è un volume Amazon Elastic Block Store (Amazon EBS). Le AMI Windows non supportano l'instance store per il dispositivo root.

Le AMI Windows configurate per un avvio più rapido con EC2 Fast Launch sono preconfigurate e utilizzano istantanee per avviare le istanze fino al 65% più velocemente. Per saperne di più su EC2 Fast Launch, consulta. Usa EC2 Fast Launch per le tue istanze Windows

> **Note**
>
> Microsoft non supporta più le versioni di Windows Server precedenti a Windows Server 2016. Ti consigliamo di avviare nuove istanze EC2 utilizzando una versione supportata di Windows

Server. Se disponi di istanze EC2 esistenti che eseguono una versione non supportata di Windows Server, ti consigliamo di aggiornare queste istanze a una versione aggiornata di Windows Server. Per ulteriori informazioni, consulta Aggiornamento di un'istanza Amazon EC2 Windows a una versione più recente di Windows Server.

Tipi di AMI

Puoi selezionare un'AMI da utilizzare in base alle seguenti caratteristiche:

- Regione (consulta Regioni e zone)
- Sistema operativo
- Architettura (a 32 bit o a 64 bit)
- Permessi di avvio
- Archiviazione del dispositivo root

Permessi di avvio

Il proprietario di un'AMI determina la disponibilità dell'AMI stessa specificando i permessi di avvio. I permessi di avvio sono suddivisi nelle seguenti categorie.

Permesso di avvio	Descrizione
pubblico	Il proprietario concede le autorizzazioni di avvio a tutti gli AWS account.
esplicito	Il proprietario concede le autorizzazioni di avvio a specifici AWS account, organizzazioni o unità organizzative (OU).
implicito	Il proprietario concede permessi di avvio impliciti per un'AMI.

Amazon e la community Amazon EC2 mettono a disposizione un'ampia selezione di AMI pubbliche. Per ulteriori informazioni, consulta AMI condivise. Gli sviluppatori possono richiedere un pagamento per le proprie AMI. Per ulteriori informazioni, consulta AMI a pagamento.

Archiviazione del dispositivo root

Tutte le AMI sono suddivise tra AMI supportate da Amazon EBS e AMI supportate dall'archivio istanza.

- AMI Amazon EBS-backed: il dispositivo root per un'istanza avviata dall'AMI è un volume Amazon Elastic Block Store (Amazon EBS) creato da uno snapshot (Amazon EBS). Supportato per le AMI Linux e Windows.
- AMI supportata dall'archivio dell'istanza Amazon: il dispositivo root per un'istanza avviata dall'AMI è un volume di archivio istanza creato da un modello archiviato in Amazon S3. Supportato solo per le AMI Linux. Le AMI di Windows non supportano l'archivio istanza per il dispositivo root.

Per ulteriori informazioni, consulta Volumi root per le tue istanze Amazon EC2.

La tabella seguente offre un riepilogo delle principali differenze relative all'utilizzo dei due tipi di AMI.

Caratteristica	AMI Amazon EBS-backed	AMI supportata da instance store di Amazon
Tempo di avvio di un'istanza	In genere meno di 1 minuto	In genere meno di 5 minuti
Limite delle dimensioni di un dispositivo root	64 TiB**	10 GiB
Volume dispositivo root	Volume EBS	Volume di instance store
Persistenza dei dati	Per impostazione predefinita, il volume root viene eliminato quando viene terminata l'istanza .* I dati su qualsiasi altro volume EBS sono persistenti dopo l'interruzione dell'istanza per impostazione predefinita.	I dati in qualsiasi volume instance store sono persistenti solo durante il ciclo di vita dell'istanza.

Caratteristica	AMI Amazon EBS-backed	AMI supportata da instance store di Amazon
Modifiche	Il tipo di istanza, il kernel, il disco RAM e i dati utente possono essere modificati mentre l'istanza è arrestata.	Gli attributi di istanza sono fissi per la durata di un'istanza.
Costi	Ti vengono addebitati i costi per l'utilizzo dell'istanza, l'utilizzo del volume EBS e l'archiviazione dell'AMI come snapshot EBS.	Ti vengono addebitati i costi per l'utilizzo dell'istanza e l'archivi azione dell'AMI in Amazon S3.
Creazione/raggrupp amento delle AMI	Utilizza un unico comando/c hiamata	Richiede l'installazione e l'utilizzo degli strumenti AMI
Stato arrestato	Può essere in uno stato di arresto. Anche quando l'istanza viene arrestata e non in è esecuzione, il volume root viene mantenuto in Amazon EBS	Non possono essere in stato arrestate; le istanze sono in esecuzione o terminate

* Per impostazione predefinita, i volumi root EBS hanno il flag `DeleteOnTermination` impostato su `true`. Per informazioni su come modificare questo flag in modo che il volume sia persistente dopo l'interruzione, consulta Modifica il volume root di un'istanza Amazon EC2 in modo che rimanga.

** Supportato solo con `io2` EBS Block Express. Per ulteriori informazioni, consulta i volumi Provisioned IOPS SSD Block Express nella Amazon EBS User Guide.

Determinare il tipo di dispositivo root dell'AMI

Per definire il tipo di dispositivo root di un'AMI utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli AMI, quindi seleziona l'AMI.

3. Nella scheda Details (Dettagli), controllare il valore di Root device type (Tipo di dispositivo root) come riportato di seguito:

   - `ebs` — Si tratta di un'AMI supportata da EBS.
   - `instance store` — Si tratta di un'AMI supportata dall'archivio dell'istanza

Per determinare il tipo di dispositivo root di un'AMI utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- describe-images (AWS CLI)
- Get-EC2Image (AWS Tools for Windows PowerShell)

Stato arrestato

È possibile arrestare un'istanza con un volume EBS per il dispositivo root, ma non è possibile arrestare un'istanza con un volume di archivio istanza per il dispositivo root.

L'arresto fa sì che l'esecuzione dell'istanza venga interrotta (il suo stato passa da `running` a `stopping` a `stopped`). Un'istanza arrestata rimane persistente in Amazon EBS, dove è possibile riavviarla. L'arresto è diverso dalla terminazione dell'istanza. Non è possibile, infatti, riavviare un'istanza terminata. Poiché le istanze con un volume di archivio istanza per il dispositivo root non possono essere arrestate, esse sono in esecuzione o terminate. Per ulteriori informazioni su cosa accade e su cosa è possibile fare quando un'istanza viene arrestata, consulta Arresta e avvia le istanze Amazon EC2.

Archiviazione dei dati di default e persistenza

Le istanze che utilizzano un volume di archivio istanza per il dispositivo root dispongono automaticamente di un archivio istanza (il volume root contiene la partizione root, dove potrai archiviare dati aggiuntivi). Puoi aggiungere un'archiviazione persistente all'istanza collegando uno o più volumi EBS. Tutti i dati in un volume instance store vengono eliminati quando l'istanza ha esito negativo o viene terminata. Per ulteriori informazioni, consulta Volume dell'archivio dell'istanza e durata dei dati.

Le istanze che hanno Amazon EBS per il dispositivo root viene hanno automaticamente un volume EBS collegato. Il volume viene visualizzato nell'elenco di volumi come qualsiasi altro. Per la maggior

parte dei tipi di istanza, le istanze che dispongono di un volume EBS per il dispositivo root non dispongono di volumi di archivio istanza per impostazione predefinita. Puoi aggiungere dei volumi di archivio istanza o altri volumi EBS utilizzando una mappatura dei dispositivi a blocchi. Per ulteriori informazioni, consulta Mappatura dei dispositivi a blocchi.

Tempi di avvio

Le istanze avviate da un'AMI Amazon EBS-backed sono caratterizzate da un avvio più rapido rispetto alle istanze avviate da un'AMI supportata da instance store. Quando avvii un'istanza da un'AMI supportata da instance store, tutte le parti dovranno essere recuperate da Amazon S3 prima che l'istanza sia disponibile. Con un'AMI Amazon EBS-backed, solo le parti necessarie per l'avvio dell'istanza devono essere recuperate dallo snapshot prima che l'istanza sia disponibile. Tuttavia, le prestazioni di un'istanza che utilizza un volume EBS per il proprio dispositivo root sono più lente per un breve periodo, durante il quale le restanti parti vengono recuperate dallo snapshot e caricate nel volume. Quando arresti e riavvii l'istanza, questa viene avviata rapidamente, perché lo stato è memorizzato in un volume EBS.

Creazione di AMI

Per creare AMI Linux supportate da instance store, devi creare un'AMI dall'istanza sull'istanza stessa utilizzando gli strumenti AMI di Amazon EC2. Tieni presente che le AMI Windows non supportano l'archivio di istanze per il dispositivo root.

La creazione di AMI è molto più semplice per le AMI supportate da Amazon EBS. L'operazione API `CreateImage` crea un'AMI Amazon EBS-backed e la registra. C'è anche un pulsante AWS Management Console che consente di creare un AMI da un'istanza in esecuzione. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.

Come vengono addebitati i costi

Con le AMI supportate da instance store, ti vengono addebitati i costi per l'utilizzo dell'istanza e l'archiviazione dell'AMI in Amazon S3. Con le AMI supportate da Amazon EBS, ti vengono addebitati i costi per l'utilizzo dell'istanza, l'utilizzo dell'archiviazione del volume EBS e l'archiviazione dell'AMI come snapshot EBS.

Con le AMI supportate da instance store Amazon EC2 ogni volta che personalizzi un'AMI e ne crei una nuova, tutte le parti per ogni AMI vengono memorizzate in Amazon S3. Pertanto, il footprint dell'archiviazione per ciascuna AMI personalizzata è dato dalle dimensioni complete dell'AMI. Per le AMI Amazon EBS-backed, ogni volta che personalizzi un'AMI e ne crei una nuova, vengono memorizzate solo le modifiche. Pertanto, il footprint dell'archiviazione per le successive AMI

personalizzate dopo la prima è sensibilmente più piccolo. Ciò comporta costi di archiviazione delle AMI più bassi.

Quando un'istanza supportata da viene arrestata, non ti verranno addebitati costi per l'utilizzo dell'istanza. Ti verranno comunque addebitati i costi relativi all'archiviazione del volume. Non appena avvii l'istanza, ti verrà addebitato un minimo di un minuto per l'utilizzo. Dopo un minuto, ti vengono addebitati soli i secondi utilizzati. Ad esempio, se esegui un'istanza per 20 secondi e poi la arresti, ti viene addebitato un minuto completo. Se esegui un'istanza per 3 minuti e 40 secondi, ti vengono addebitati esattamente 3 minuti e 40 secondi di utilizzo. Ti addebiteremo il costo per ogni secondo, con un minimo di un minuto, di esecuzione dell'istanza, anche se l'istanza rimane inattiva e tu non sei collegato a essa.

Tipi di virtualizzazione dell'AMI

Le Amazon Machine Image utilizzano uno dei due tipi di virtualizzazione disponibili: paravirtuale (PV) o hardware virtual machine (HVM). Le principali differenze tra le AMI PV e HVM risiedono nel modo in cui vengono avviate e nella loro capacità di sfruttare i vantaggi delle estensioni hardware speciali (CPU, rete e archiviazione) per l'ottimizzazione delle prestazioni. Le AMI Windows sono AMI HVM.

Per ottenere prestazioni ottimali, ti consigliamo di utilizzare i tipi di istanza della generazione attuale e le AMI HVM quando avvii le istanze. Per ulteriori informazioni su questi tipi di istanze, consulta Tipi di istanze di Amazon EC2. Se invece utilizzi i tipi di istanza di generazioni precedenti e desideri eseguire l'aggiornamento, consulta Procedure di upgrade e Cambiare il tipo di istanza.

Nella tabella seguente vengono confrontate le AMI HVM e PV.

	HVM	PV
Descrizione	Le AMI HVM sono caratteri zzate da un set completam ente virtualizzato di hardware e configurazione di avvio mediante l'esecuzione della partizione Master Boot Record (MBR) del dispositivo a blocchi root dell'immagine. Questo tipo di virtualizzazione ti permette di eseguire un	Le AMIs PV vengono avviate tramite uno speciale caricator e di avvio denominato PV-GRUB, che inizia il ciclo di avvio e quindi carica in sequenza il kernel specificato nel file `menu.lst` nell'imma gine. I guest paravirtuali possono essere eseguiti su hardware host che non

	HVM	PV
	sistema operativo direttamente su una macchina virtuale senza la necessità di alcuna modifica, come se venisse eseguito su hardware Bare Metal. Il sistema host Amazon EC2 emula parte o tutto l'hardware sottostante presentato al sistema guest.	dispone di supporto esplicito per la virtualizzazione. Storicamente parlando, i sistemi guest PV sono caratterizzati da prestazioni migliori rispetto ai sistemi guest HVM in molti casi, ma in seguito ai miglioramenti apportati alla virtualizzazione HVM e alla disponibilità di driver PV per AMI HVM, ciò non è più vero. Per ulteriori informazioni su PV-GRUB e il suo utilizzo in Amazon EC2, consulta Kernels forniti dall'utente.

	HVM	PV
Supporto per estensioni hardware	Sì. A differenza dei sistemi guest PV, i sistemi guest HVM possono sfruttare le estension i hardware che forniscon o accesso rapido all'hardw are sottostante sul sistema host. Per ulteriori informazi oni sulle estensioni di virtualiz zazione della CPU disponibili in Amazon EC2, consulta Intel Virtualization Technology sul sito Web di Intel. È consigliabile utilizzare le AMI HVM se desideri sfruttare le funzionalità avanzate di rete e la capacità di elaborazi one della GPU. Per garantire il passaggio delle istruzioni ai dispositivi di rete specializ zati e ai dispositivi GPU, il sistema operativo deve essere in grado di accedere alla piattaforma hardware nativa. Ciò è garantito dalla virtualiz zazione HVM. Per ulteriori informazioni, consulta Rete avanzata su Amazon EC2.	No, non possono usufruire di estensioni hardware speciali come reti avanzate o elaborazi one GPU.

	HVM	PV
Tipi di istanze supportati	Tutti i tipi di istanza della generazione corrente supportano le AMI HVM.	I seguenti tipi di istanza di generazioni precedenti supportano le AMI PV: C1, C3, M1, M3, M2 e T1. I tipi di istanza di generazioni precedenti non supportano le AMI PV.
Regioni supportate	Tutte le regioni supportano le istanze HVM.	Asia Pacifico (Tokyo), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Europa (Francoforte), Europa (Irlanda) , Sud America (San Paolo), US East (N. Virginia), Stati Uniti occidentali (California settentrionale) e Stati Uniti occidentali (Oregon)
Come trovare	Verifica che il tipo di virtualiz zazione dell'AMI sia impostato su `hvm`, utilizzando la console o il comando describe-images. Per ulteriori informazioni, consulta Trovare una AMI.	Verifica che il tipo di virtualiz zazione dell'AMI sia impostato su `paravirtual` , utilizzan do la console o il comando describe-images. Per ulteriori informazioni, consulta Trovare una AMI.

PV su HVM

I sistemi guest PV tradizionalmente hanno prestazioni migliori a livello di operazioni di archiviazione e rete rispetto ai sistemi guest HVM perché possono utilizzare i driver speciali per l'I/O che evitano l'overhead dell'emulazione dell'hardware di rete e del disco, mentre i sistemi guest HVM devono tradurre queste istruzioni per l'hardware emulato. I driver PV sono ora disponibili per i sistemi guest HVM. Pertanto i sistemi operativi che non possono essere eseguiti in un ambiente paravirtualizzato possono comunque riscontrare incrementi delle prestazioni a livello di I/O di archiviazione e rete

grazie all'utilizzo di tali driver. Grazie a questi driver PV su HVM, i sistemi guest HVM possono essere caratterizzati dallo stesso livello di prestazioni dei sistemi guest PV.

Modalità di avvio di Amazon EC2

All'avvio di un computer, il primo software in esecuzione è responsabile dell'inizializzazione della piattaforma e fornisce un'interfaccia al sistema operativo per eseguire operazioni specifiche della piattaforma.

Amazon EC2 supporta due varianti del software in modalità di avvio: Unified Extensible Firmware Interface (UEFI) e BIOS legacy.

Possibili parametri della modalità di avvio su un'AMI

Un'AMI può avere uno dei seguenti valori per i parametri della modalità di avvio: `uefi`, `legacy-bios` o `uefi-preferred`. Il parametro della modalità di avvio dell'AMI è facoltativo. Le istanze avviate da AMI che non dispongono di parametri della modalità di avvio utilizzano il valore predefinito del tipo di istanza.

Scopo del parametro della modalità di avvio dell'AMI

Il parametro della modalità di avvio dell'AMI segnala ad Amazon EC2 quale modalità di avvio utilizzare quando si avvia un'istanza. Quando il parametro della modalità di avvio è impostato su `uefi`, EC2 tenta di avviare l'istanza su UEFI. Se il sistema operativo non è configurato per supportare UEFI, l'avvio dell'istanza avrà esito negativo.

Parametro della modalità di avvio UEFI Preferred

Con il parametro della modalità di avvio `uefi-preferred`, puoi creare AMI che supportano sia la variante UEFI che BIOS legacy. Se il parametro della modalità di avvio è impostato su `uefi-preferred` e se il tipo di istanza supporta UEFI, l'istanza viene avviata su UEFI. Se il tipo di istanza non supporta UEFI, l'istanza viene avviata su BIOS legacy.

> **Warning**
>
> Alcune funzionalità, ad esempio l'avvio protetto UEFI, sono disponibili solo per le istanze con modalità di avvio UEFI. Se utilizzi il parametro della modalità di avvio dell'AMI `uefi-preferred` con un tipo di istanza che non supporta UEFI, l'istanza viene avviata come BIOS legacy, con la funzionalità dipendente da UEFI disabilitata. Se fai affidamento sulla

disponibilità di una funzionalità dipendente da UEFI, imposta il parametro della modalità di avvio dell'AMI su `uefi`.

Modalità di avvio predefinite per tipi di istanza

- Tipi di istanza Graviton: UEFI
- Tipi di istanze Intel e AMD: BIOS Legacy

Eseguire tipi di istanze Intel e AMD su UEFI

Most Intel and AMD instance types possono essere eseguiti sia su UEFI sia su BIOS legacy. Per utilizzare UEFI, devi selezionare un'AMI con il parametro della modalità di avvio impostato su `uefi` o `uefi-preferred` e il sistema operativo contenuto nell'AMI configurato per supportare UEFI.

Argomenti della modalità avvio

- Avvio di un'istanza
- Determinare il parametro della modalità di avvio di un'AMI
- Determinare le modalità di avvio supportate di un tipo di istanza
- Determinare la modalità di avvio di un'istanza
- Determinare la modalità di avvio del sistema operativo
- Impostare la modalità di avvio di un'AMI
- Variabili UEFI
- UEFI Secure Boot

Avvio di un'istanza

Puoi avviare un'istanza in modalità di avvio UEFI o BIOS Legacy.

Argomenti

- Limitazioni
- Considerazioni
- Requisiti per l'avvio di un'istanza con UEFI

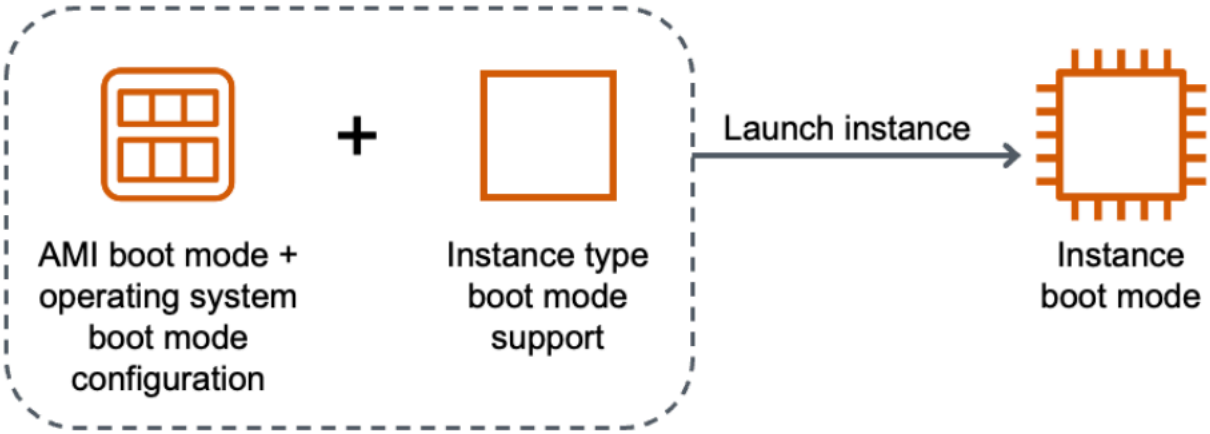
Limitazioni

L'avvio UEFI non è supportato nelle zone locali, nelle zone Wavelength o con AWS Outposts.

Considerazioni

Tieni presente le seguenti informazioni seguenti all'avvio di un'istanza:

- La modalità di avvio dell'istanza è determinata dalla configurazione dell'AMI, dal sistema operativo in essa contenuto e dal tipo di istanza, come illustrato nell'immagine seguente:



La tabella seguente mostra che la modalità di avvio di un'istanza (indicata dalla colonna Modalità di avvio dell'istanza risultante) è determinata dalla combinazione del parametro della modalità di avvio dell'AMI (colonna 1), della configurazione della modalità di avvio del sistema operativo contenuto nell'AMI (colonna 2) e del supporto della modalità di avvio del tipo di istanza (colonna 3).

Parametro della modalità di avvio dell'AMI	Configurazione della modalità di avvio del sistema operativo	Supporto della modalità di avvio del tipo di istanza	Modalità di avvio dell'istanza risultante
UEFI	UEFI	UEFI	UEFI
BIOS legacy	BIOS legacy	BIOS legacy	BIOS legacy
UEFI Preferred	UEFI	UEFI	UEFI
UEFI Preferred	UEFI	UEFI e BIOS legacy	UEFI

Parametro della modalità di avvio dell'AMI	Configurazione della modalità di avvio del sistema operativo	Supporto della modalità di avvio del tipo di istanza	Modalità di avvio dell'istanza risultante
UEFI Preferred	BIOS legacy	BIOS legacy	BIOS legacy
UEFI Preferred	BIOS legacy	UEFI e BIOS legacy	BIOS legacy
Nessuna modalità di avvio specificata - ARM	UEFI	UEFI	UEFI
Nessuna modalità di avvio specificata - x86	BIOS legacy	UEFI e BIOS legacy	BIOS legacy

- Modalità di avvio predefinite:
  - Tipi di istanza Graviton: UEFI
  - Tipi di istanze Intel e AMD: BIOS Legacy
- I tipi di istanze Intel e AMD che supportano UEFI, oltre al BIOS Legacy:
  - Tutte le istanze basate sul sistema AWS Nitro, tranne: istanze bare metal, DL1, G4ad, P4, u-3tb1, u-6tb1, u-9tb1, u-12tb1, u-18tb1, u-24tb1 e VT1

Per visualizzare i tipi di istanza disponibili che supportano UEFI in una regione specifica

I tipi di istanza disponibili variano in base alla Regione AWS. Per vedere i tipi di istanza disponibili che describe-instance-typessupportano `--region` UEFI in una regione, usa il comando con il parametro. Se ometti il parametro `--region`, nella richiesta viene utilizzata la regione predefinita. Includi il parametro `--filters` per assegnare i risultati ai tipi di istanza che supportano UEFI e il parametro `--query` per assegnare l'output al valore di `InstanceType`.

Utilizzate il comando per il vostro sistema operativo.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi --
query "InstanceTypes[*].[InstanceType]" --output text | sort

a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c5.12xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
 Where-Object {$_.SupportedBootModes -Contains "uefi"} | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration

CurrentGeneration: False

InstanceType
------------
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge

CurrentGeneration: True

InstanceType
------------
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
```

```
c5.9xlarge
...
```

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=processor-info.supported-architecture,Values=x86_64 --query "InstanceTypes[*].
[InstanceType]" --output text | sort

c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
c5.large
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
 Where-Object {
     $_.SupportedBootModes -Contains "uefi" -and `
     $_.ProcessorInfo.SupportedArchitectures -eq "x86_64"
     } | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration

CurrentGeneration: True

InstanceType
------------
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
...
```

Per visualizzare i tipi di istanza disponibili che supportano UEFI Secure Boot e mantengono le variabili non volatili in una regione specifica

Attualmente, le istanze bare metal non supportano UEFI Secure Boot e le variabili non volatili. Utilizzate il describe-instance-typescomando come descritto nell'esempio precedente, ma filtrate le istanze bare metal includendo il filtro. `Name=bare-metal,Values=false` Per informazioni su UEFI Secure Boot, consulta UEFI Secure Boot..

Utilizzate il comando per il vostro sistema operativo.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=bare-metal,Values=false --query "InstanceTypes[*].[InstanceType]" --output
 text | sort

a1.2xlarge
a1.4xlarge
a1.large
a1.medium
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
 @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}

InstanceType     SupportedBootModes  BareMetal SupportedArchitectures
------------     ------------------  --------- ----------------------
a1.2xlarge       {uefi}                  False arm64
a1.4xlarge       {uefi}                  False arm64
```

```
a1.large         {uefi}                 False arm64
a1.medium        {uefi}                 False arm64
a1.xlarge        {uefi}                 False arm64
c5.12xlarge      {legacy-bios, uefi}    False x86_64
c5.18xlarge      {legacy-bios, uefi}    False x86_64
```

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-
mode,Values=uefi Name=bare-metal,Values=false Name=processor-info.supported-
architecture,Values=x86_64 --query "InstanceTypes[*].[InstanceType]" --output text |
 sort

c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False -and `
        $_.ProcessorInfo.SupportedArchitectures -eq "x86_64"
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
 @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}

InstanceType    SupportedBootModes  BareMetal SupportedArchitectures
------------    ------------------  --------- ----------------------
c5.12xlarge     {legacy-bios, uefi}     False x86_64
c5.18xlarge     {legacy-bios, uefi}     False x86_64
c5.24xlarge     {legacy-bios, uefi}     False x86_64
c5.2xlarge      {legacy-bios, uefi}     False x86_64
c5.4xlarge      {legacy-bios, uefi}     False x86_64
c5.9xlarge      {legacy-bios, uefi}     False x86_64
```

Requisiti per l'avvio di un'istanza con UEFI

Per avviare un'istanza con modalità di avvio UEFI, devi selezionare un tipo di istanza che supporti UEFI e configurare l'AMI e il sistema operativo per UEFI nel modo seguente:

Tipo di istanza

Quando si avvia un'istanza, è necessario selezionare un tipo di istanza che supporti UEFI. Per ulteriori informazioni, consulta Determinare le modalità di avvio supportate di un tipo di istanza.

AMI

Quando si avvia un'istanza, è necessario selezionare un'AMI configurata per UEFI. L'AMI deve essere configurata come segue:

- Sistema operativo: il sistema operativo contenuto nell'AMI deve essere configurato per utilizzare UEFI; in caso contrario, l'avvio dell'istanza avrà esito negativo. Per ulteriori informazioni, consulta Determinare la modalità di avvio del sistema operativo.
- Parametro della modalità di avvio dell'AMI: il parametro della modalità di avvio dell'AMI deve essere impostato su `uefi` o `uefi-preferred`. Per ulteriori informazioni, consulta Determinare il parametro della modalità di avvio di un'AMI.

Linux: fornisce AWS solo AMI Linux configurate per supportare UEFI per tipi di istanze basati su Graviton. Per utilizzare Linux su altri tipi di istanze UEFI, è necessario configurare l'AMI, importare l'AMI tramite VM Import/Export o importare l'AMI tramite. CloudEndure

Windows: le seguenti AMI Windows supportano UEFI:

- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base
- TPM-Windows_Server-2016-English-Core-Base

Determinare il parametro della modalità di avvio di un'AMI

Il parametro della modalità di avvio dell'AMI è facoltativo. Un'AMI può avere uno dei seguenti valori per i parametri della modalità di avvio: `uefi`, `legacy-bios` o `uefi-preferred`.

Alcune AMI non dispongono di parametri della modalità di avvio. Quando un'AMI non dispone di parametri della modalità di avvio, le istanze avviate da tale AMI utilizzano il valore predefinito del tipo di istanza, vale a dire `uefi` su Graviton, e `legacy-bios` sui tipi di istanza Intel e AMD.

Console

Per determinare il parametro della modalità di avvio di un'AMI (console)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli AMI, e quindi seleziona l'AMI.
3. Ispeziona il campo Modalità di avvio.
   - Il valore uefi indica che l'AMI supporta UEFI.
   - Il valore uefi-preferred indica che l'AMI supporta sia UEFI sia BIOS legacy.
   - Se non è presente un valore, le istanze avviate dall'AMI utilizzano il valore predefinito del tipo di istanza.

Per determinare il parametro della modalità di avvio di un'AMI all'avvio di un'istanza (console)

Quando si avvia un'istanza utilizzando la procedura guidata di avvio dell'istanza, nella fase di selezione dell'AMI, controlla il campo Boot mode (Modalità di avvio). Per ulteriori informazioni, consulta Immagini di applicazioni e sistema operativo (Amazon Machine Image).

AWS CLI

Per determinare il parametro della modalità di avvio di un'AMI (AWS CLI)

Utilizza l'operazione describe-images per determinare la modalità di avvio di un'AMI.

```
aws ec2 describe-images --region us-east-1 --image-id ami-0abcdef1234567890

{
    "Images": [
        {
         ...
            ],
            "EnaSupport": true,
            "Hypervisor": "xen",
            "ImageOwnerAlias": "amazon",
            "Name": "UEFI_Boot_Mode_Enabled-Windows_Server-2016-English-Full-
Base-2020.09.30",
```

```
            "RootDeviceName": "/dev/sda1",
            "RootDeviceType": "ebs",
            "SriovNetSupport": "simple",
            "VirtualizationType": "hvm",
            "BootMode":
 "uefi"
        }
    ]
}
```

Nell'output, il campo `BootMode` indica la modalità di avvio dell'AMI. Il valore `uefi` indica che l'AMI supporta UEFI. Il valore `uefi-preferred` indica che l'AMI supporta sia UEFI che BIOS legacy. Se non è presente un valore, le istanze avviate dall'AMI utilizzano il valore predefinito del tipo di istanza.

PowerShell

Per determinare il parametro della modalità di avvio di un'AMI (Strumenti per PowerShell)

Utilizza il cmdlet Get-EC2Image per determinare la modalità di avvio di un'AMI.

```
PS C:\> Get-EC2Image -Region us-east-1 -ImageId ami-0abcdef1234567890 | Format-List
 Name, BootMode, TpmSupport

Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
BootMode   : uefi
TpmSupport : v2.0
```

Nell'output, il campo `BootMode` indica la modalità di avvio dell'AMI. Il valore `uefi` indica che l'AMI supporta UEFI. Il valore `uefi-preferred` indica che l'AMI supporta sia UEFI che BIOS legacy. Se non è presente un valore, le istanze avviate dall'AMI utilizzano il valore predefinito del tipo di istanza.

Determinare le modalità di avvio supportate di un tipo di istanza

È possibile utilizzare AWS CLI o gli strumenti per PowerShell determinare le modalità di avvio supportate per un tipo di istanza.

Per determinare le modalità di avvio supportate di un tipo di istanza

Per determinare le modalità di avvio supportate di un tipo di istanza, utilizza i metodi seguenti .

AWS CLI

Per determinare le modalità di avvio supportate di un tipo di istanza, utilizza il comando describe-instance-types. Includendo il parametro `--query`, è possibile filtrare l'output. In questo esempio, l'output viene filtrato per restituire solo le modalità di avvio supportate.

L'esempio seguente mostra che `m5.2xlarge` supporta entrambe le modalità di avvio UEFI e BIOS Legacy.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types m5.2xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Output previsto:

```
[
    [
        "legacy-bios",
        "uefi"
    ]
]
```

L'esempio seguente mostra che `t2.xlarge` supporta solo BIOS Legacy.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types t2.xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Output previsto:

```
[
    [
        "legacy-bios"
    ]
]
```

PowerShell

È possibile utilizzare il cmdlet Get-EC2InstanceType(Tools for PowerShell) per determinare le modalità di avvio supportate per un tipo di istanza.

L'esempio seguente mostra che `m5.2xlarge` supporta entrambe le modalità di avvio UEFI e BIOS Legacy.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType m5.2xlarge | Format-List
 InstanceType, SupportedBootModes
```

Output previsto:

```
InstanceType       : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

L'esempio seguente mostra che `t2.xlarge` supporta solo BIOS Legacy.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType t2.xlarge | Format-List
 InstanceType, SupportedBootModes
```

Output previsto:

```
InstanceType       : t2.xlarge
SupportedBootModes : {legacy-bios}
```

Determinare la modalità di avvio di un'istanza

La modalità di avvio di un'istanza viene visualizzata nel campo Modalità di avvio della console Amazon EC2 e dal parametro `currentInstanceBootMode` nella AWS CLI.

Quando viene avviata un'istanza, il valore per il parametro della modalità di avvio è determinato dal valore del parametro della modalità di avvio dell'AMI utilizzata per avviarla, come segue:

- Un'AMI con un parametro della modalità di avvio di `uefi` crea un'istanza con un parametro `currentInstanceBootMode` di `uefi`.
- Un'AMI con un parametro della modalità di avvio di `legacy-bios` crea un'istanza con un parametro `currentInstanceBootMode` di `legacy-bios`.
- Un'AMI con un parametro della modalità di avvio di `uefi-preferred` crea un'istanza con un parametro`currentInstanceBootMode` di `uefi` se il tipo di istanza supporta UEFI. In caso contrario, crea un'istanza con un parametro `currentInstanceBootMode` di `legacy-bios`.
- Un'AMI senza alcun valore per il parametro della modalità di avvio crea un'istanza con un parametro `currentInstanceBootMode` che dipende dal fatto che l'architettura AMI sia ARM o x86 e dalla modalità di avvio supportata del tipo di istanza. La modalità di avvio predefinita è `uefi` su istanze Graviton e `legacy-bios` su tipi di istanza Intel e AMD.

Console

Per determinare la modalità di avvio di un'istanza (console)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e seleziona l'istanza desiderata.
3. Nella scheda Details (Dettagli) controlla il campo Boot mode (Modalità di avvio).

AWS CLI

Per determinare la modalità di avvio di un'istanza (AWS CLI)

Utilizza il comando describe-instances per determinare la modalità di avvio di un'istanza. Puoi inoltre determinare la modalità di avvio dell'AMI utilizzata per creare l'istanza.

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0

{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0e2063e7f6dc3bee8",
                    "InstanceId": "i-1234567890abcdef0",
                    "InstanceType": "m5.2xlarge",
                    ...
                    },
                   "BootMode": "uefi",
                   "CurrentInstanceBootMode": "uefi"
                }
            ],
            "OwnerId": "1234567890",
            "ReservationId": "r-1234567890abcdef0"
        }
    ]
}
```

PowerShell

Per determinare la modalità di avvio di un'istanza (Tools for) PowerShell

Utilizza il cmdlet Get-EC2Image per determinare la modalità di avvio di un'istanza. Puoi inoltre determinare la modalità di avvio dell'AMI utilizzata per creare l'istanza.

Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
 CurrentInstanceBootMode, InstanceType, ImageId

BootMode                : uefi
CurrentInstanceBootMode : uefi
InstanceType            : c5a.large
ImageId                 : ami-0265446f88eb4021b
```

Nell'output, i parametri seguenti descrivono la modalità di avvio:

- `BootMode`: la modalità di avvio dell'AMI utilizzata per creare l'istanza.
- `CurrentInstanceBootMode`: la modalità di avvio utilizzata per avviare l'istanza.

Determinare la modalità di avvio del sistema operativo

La modalità di avvio dell'AMI indica ad Amazon EC2 quale modalità di avvio utilizzare per avviare un'istanza. Per vedere se il sistema operativo dell'istanza è configurato per UEFI, è necessario connettersi all'istanza tramite SSH (istanze Linux) o RDP (istanze Windows).

Consulta le istruzioni relative al sistema operativo della tua istanza.

Linux

Per determinare la modalità di avvio del sistema operativo dell'istanza

1. Connettiti alla tua istanza Linux usando SSH.
2. Per visualizzare la modalità di avvio del sistema operativo, prova una delle seguenti operazioni:

   - Esegui il comando seguente.

     ```
     [ec2-user ~]$ sudo /usr/sbin/efibootmgr
     ```

     Output previsto da un'istanza avviata in modalità di avvio UEFI

     ```
     BootCurrent: 0001
     ```

```
Timeout: 0 seconds
BootOrder: 0000,0001
Boot0000* UiApp
Boot0001* UEFI Amazon Elastic Block Store vol-xyz
```

- Esegui il comando seguente per verificare l'esistenza della directory `/sys/firmware/efi`. Questa directory esiste solo se l'istanza viene avviata utilizzando UEFI. Se la directory non esiste, il comando restituisce `Legacy BIOS Boot Detected`.

```
[ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo
 "Legacy BIOS Boot Detected"
```

Output previsto da un'istanza avviata in modalità di avvio UEFI

```
UEFI Boot Detected
```

Output previsto da un'istanza avviata in modalità di avvio BIOS Legacy

```
Legacy BIOS Boot Detected
```

- Esegui il comando seguente per verificare che EFI venga visualizzata nell'output `dmesg`.

```
[ec2-user ~]$ dmesg | grep -i "EFI"
```

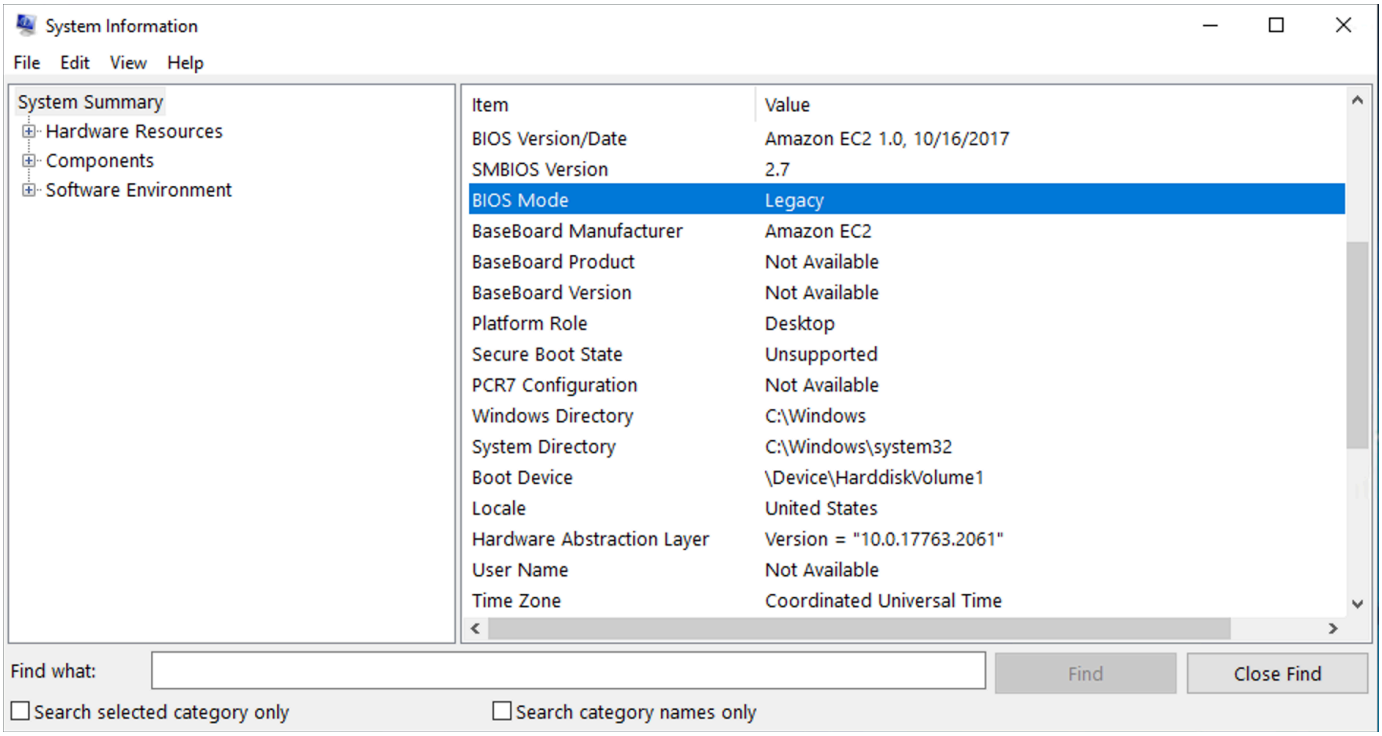
Output previsto da un'istanza avviata in modalità di avvio UEFI

```
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: EFI v2.70 by EDK II
```

Windows

Per determinare la modalità di avvio del sistema operativo dell'istanza

1. Connettiti all'istanza Windows utilizzando RDP.
2. Vai a System Information (Informazioni di sistema) e controlla la riga BIOS Mode (Modalità BIOS).



Impostare la modalità di avvio di un'AMI

Quando crei un'AMI utilizzando il comando register-image, puoi impostare la modalità di avvio dell'AMI su `uefi`, `legacy-bios` o `uefi-preferred`.

Quando la modalità di avvio dell'AMI è impostata su `uefi-preferred`, l'istanza si avvia come segue:

- Per i tipi di istanza che supportano sia UEFI che BIOS legacy (ad esempio `m5.large`), l'istanza si avvia utilizzando UEFI.
- Per i tipi di istanza che supportano solo BIOS legacy (ad esempio `m4.large`), l'istanza si avvia utilizzando tale modalità.

> **Note**
>
> Se imposti la modalità di avvio dell'AMI su `uefi-preferred`, il sistema operativo deve essere in grado di supportare sia la modalità UEFI che BIOS legacy.
> Al momento, non è possibile utilizzare il comando register-image per creare un'AMI che supporti sia NitroTPM che UEFI Preferred.

> **Warning**
>
> Alcune funzionalità, ad esempio l'avvio protetto UEFI, sono disponibili solo per le istanze con modalità di avvio UEFI. Se utilizzi il parametro della modalità di avvio dell'AMI `uefi-preferred` con un tipo di istanza che non supporta UEFI, l'istanza viene avviata come BIOS legacy, con la funzionalità dipendente da UEFI disabilitata. Se fai affidamento sulla disponibilità di una funzionalità dipendente da UEFI, imposta il parametro della modalità di avvio dell'AMI su `uefi`.

Per convertire un'istanza esistente basata su BIOS Legacy in UEFI o un'istanza esistente basata su UEFI in BIOS Legacy, è necessario eseguire una serie di fasi: innanzitutto, devi modificare il volume e il sistema operativo dell'istanza di modo che supportino la modalità di avvio selezionata. Creare quindi uno snapshot del volume. Infine, utilizza register-image per creare l'AMI utilizzando lo snapshot.

Non puoi impostare la modalità di avvio di un'AMI utilizzando il comando create-image. Con create-image, l'AMI eredita la modalità di avvio dell'istanza EC2 utilizzata per creare l'AMI. Ad esempio, se si crea un'AMI da un'istanza EC2 in esecuzione su BIOS Legacy, la modalità di avvio dell'AMI verrà configurata come `legacy-bios`. Se crei un'AMI da un'istanza EC2 avviata utilizzando un'AMI con una modalità di avvio impostata su `uefi-preferred`, anche l'AMI creata avrà la modalità di avvio `uefi-preferred`.

> **Warning**
>
> L'impostazione del parametro della modalità di avvio dell'AMI non configura automaticamente il sistema operativo per la modalità di avvio specificata. Prima di procedere con queste fasi, devi apportare le modifiche adeguate al volume e al sistema operativo dell'istanza per supportare l'avvio tramite la modalità di avvio selezionata; in caso contrario, l'AMI risultante non sarà utilizzabile. Ad esempio, se si sta convertendo un'istanza di Windows basata su BIOS legacy in UEFI, è possibile utilizzare lo strumento MBR2GPT di Microsoft per convertire il disco di sistema da MBR a GPT. Le modifiche necessarie sono specifiche del sistema operativo. Per ulteriori informazioni, consulta il manuale del sistema operativo in uso.

Per impostare la modalità di avvio di un'AMI (AWS CLI)

1. Apporta le modifiche adeguate al volume e al sistema operativo dell'istanza per supportare l'avvio tramite la modalità di avvio selezionata. Le modifiche necessarie sono specifiche del sistema operativo. Per ulteriori informazioni, consulta il manuale del sistema operativo in uso.

   > **Note**
   >
   > Se non si esegue questa fase, l'AMI non sarà utilizzabile.

2. Per trovare l'ID del volume dell'istanza, utilizza il comando describe-instances. Verrà creato uno snapshot del volume nella fase successiva.

   ```
   aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0
   ```

   Output previsto

   ```
   ...
               "BlockDeviceMappings": [
                           {
                               "DeviceName": "/dev/sda1",
                               "Ebs": {
                                   "AttachTime": "",
                                   "DeleteOnTermination": true,
                                   "Status": "attached",
                                   "VolumeId": "vol-1234567890abcdef0"
                               }
                           }
                           ...
   ```

3. Per creare uno snapshot del volume, utilizza il comando create-snapshot. Utilizza l'ID del volume della fase precedente.

   ```
   aws ec2 create-snapshot --region us-east-1 --volume-id vol-1234567890abcdef0 --
   description "add text"
   ```

   Output previsto

   ```
   {
    "Description": "add text",
   ```

```
 "Encrypted": false,
 "OwnerId": "123",
 "Progress": "",
 "SnapshotId": "snap-01234567890abcdef",
 "StartTime": "",
 "State": "pending",
 "VolumeId": "vol-1234567890abcdef0",
 "VolumeSize": 30,
 "Tags": []
}
```

4. Annota l'ID dello snapshot nell'output della fase precedente.
5. Attendi che la creazione dello snapshot sia `completed` prima di passare alla fase successiva. Per eseguire una query sullo stato dello snapshot, utilizza il comando describe-snapshots.

```
aws ec2 describe-snapshots --region us-east-1 --snapshot-ids snap-01234567890abcdef
```

Output di esempio

```
{
    "Snapshots": [
        {
            "Description": "This is my snapshot",
            "Encrypted": false,
            "VolumeId": "vol-049df61146c4d7901",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2019-02-28T21:28:32.000Z",
            "Progress": "100%",
            "OwnerId": "012345678910",
            "SnapshotId": "snap-01234567890abcdef",
...
```

6. Per creare una nuova AMI, utilizza il comando register-image. Utilizza l'ID dello snapshot annotato nella fase precedente.

   - Per impostare la modalità di avvio su UEFI, aggiungi il parametro `--boot-mode` al comando e specifica il valore `uefi`.

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
```

```
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi
```

- Per impostare la modalità di avvio su `uefi-preferred`, aggiungi il parametro `--boot-mode` al comando e specifica il valore `uefi-preferred`.

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi-preferred
```

Output previsto

```
{
"ImageId": "ami-new_ami_123"
}
```

7. Per verificare che l'AMI appena creata disponga della modalità di avvio specificata nella fase precedente, utilizza il comando describe-images.

```
aws ec2 describe-images --region us-east-1 --image-id ami-new_ami_123
```

Output previsto

```
{
  "Images": [
   {
   "Architecture": "x86_64",
```

```
    "CreationDate": "2021-01-06T14:31:04.000Z",
    "ImageId": "ami-new_ami_123",
    "ImageLocation": "",
    ...
    "BootMode": "uefi"
    }
    ]
}
```

8. Avvia una nuova istanza utilizzando l'AMI appena creata.

   Se la modalità di avvio dell'AMI è `uefi` o `legacy-bios`, le istanze create da questa AMI avranno la stessa modalità di avvio. Se la modalità di avvio dell'AMI è `uefi-preferred`, l'istanza verrà avviata utilizzando UEFI se il tipo di istanza supporta tale modalità. In caso contrario, l'istanza verrà avviata utilizzando BIOS legacy. Per ulteriori informazioni, consulta Considerazioni.

9. Per verificare che la nuova istanza disponga della modalità di avvio prevista, utilizza il comando describe-instances.

Variabili UEFI

Quando si avvia un'istanza in cui la modalità di avvio è impostata su UEFI, viene creato un archivio chiave-valore per le variabili. L'archivio può essere utilizzato da UEFI e dal sistema operativo dell'istanza per l'archiviazione delle variabili UEFI.

Le variabili UEFI vengono utilizzate dal bootloader e dal sistema operativo per configurare il startup iniziale del sistema. Consentono al sistema operativo di gestire alcune impostazioni del processo di avvio, come l'ordine di avvio, o di gestire le chiavi per UEFI Secure Boot.

> **Warning**
>
> Chiunque sia in grado di connettersi all'istanza (e potenzialmente a qualsiasi software in esecuzione sull'istanza) o chiunque disponga delle autorizzazioni per utilizzare l'API sull'istanza può leggere le variabili. GetInstanceUefiData Non è necessario archiviare dati sensibili, ad esempio password o informazioni di identificazione personale, nell'archivio variabili UEFI.

Persistenza delle variabili UEFI

- Per le istanze avviate prima del 10 maggio 2022 incluso, le variabili UEFI vengono cancellate al riavvio o all'arresto.
- Per le istanze avviate dopo l'11 maggio 2022 incluso, le variabili UEFI contrassegnate come non volatili vengono mantenute al riavvio e all'arresto/avvio.
- Le istanze bare metal non conservano le variabili non volatili UEFI nelle operazioni di interruzione/avvio dell'istanza.

UEFI Secure Boot

UEFI Secure Boot si basa sul processo di avvio sicuro di lunga data di Amazon EC2 e fornisce funzionalità aggiuntive defense-in-depth che aiutano i clienti a proteggere il software dalle minacce che persistono anche dopo i riavvii. Garantisce che l'istanza avvia solo il software firmato con chiavi crittografiche. Le chiavi sono archiviate nel database delle chiavi dell'archivio delle variabili non volatili UEFI. UEFI Secure Boot impedisce la modifica non autorizzata del flusso di avvio dell'istanza.

Argomenti

- Come funziona UEFI Secure Boot
- Avvio di un'istanza con supporto UEFI Secure Boot
- Verifica dell'abilitazione di un'istanza per UEFI Secure Boot
- Creazione di un'AMI Linux che supporti UEFI Secure Boot
- Come viene creato il blob binario AWS

Come funziona UEFI Secure Boot

UEFI Secure Boot è una caratteristica specificata in UEFI, che fornisce la verifica dello stato della catena di avvio. È progettato per garantire che solo i file binari UEFI verificati crittograficamente vengano eseguiti dopo l'inizializzazione automatica del firmware. Questi file binari includono i driver UEFI e il bootloader principale, oltre a componenti caricati a catena.

UEFI Secure Boot specifica quattro database chiave, utilizzati in una catena di attendibilità. I database sono archiviati nell'archivio delle variabili UEFI.

La catena di attendibilità è la seguente:

Database delle chiavi della piattaforma (Platform Key, PK)

Il database PK è il root di attendibilità. Contiene una singola chiave PK pubblica che viene utilizzata nella catena di attendibilità per l'aggiornamento del database delle chiavi di scambio delle chiavi (Key Exchange Key, KEK).

Per modificare il database PK, è necessario disporre della chiave PK privata per firmare una richiesta di aggiornamento. Ciò include l'eliminazione del database PK scrivendo una chiave PK vuota.

Database delle chiavi di scambio delle chiavi (KEK)

Il database KEK è un elenco di chiavi KEK pubbliche utilizzate nella catena di attendibilità per l'aggiornamento dei database delle firme (DB) e denylist (dbx).

Per modificare il database KEK pubblico, è necessario disporre della chiave PK privata per firmare una richiesta di aggiornamento.

Database firma (DB)

Il database DB è un elenco di chiavi pubbliche e hash utilizzati nella catena di attendibilità per convalidare tutti i file binari di avvio UEFI.

Per modificare il database db, è necessario disporre della chiave PK privata o di chiavi KEK private per firmare una richiesta di aggiornamento.

Database di denylist firme (dbx)

Il database dbx è un elenco di chiavi pubbliche e hash binari che non sono attendibili e vengono utilizzati nella catena di attendibilità come file di revoca.

Il database dbx ha sempre la precedenza su tutti gli altri database di chiavi.

Per modificare il database dbx, è necessario disporre della chiave PK privata o di chiavi KEK private per firmare una richiesta di aggiornamento.

Il forum UEFI mantiene un dbx disponibile pubblicamente per molti file binari e certificati reputati non validi all'indirizzo https://uefi.org/revocationlistfile.

> **Important**
>
> UEFI Secure Boot applica la convalida della firma su qualsiasi file binario UEFI. Per consentire l'esecuzione di un binario UEFI in UEFI Secure Boot, lo devi firmare con una delle chiavi db private descritte sopra.

Per impostazione predefinita, UEFI Secure Boot è disabilitato e il sistema è in modalità `SetupMode`. Quando il sistema è in modalità `SetupMode`, tutte le variabili chiave possono essere aggiornate senza una firma crittografica. Quando il PK è impostato, UEFI Secure Boot viene abilitato e viene chiuso. SetupMode

Avvio di un'istanza con supporto UEFI Secure Boot

Quando avvii un'istanza con i seguenti prerequisiti, l'istanza convaliderà automaticamente i binari di avvio UEFI rispetto al database UEFI Secure Boot. Puoi configurare UEFI Secure Boot su un'istanza anche dopo l'avvio.

> **Note**
>
> UEFI Secure Boot protegge l'istanza e il suo sistema operativo dalle modifiche del flusso di avvio. Se crei una nuova AMI da un AMI di origine con UEFI Secure Boot abilitato e modifichi determinati parametri durante il processo di copia, ad esempio cambiando l'`UefiData`interno dell'AMI, puoi disabilitare UEFI Secure Boot.

Prerequisiti

AMI Linux

Per avviare un'istanza Linux, l'AMI Linux deve avere UEFI Secure Boot abilitato.

Amazon Linux supporta UEFI Secure Boot a partire dal rilascio AL2023 2023.1. Tuttavia, UEFI Secure Boot non è abilitato nelle AMI predefinite. Per ulteriori informazioni, consulta la sezione UEFI Secure Boot nella Guida per l'utente di AL2023. Le versioni precedenti delle AMI Amazon Linux non sono abilitate per UEFI Secure Boot. Per utilizzare un'AMI supportata, è necessario eseguire una serie di passaggi di configurazione sulla propria AMI Linux. Per ulteriori informazioni, consulta Creazione di un'AMI Linux che supporti UEFI Secure Boot.

AMI Windows

Per avviare un'istanza Windows, l'AMI Windows deve avere UEFI Secure Boot abilitato.

Le seguenti AMI Windows sono preconfigurate per abilitare UEFI Secure Boot con chiavi Microsoft:

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise
- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

Al momento, l'importazione di Windows con UEFI Secure Boot tramite il comando import-image non è supportata.

Tipo di istanza

- Supportato: tutti i tipi di istanze virtualizzate che supportano UEFI supportano anche UEFI Secure Boot. Per i tipi di istanza che supportano UEFI Secure Boot, consulta Considerazioni.
- Non supportato: i tipi di istanza bare metal non supportano UEFI Secure Boot.

Verifica dell'abilitazione di un'istanza per UEFI Secure Boot

Istanze Linux

Per verificare se un'istanza Linux è abilitata per UEFI Secure Boot, utilizza l'utilità `mokutil`. Installa `mokutil` se non è già presente nell'istanza. Per le istruzioni di installazione per Amazon Linux 2, consultahttps://docs.aws.amazon.com/linux/al2/ug/find-install-software.html. Per altre distribuzioni Linux, consulta la relativa documentazione specifica.

Per verificare se un'istanza Linux è abilitata per UEFI Secure Boot

Su un'istanza, esegui il comando seguente come `root`.

```
mokutil --sb-state
```

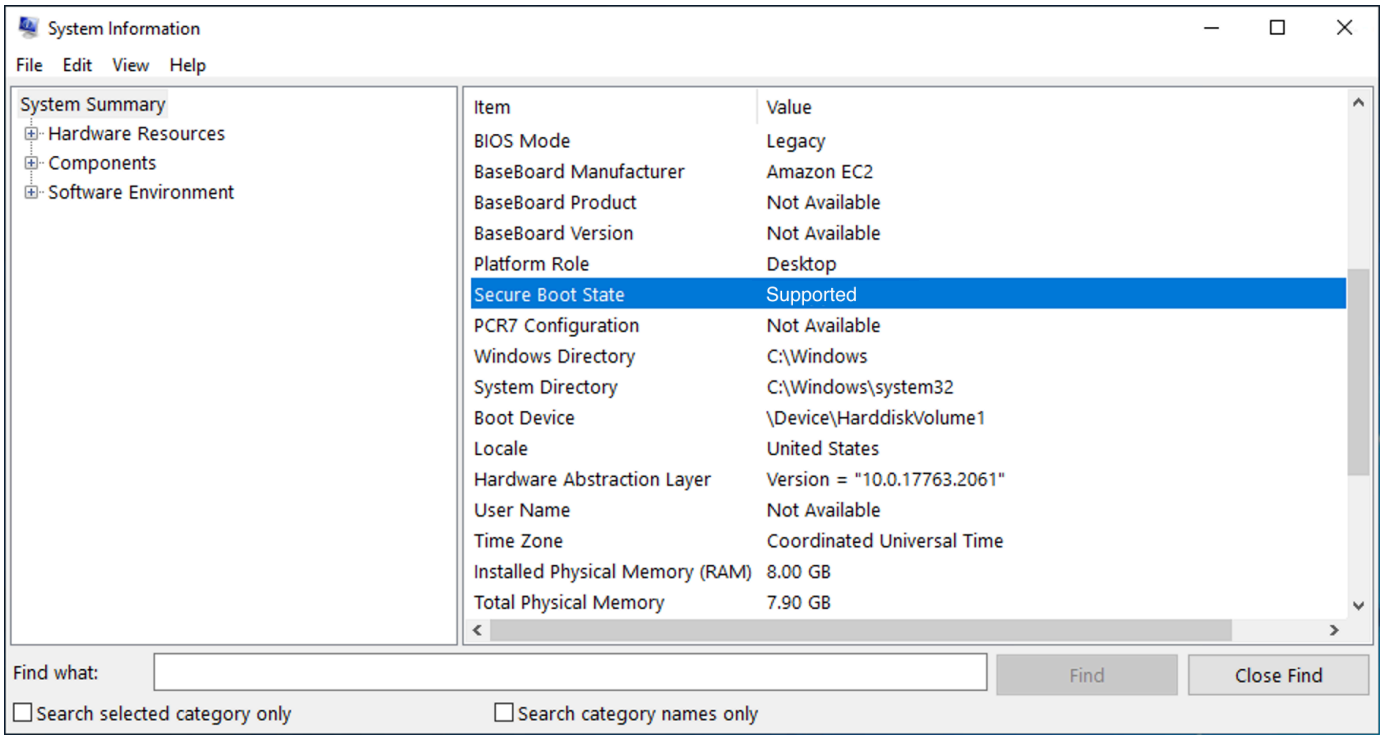
Output previsto:

- Se UEFI Secure Boot è abilitato, l'output contiene `SecureBoot enabled`.
- Se UEFI Secure Boot non è abilitato, l'output contiene `SecureBoot disabled` o `Failed to read SecureBoot`.

Istanze Windows

Per verificare se un'istanza Windows è abilitata per UEFI Secure Boot

1. Apri lo strumento msinfo32.
2. Controlla il campo Secure Boot State (Stato Secure Boot). Supported (Supportato) indica che UEFI Secure Boot è abilitato.



È inoltre possibile utilizzare il PowerShell cmdlet Windows `Confirm-SecureBootUEFI` per verificare lo stato di Secure Boot. Per ulteriori informazioni sul cmdlet, vedere Confirm- SecureBoot UEFI nel sito Web Microsoft Documentation.

Creazione di un'AMI Linux che supporti UEFI Secure Boot

Le seguenti procedure descrivono come creare un archivio delle variabili UEFI per l'avvio sicuro con chiavi private personalizzate. Amazon Linux supporta UEFI Secure Boot a partire dal rilascio AL2023 2023.1. Per ulteriori informazioni, consulta la sezione UEFI Secure Boot nella Guida per l'utente di AL2023.

> **Important**
>
> Le seguenti procedure per la creazione di un'AMI che supporti UEFI Secure Boot sono destinate esclusivamente agli utenti avanzati. Per utilizzare queste procedure è necessario disporre di una conoscenza sufficiente del flusso di avvio della distribuzione SSL e Linux.

Prerequisiti

- Verranno utilizzati i seguenti strumenti:
  - OpenSSL: https://www.openssl.org/
  - efivar: https://github.com/rhboot/efivar
  - efitools: https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git/
  - get-instance-uefi-data AWS CLI comando
- L'istanza Linux deve essere stata avviata con un'AMI Linux che supporta la modalità di avvio UEFI e deve contenere dati non volatili.

Le istanze appena create senza chiavi UEFI Secure Boot vengono create in `SetupMode`, che ti consente di registrare le tue chiavi. Alcune AMI sono preconfigurate con UEFI Secure Boot e non è possibile modificare le chiavi esistenti. Se desideri modificare le chiavi, devi creare una nuova AMI basata sull'AMI originale.

Sono disponibili due modi per propagare le chiavi nell'archivio delle variabili, descritti di seguito sotto Opzione A e Opzione B. L'Opzione A descrive come farlo dall'interno dell'istanza, imitando il flusso di hardware reale. L'Opzione B descrive come creare un blob binario, che viene poi passato come file con codifica base64 quando si crea l'AMI. Per entrambe le opzioni, è necessario innanzitutto creare le tre coppie di chiavi, utilizzate per la catena di attendibilità.

Per creare un'AMI Linux che supporti UEFI Secure Boot, prima devi creare le tre coppie di chiavi e quindi completare l'Opzione A o l'Opzione B:

- Creazione di tre coppie di chiavi
- Opzione A: aggiunta delle chiavi all'archivio delle variabili dall'interno dell'istanza
- Opzione B: creazione di un blob binario contenente un archivio delle variabili preriempito

> **Note**
>
> Queste istruzioni possono essere utilizzate solo per creare un'AMI Linux. Se hai bisogno di un'AMI Windows, usa una delle AMI Windows supportate. Per ulteriori informazioni, consulta Avvio di un'istanza con supporto UEFI Secure Boot.

Creazione di tre coppie di chiavi

UEFI Secure Boot si basa sui seguenti tre database di chiavi, utilizzati in una catena di attendibilità: la chiave di piattaforma (PK), la chiave di scambio delle chiavi (KEK) e il database delle firme (DB).[1]

Crea ciascuna chiave sull'istanza. Per preparare le chiavi pubbliche in un formato valido per lo standard UEFI Secure Boot, devi creare un certificato per ciascuna chiave. `DER` definisce il formato SSL (codifica binaria di un formato). Devi quindi convertire ogni certificato in un elenco di firme UEFI, che è il formato binario compreso da UEFI Secure Boot. Infine, devi firmare ogni certificato con la chiave pertinente.

Argomenti

- Preparazione alla creazione delle coppie di chiavi
- Coppia di chiavi 1: crea la chiave della piattaforma (PK)
- Coppia di chiavi 2: crea la chiave di scambio chiave (KEK)
- Coppia di chiavi 3: crea il database delle firme (DB)
- Firma l'immagine di avvio (kernel) con la chiave privata.

Preparazione alla creazione delle coppie di chiavi

Prima di creare le coppie di chiavi, crea un identificatore univoco globale (GUID) da utilizzare nella generazione delle chiavi.

1. Collegati all'istanza.
2. Esegui il comando seguente in un prompt della shell.

```
uuidgen --random > GUID.txt
```

Coppia di chiavi 1: crea la chiave della piattaforma (PK)

La PK è il root di attendibilità per le istanze UEFI Secure Boot. La PK privata viene utilizzata per aggiornare la KEK, che a sua volta può essere utilizzata per aggiungere chiavi autorizzate al database delle firme (DB).

Lo standard X.509 viene utilizzato per creare la coppia di chiavi. Per informazioni sullo standard, consulta X.509 su Wikipedia.

Per creare la PK

1. Crea la chiave. Devi assegnare un nome alla variabile PK.

   ```
   openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -
   subj "/CN=Platform key/" -out PK.crt
   ```

   Vengono specificati i seguenti parametri:

   - `-keyout PK.key`: il file della chiave privata.
   - `-days 3650`: il numero di giorni per cui il certificato è valido.
   - `-out PK.crt`: il certificato che viene utilizzato per creare la variabile UEFI.
   - CN=*Platform key*: il nome comune (CN) della chiave. Puoi inserire il nome della tua organizzazione al posto di *Platform key* (Chiave della piattaforma).
2. Crea il certificato.

   ```
   openssl x509 -outform DER -in PK.crt -out PK.cer
   ```
3. Converti il certificato in un elenco di firme UEFI.

   ```
   cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
   ```
4. Firma l'elenco delle firme UEFI con la PK privata (autofirmata).

   ```
   sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
   ```

Coppia di chiavi 2: crea la chiave di scambio chiave (KEK)

La KEK privata viene utilizzata per aggiungere chiavi al db, ossia l'elenco delle firme autorizzate da avviare sul sistema.

Per creare la KEK

1. Crea la chiave.

```
openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Key Exchange Key/" -out KEK.crt
```

2. Crea il certificato.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Converti il certificato in un elenco di firme UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Firma l'elenco delle firme con la PK privata.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Coppia di chiavi 3: crea il database delle firme (DB)

L'elenco db contiene chiavi autorizzate per l'avvio sul sistema. Per modificare l'elenco, è necessaria la KEK privata. Le immagini di avvio saranno firmate con la chiave privata creata in questa fase.

Per creare il db

1. Crea la chiave.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -
subj "/CN=Signature Database key/" -out db.crt
```

2. Crea il certificato.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Converti il certificato in un elenco di firme UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Firma l'elenco delle firme con la KEK privata.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Firma l'immagine di avvio (kernel) con la chiave privata.

Per Ubuntu 22.04, le seguenti immagini richiedono le firme.

```
/boot/efi/EFI/ubuntu/shimx64.efi
/boot/efi/EFI/ubuntu/mmx64.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/vmlinuz
```

Per firmare un'immagine

Utilizza una sintassi come la seguente per firmare un'immagine.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

> **Note**
>
> Devi firmare tutti i nuovi kernel. Di solito, */boot/vmlinuz* esegue un collegamento simbolico all'ultimo kernel installato.

Per informazioni sulla catena di avvio e sulle immagini richieste, consulta la documentazione per la distribuzione.

[1] Grazie alla ArchWiki community per tutto il lavoro svolto. I comandi per creare il PK, creare il KEK, creare il DB e firmare l'immagine provengono da Creating keys, creato dal team di ArchWiki manutenzione e/o dai collaboratori. ArchWiki

Opzione A: aggiunta delle chiavi all'archivio delle variabili dall'interno dell'istanza

Dopo avere creato le tre coppie di chiavi, puoi connetterti alla tua istanza e aggiungere le chiavi all'archivio delle variabili dall'interno dell'istanza completando le fasi seguenti.

Fasi dell'Opzione A:

- Fase 1: avvio di un'istanza che supporti UEFI Secure Boot
- Fase 2: configurazione di un'istanza per supportare UEFI Secure Boot
- Fase 3: creazione di un'AMI dall'istanza

Fase 1: avvio di un'istanza che supporti UEFI Secure Boot

Quando avvii un'istanza con i seguenti prerequisiti, l'istanza sarà pronta per essere configurata per supportare UEFI Secure Boot. È possibile abilitare il supporto per UEFI Secure Boot su un'istanza solo al momento dell'avvio; non è possibile abilitarlo in un secondo momento.

Prerequisiti

- AMI: l'AMI Linux deve supportare la modalità di avvio UEFI. Per verificare che l'AMI supporti la modalità di avvio UEFI, il parametro della modalità di avvio AMI deve essere uefi. Per ulteriori informazioni, consulta Determinare il parametro della modalità di avvio di un'AMI.

  Nota che fornisce AWS solo AMI Linux configurate per supportare UEFI per tipi di istanze basate su Graviton. AWS attualmente non fornisce AMI Linux x86_64 che supportano la modalità di avvio UEFI. Puoi configurare un'AMI personalizzata che supporta la modalità di avvio UEFI per tutte le architetture. Per utilizzare un'AMI personalizzata che supporta la modalità di avvio UEFI, devi eseguire una serie di passaggi di configurazione sulla tua AMI. Per ulteriori informazioni, consulta Impostare la modalità di avvio di un'AMI.
- Tipo di istanza: tutti i tipi di istanze virtualizzate che supportano UEFI supportano anche UEFI Secure Boot. I tipi di istanza bare metal non supportano UEFI Secure Boot. Per i tipi di istanza che supportano UEFI Secure Boot, consulta Considerazioni.
- Avvia l'istanza dopo il rilascio di UEFI Secure Boot. Solo le istanze avviate dopo il 10 maggio 2022 (quando è stato rilasciato UEFI Secure Boot) possono supportare UEFI Secure Boot.

Dopo avere avviato l'istanza, puoi verificare che sia pronta per essere configurata per supportare UEFI Secure Boot (in altre parole, puoi procedere alla Fase 2) verificando se i dati UEFI sono presenti. La presenza di dati UEFI indica che i dati non volatili sono persistenti.

Per verificare se l'istanza è pronta per la fase 2

Utilizza il comando get-instance-uefi-data e specifica l'ID dell'istanza.

```
aws ec2 get-instance-uefi-data --instance-id i-0123456789example
```

L'istanza è pronta per la fase 2 se i dati UEFI sono presenti nell'output. Se l'output è vuoto, l'istanza non può essere configurata per supportare UEFI Secure Boot. Ciò può verificarsi se l'istanza è stata avviata prima che il supporto UEFI Secure Boot fosse disponibile. Avvia una nuova istanza e riprova.

Fase 2: configurazione di un'istanza per supportare UEFI Secure Boot

Registrazione delle coppie di chiavi nell'archivio delle variabili UEFI dell'utente sull'istanza

> **Warning**
>
> Le immagini di avvio devono essere firmate dopo avere registrato le chiavi, altrimenti non potrai avviare l'istanza.

Dopo avere creato gli elenchi di firme UEFI firmati (`PK`, `KEK` e `db`), gli elenchi devono essere iscritti al firmware UEFI.

La scrittura nella variabile `PK` è possibile solo se:

- Nessuna PK è ancora iscritta, nel qual caso la variabile `SetupMode` ha il valore `1`. Per verificarlo, utilizza il comando seguente. L'output è `1` o `0`.

  ```
  efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
  ```

- La nuova PK è firmata dalla chiave privata della PK esistente.

Per registrare le chiavi nell'archivio delle variabili UEFI dell'utente

I seguenti comandi devono essere eseguiti sull'istanza.

Se SetupMode è abilitato (il valore è1), le chiavi possono essere registrate eseguendo i seguenti comandi sull'istanza:

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

Per verificare che UEFI Secure Boot sia abilitato

Per verificare che UEFI Secure Boot sia abilitato, attieniti alla procedura descritta in Verifica dell'abilitazione di un'istanza per UEFI Secure Boot.

Ora puoi esportare l'archivio delle variabili UEFI con il comando CLI get-instance-uefi-data oppure procedere alla fase successiva e firmare le immagini di avvio per riavviare un'istanza abilitata per UEFI Secure Boot.

Fase 3: creazione di un'AMI dall'istanza

Per creare un'AMI dall'istanza, puoi utilizzare la console o l'API `CreateImage`, la CLI o gli SDK. Per le istruzioni relative alla console, consulta la sezione Crea un'AMI supportata da Amazon EBS. Per le istruzioni sull'API, consulta CreateImage.

> **Note**
>
> L'API `CreateImage` copia automaticamente l'archivio delle variabili UEFI dell'istanza nell'AMI. La console utilizza l'API `CreateImage`. Dopo avere avviato le istanze utilizzando questa AMI, le istanze avranno lo stesso archivio delle variabili UEFI.

Opzione B: creazione di un blob binario contenente un archivio delle variabili preriempito

Dopo aver creato le tre coppie di chiavi, puoi creare un blob binario contenente un archivio delle variabili preriempito contenente le chiavi UEFI Secure Boot.

> **Warning**
>
> Le immagini di avvio devono essere firmate prima di registrare le chiavi, altrimenti non potrai avviare l'istanza.

Fase dell'opzione B:

- Fase 1: creazione di un nuovo archivio delle variabili o aggiornamento di un archivio esistente
- Fase 2: caricamento del blob binario al momento della creazione dell'AMI

Fase 1: creazione di un nuovo archivio delle variabili o aggiornamento di un archivio esistente

Puoi creare l'archivio delle variabili non in linea senza un'istanza in esecuzione utilizzando lo strumento python-uefivars. Lo strumento può creare un nuovo archivio delle variabili a partire dalle chiavi. Lo script attualmente supporta il formato EDK2, il AWS formato e una rappresentazione JSON che è più facile da modificare con strumenti di livello superiore.

Per creare l'archivio delle variabili non in linea senza un'istanza in esecuzione

1. Scarica lo strumento al seguente link.

   ```
   https://github.com/awslabs/python-uefivars
   ```

2. Crea un nuovo archivio delle variabili a partire dalle chiavi eseguendo il comando seguente. Ciò creerà un blob binario con codifica base64 in *your_binary_blob*.bin. Lo strumento supporta anche l'aggiornamento di un blob binario tramite il parametro `-I`.

   ```
   ./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db
    db.esl --dbx dbx.esl
   ```

Fase 2: caricamento del blob binario al momento della creazione dell'AMI

Utilizza register-image per passare i dati dell'archivio delle variabili UEFI. Per il parametro `--uefi-data` specifica il blob binario, mentre per il parametro `--boot-mode` specifica `uefi`.

```
aws ec2 register-image \
    --name uefi_sb_tpm_register_image_test \
    --uefi-data $(cat your_binary_blob.bin) \
    --block-device-mappings "DeviceName=/dev/sda1,Ebs=
 {SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \
    --architecture x86_64 \
    --root-device-name /dev/sda1 \
    --virtualization-type hvm \
    --ena-support \
    --boot-mode uefi
```

Come viene creato il blob binario AWS

Puoi completare le fasi seguenti per personalizzare le variabili UEFI Secure Boot durante la creazione di un'AMI. La KEK che viene utilizzata in queste fasi è in vigore a partire da settembre 2021. Se Microsoft aggiorna la KEK, devi utilizzare la KEK più recente.

Per creare il blob AWS binario

1. Crea un elenco di firme PK vuoto.

```
touch empty_key.crt
cert-to-efi-sig-list empty_key.crt PK.esl
```

2. Scarica i certificati KEK.

```
https://go.microsoft.com/fwlink/?LinkId=321185
```

3. Avvolgi i certificati KEK in un elenco di firme UEFI (`siglist`).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Scarica i certificati db di Microsoft.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011_2011-06-27.crt
```

5. Genera l'elenco delle firme db.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. Scarica una richiesta di modifica dbx aggiornata dal seguente link.

```
https://uefi.org/revocationlistfile
```

7. La richiesta di modifica dbx scaricata nella fase precedente è già firmata con la chiave Microsoft, quindi è necessario svuotarla o decomprimerla. Puoi usare i seguenti link.

```
https://gist.github.com/out0xb2/f8e0bae94214889a89ac67fceb37f8c0
```

```
https://support.microsoft.com/en-us/topic/microsoft-guidance-for-applying-secure-boot-dbx-update-e3b9e4cb-a330-b3ba-a602-15083965d9ca
```

8. Crea un archivio delle variabili UEFI usando lo script `uefivars.py`.

```
./uefivars.py -i none -o aws -O uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K
 ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx ~/dbx-2021-April.bin
```

9. Controlla il blob binario e l'archivio delle variabili UEFI.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. È possibile aggiornare il blob passandolo nuovamente allo stesso strumento.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -O uefiblob-
microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx
 ~/dbx-2021-April.bin
```

Output previsto

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Trovare una AMI

Un'AMI include i componenti e le applicazioni, come il sistema operativo e il tipo di volume root, necessari per avviare un'istanza. Per avviare un'istanza che soddisfi le tue esigenze, devi trovare un'AMI che soddisfi le tue esigenze.

Quando selezioni un'AMI, considera i seguenti requisiti che potresti avere per le istanze che desideri avviare:

- La regione: gli ID AMI sono unici per ogni AWS regione.
- Il sistema operativo

- L'architettura: 32 bit (`i386`), 64 bit (`x86_64`) o 64 bit ARM (`arm64`)
- Il tipo di dispositivo root: Amazon EBS o instance store
- Il fornitore (ad esempio Amazon Web Services)
- Software aggiuntivo (ad esempio SQL Server)

Esistono vari modi per trovare un'AMI che soddisfi le tue esigenze. Questo argomento descrive come trovare un'AMI utilizzando la console Amazon EC2, AWS CLI AWS Tools for Windows PowerShell, e. AWS Systems Manager

Argomenti

Trova un'AMI utilizzando la console Amazon EC2

Puoi trovare le AMI utilizzando la console Amazon EC2. È possibile scegliere dall'elenco delle AMI quando si utilizza la procedura guidata di avvio dell'istanza per avviare un'istanza oppure è possibile eseguire ricerche tra tutte le AMI disponibili utilizzando la pagina Images (Immagini).

Per trovare un'AMI utilizzando la procedura guidata di avvio dell'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione selezionare la regione in cui avviare le istanze. È possibile selezionare qualsiasi regione disponibile, indipendentemente dalla posizione. Gli ID AMI sono unici per ogni AWS regione.
3. Dal pannello di controllo della console, scegliere Launch Instance (Avvia istanza).
4. (Nuova console) In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo (Amazon Machine Image), scegliere Quick Start (Avvio rapido), scegliere il sistema operativo per l'istanza, quindi da Amazon Machine Image (AMI), selezionare nell'elenco una delle AMI comunemente utilizzate. Se l'AMI che si desidera utilizzare non è

visualizzata, è scegliere Browse more AMIs (Sfoglia altre AMI) per sfogliare il catalogo completo di AMI. Per ulteriori informazioni, consulta Immagini di applicazioni e sistema operativo (Amazon Machine Image).

(Vecchia console) Nella scheda Quick Start (Avvio rapido) selezionare nell'elenco un delle AMI comunemente utilizzate. Se l'AMI da usare non viene visualizzata, scegli la scheda My AMIs (Le mie AMI), Marketplace AWS, o Community AMIs (AMI della community) per individuare AMI aggiuntive. Per ulteriori informazioni, consulta Fase 1: scelta di un'Amazon Machine Image (AMI).

Per trovare un'AMI utilizzando la pagina AMI

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione selezionare la regione in cui avviare le istanze. È possibile selezionare qualsiasi regione disponibile, indipendentemente dalla posizione. Gli ID AMI sono unici per ogni AWS regione.
3. Nel riquadro di navigazione scegliere AMIs (AMI).
4. (Opzionale) Utilizza le opzioni di filtro e ricerca per definire l'ambito dell'elenco delle AMI visualizzate e visualizzare solo le AMI corrispondenti ai criteri.

   Ad esempio, per elencare tutte le AMI fornite da AWS, scegli Immagini pubbliche. Quindi utilizza le opzioni di ricerca per definire ulteriormente l'ambito delle AMI visualizzate. Scegli la barra Search (Ricerca) e scegli Owner alias (Alias proprietario) dal menu, quindi seleziona l'operatore = e infine il valore amazon. Per trovare le AMI che corrispondono a una piattaforma specifica, ad esempio Linux o Windows, scegli nuovamente la barra di ricerca per scegliere Piattaforma, quindi l'operatore = e infine il sistema operativo dall'elenco fornito.
5. (Facoltativo) Scegli l'icona Mostra/Nascondi colonne per selezionare gli attributi immagine da visualizzare, come il tipo di dispositivo root. In alternativa, selezione un'AMI dall'elenco e visualizzarne le proprietà nella scheda Details (Dettagli).
6. Prima di selezionare un'AMI, è necessario controllare se è supportata da instance store o da Amazon EBS e conoscere gli effetti di questa differenza. Per ulteriori informazioni, consulta Archiviazione del dispositivo root.
7. Per avviare un'istanza da questa AMI, selezionala e scegli Avvia istanza. Per informazioni sull'utilizzo della console per avviare un'istanza, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza. Se non si è ancora pronti per avviare l'istanza, annotare l'ID dell'AMI per un utilizzo successivo.

Trova un AMI utilizzando il AWS CLI

Puoi utilizzare il AWS CLI comando describe-images per elencare solo le AMI che soddisfano i tuoi requisiti. Dopo aver individuato l'AMI corrispondente ai requisiti, annotane l'ID per utilizzarlo per avviare le istanze. Per ulteriori informazioni, consulta la pagina Avvio di un'istanza nella Guida per l'utente di AWS Command Line Interface .

Il comando describe-images supporta il filtraggio dei parametri. Ad esempio, utilizza il parametro `--owners` per visualizzare le AMI pubbliche di proprietà di Amazon.

```
aws ec2 describe-images --owners amazon
```

Puoi aggiungere il filtro seguente al comando precedente per visualizzare solo le AMI Windows.

```
--filters "Name=platform,Values=windows"
```

Puoi aggiungere il filtro seguente al comando precedente per visualizzare solo le AMI supportate da Amazon EBS:

```
--filters "Name=root-device-type,Values=ebs"
```

> **Important**
>
> Se ometti il `--owners` parametro dal `describe-images` comando, vengono restituite tutte le immagini per le quali disponi delle autorizzazioni di avvio, indipendentemente dalla proprietà.

Trova un AMI utilizzando il AWS Tools for Windows PowerShell

È possibile utilizzare i PowerShell cmdlet per elencare solo le AMI Windows che soddisfano i requisiti. Per informazioni ed esempi, consulta Find an Amazon Machine Image Using Windows PowerShell nella AWS Tools for Windows PowerShell User Guide.

Dopo aver individuato l'AMI corrispondente ai requisiti, annotane l'ID per utilizzarlo per avviare le istanze. Per ulteriori informazioni, consulta Launch an Amazon EC2 Instance Using Windows PowerShell nella Guida per l'AWS Tools for Windows PowerShell utente.

Trova un'AMI utilizzando un parametro Systems Manager

Quando avvii un'istanza utilizzando la procedura guidata di avvio dell'istanza EC2 nella console Amazon EC2, puoi selezionare un AMI dall'elenco (descritto Trova un'AMI utilizzando la console Amazon EC2 in) oppure puoi selezionare AWS Systems Manager un parametro che punti a un ID AMI (descritto in questa sezione). Se utilizzi codice di automazione per avviare le istanze, puoi specificare il parametro Systems Manager anziché l'ID AMI.

Un parametro Systems Manager è una coppia chiave-valore definita dal cliente che puoi creare nell'archivio parametri Systems Manager. Archivio parametri fornisce uno store centralizzato per esternalizzare i valori di configurazione dell'applicazione. Per ulteriori informazioni, consulta Archivio parametri AWS Systems Manager nella Guida per l'utente di AWS Systems Manager Systems Manager.

Quando crei un parametro che punta ad un ID AMI, assicurati di specificare il tipo di dati come `aws:ec2:image`. Specificare questo tipo di dati garantisce che quando il parametro viene creato o modificato, il valore del parametro viene convalidato come un ID AMI. Per ulteriori informazioni, consulta Supporto dei parametri nativi per gli ID di Amazon Machine Image (AMI) nella Guida per l'utente di AWS Systems Manager .

Argomenti

Casi d'uso

Quando si utilizzano i parametri di Systems Manager per puntare agli ID AMI, è più facile selezionare l'AMI corretta durante l'avvio delle istanze. I parametri di Systems Manager possono inoltre semplificare la manutenzione del codice di automazione.

Più facile per gli utenti

Se è richiesto che le istanze vengano avviate utilizzando un'AMI specifica e se tale AMI viene aggiornata regolarmente, si consiglia di richiedere agli utenti di selezionare un parametro Systems Manager per trovare l'AMI. Richiedendo agli utenti di selezionare un parametro Systems Manager, puoi assicurarti che l'AMI più recente venga utilizzata per avviare le istanze.

Ad esempio, ogni mese nell'organizzazione è possibile creare una nuova versione dell'AMI con le patch del sistema operativo e delle applicazioni più recenti. Puoi inoltre richiedere che gli utenti avviino istanze utilizzando l'ultima versione dell'AMI. Per assicurarti che gli utenti utilizzino la versione più recente, puoi creare un parametro Systems Manager (ad esempio, `golden-ami`) che punta all'ID AMI corretto. Ogni volta che viene creata una nuova versione dell'AMI, il valore dell'ID AMI nel parametro viene aggiornato in modo che punti sempre all'AMI più recente. Non occorre che gli utenti conoscano gli aggiornamenti periodici all'AMI, perché continuano ogni volta a selezionare lo stesso parametro Systems Manager. Utilizzando un parametro Systems Manager per l'AMI facilita la selezione dell'AMI corretta per l'avvio di un'istanza agli utenti.

Semplificazione della manutenzione del codice di automazione

Se utilizzi codice di automazione per avviare le istanze, puoi specificare il parametro Systems Manager anziché l'ID AMI. Se viene creata una nuova versione dell'AMI, è possibile modificare il valore dell'ID AMI nel parametro in modo che punti all'AMI più recente. Il codice di automazione che fa riferimento al parametro non deve essere modificato ogni volta che viene creata una nuova versione dell'AMI. Ciò semplifica la manutenzione dell'automazione e contribuisce a ridurre i costi di implementazione.

> **Note**
>
> Le istanze in esecuzione non sono interessate quando si modifica l'ID AMI a cui punta il parametro Systems Manager.

Autorizzazioni

Se utilizzi parametri di Systems Manager che puntano agli ID AMI nella procedura guidata di avvio dell'istanza, devi aggiungere le seguenti autorizzazioni alla tua policy IAM:

- `ssm:DescribeParameters`— Concede l'autorizzazione a visualizzare e selezionare i parametri di Systems Manager.
- `ssm:GetParameters`— Concede il permesso di recuperare i valori dei parametri di Systems Manager.

Puoi inoltre limitare l'accesso a parametri Systems Manager specifici. Per ulteriori informazioni ed esempi di policy IAM, vedere. Esempio: utilizzo della procedura guidata per l'avvio dell'istanza EC2

Limitazioni

AMI e parametri Systems Manager sono specifici della regione. Per utilizzare lo stesso nome di parametro Systems Manager tra regioni, crea un parametro Systems Manager in ogni ragione con lo stesso nome (ad esempio, `golden-ami`). In ogni regione, il parametro Systems Manager deve puntare a un'AMI in tale regione.

Avviare un'istanza utilizzando un parametro Systems Manager

Puoi avviare un'istanza utilizzando la console o l' AWS CLI. Invece di specificare un ID AMI, è possibile specificare un AWS Systems Manager parametro che punti a un ID AMI.

New console

Per trovare un'AMI utilizzando un parametro Systems Manager (console)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione selezionare la regione in cui avviare le istanze. È possibile selezionare qualsiasi regione disponibile, indipendentemente dalla posizione.
3. Dal pannello di controllo della console, scegliere Launch Instance (Avvia istanza).
4. In Applicazioni e immagini SO (Amazon Machine Image), scegli Sfoglia altre AMI.
5. Scegli il pulsante freccia a destra della barra delle ricerche, quindi scegli Cerca per parametro Systems Manager.
6. Per Systems Manager parameter (Parametro Systems Manager), selezionare un parametro. L'ID AMI corrispondente viene visualizzato sotto Attualmente si risolve in.
7. Selezionare Search (Cerca). Le AMI che corrispondono all'ID AMI vengono visualizzate nell'elenco.
8. Selezionare l'AMI dall'elenco e scegliere Select (Seleziona).

Per ulteriori informazioni sull'avvio di un'istanza tramite la procedura guidata di avvio dell'istanza, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Old console

Per trovare un'AMI utilizzando un parametro Systems Manager (console)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Dalla barra di navigazione selezionare la regione in cui avviare le istanze. È possibile selezionare qualsiasi regione disponibile, indipendentemente dalla posizione.
3. Dal pannello di controllo della console, scegliere Launch Instance (Avvia istanza).
4. Scegliere Search by Systems Manager parameter (Cerca per parametro Systems Manager) (in alto a destra).
5. Per Systems Manager parameter (Parametro Systems Manager), selezionare un parametro. L'ID AMI corrispondente viene visualizzato accanto a Currently resolves to (Attualmente si risolve in).
6. Selezionare Search (Cerca). Le AMI che corrispondono all'ID AMI vengono visualizzate nell'elenco.
7. Selezionare l'AMI dall'elenco e scegliere Select (Seleziona).

Per ulteriori informazioni sull'avvio di un'istanza da un'AMI tramite la procedura guidata di avvio dell'istanza, consulta Fase 1: scelta di un'Amazon Machine Image (AMI).

Per avviare un'istanza utilizzando un AWS Systems Manager parametro anziché un ID AMI (AWS CLI)

Nell'esempio seguente viene utilizzato il parametro Systems Manager `golden-ami` per avviare un'istanza `m5.xlarge`. Il parametro punta a un ID AMI.

Per specificare il parametro nel comando, utilizzare la sintassi seguente: `resolve:ssm:/`*`parameter-name`*, dove `resolve:ssm` è il prefisso standard e `parameter-name` è il nome del parametro univoco. Notare che il nome di parametro prevede la distinzione tra lettere maiuscole e minuscole. Le barre rovesciate per il nome del parametro sono necessarie solo quando il parametro fa parte di una gerarchia, ad esempi, `/amis/production/golden-ami`. È possibile omettere la barra rovesciata se il parametro non fa parte di una gerarchia.

In questo esempio, i parametri `--count` e `--security-group` non sono inclusi. Per `--count`, il valore predefinito è 1. Se disponibili, un VPC predefinito e un gruppo di sicurezza predefinito vengono utilizzati.

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami
    --instance-type m5.xlarge
    ...
```

Per avviare un'istanza utilizzando una versione specifica di un AWS Systems Manager parametro (AWS CLI)

I parametri Systems Manager dispongono del supporto della versione. A ogni iterazione di un parametro viene assegnato un numero di versione univoco. Puoi fare riferimento alla versione del parametro come indicato di seguito `resolve:ssm:parameter-name:version`, in cui `version` è il numero di versione univoco. Per impostazione predefinita, la versione più recente del parametro viene utilizzata quando non è specificata alcuna versione.

Nell'esempio seguente viene utilizzata la versione 2 del parametro.

In questo esempio, i parametri `--count` e `--security-group` non sono inclusi. Per `--count`, l'impostazione di default è 1. Se disponibili, vengono utilizzati un VPC di default e un gruppo di sicurezza di default.

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami:2
    --instance-type m5.xlarge
    ...
```

Per avviare un'istanza utilizzando un parametro pubblico fornito da AWS

Systems Manager fornisce parametri pubblici per le AMI pubbliche fornite da AWS. È possibile utilizzare i parametri pubblici all'avvio delle istanze per assicurarsi di utilizzare le AMI più recenti.

Per ulteriori informazioni, consulta Trova le AMI più recenti utilizzando Systems Manager.

Trova le AMI più recenti utilizzando Systems Manager

AWS Systems Manager fornisce parametri pubblici per le AMI pubbliche gestite da. AWS Puoi utilizzare i parametri pubblici all'avvio delle istanze per assicurarti di utilizzare le AMI più recenti. Ad esempio, il parametro public `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` è disponibile in tutte le regioni e punta sempre alla versione più recente dell'AMI Amazon Linux 2023 per l'architettura arm64 in una determinata regione.

I parametri pubblici sono disponibili nei seguenti percorsi:

- Linux – `/aws/service/ami-amazon-linux-latest`
- Windows – `/aws/service/ami-windows-latest`

Per visualizzare un elenco di tutte le AMI Linux o Windows nella regione corrente AWS

Usa il get-parameters-by-path AWS CLI comando seguente per visualizzare un elenco di tutte le AMI Linux o Windows nella regione corrente AWS . Il valore del `--path` parametro è diverso per Linux e Windows.

Per Linux:

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-amazon-linux-latest \
    --query "Parameters[].Name"
```

Per Windows:

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-windows-latest \
    --query "Parameters[].Name"
```

Per avviare un'istanza mediante un parametro pubblico

L'esempio seguente specifica un parametro pubblico di Systems Manager per l'ID dell'immagine per avviare un'istanza utilizzando l'ultima AMI Amazon Linux 2023.

Per specificare il parametro nel comando, utilizzare la sintassi seguente: `resolve:ssm:`*`public-parameter`*, dove `resolve:ssm` è il prefisso standard e *`public-parameter`* è il percorso e il nome del parametro pubblico.

In questo esempio, i parametri `--count` e `--security-group` non sono inclusi. Per `--count`, il valore predefinito è 1. Se disponibili, un VPC predefinito e un gruppo di sicurezza predefinito vengono utilizzati.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64 \
    --instance-type m5.xlarge \
    --key-name MyKeyPair
```

Per ulteriori informazioni, consulta la pagina Utilizzo dei parametri pubblici nella Guida per l'utente di AWS Systems Manager .

Per esempi che utilizzano i parametri di Systems Manager, consulta Query per gli ID AMI Amazon Linux più recenti con AWS Systems Manager Parameter Store e Query per l'ultima AMI Windows con AWS Systems Manager Parameter Store.

Ulteriori informazioni per trovare le AMI

Per trovare un'AMI Amazon Linux 2023, consulta AL2023 su Amazon EC2 nella Guida per l'utente di Amazon Linux 2023.

Per trovare un'AMI Ubuntu, consulta Amazon EC2 AMI Locator sul sito Web Canonical Ubuntu.

Per trovare un'AMI RHEL, consulta Red Hat Enterprise Linux Images (AMI) Disponibile su Amazon Web Services (AWS) sul sito Web Red Hat.

AMI condivise

Un'AMI condivisa è un'AMI creata da uno sviluppatore e resa disponibile per gli altri sviluppatori. Uno dei modi più semplici per iniziare a familiarizzare con Amazon EC2, consiste nell'utilizzare un'AMI condivisa con i componenti necessari e procedere poi all'aggiunta dei contenuti personalizzati. Puoi anche creare AMI personalizzate e condividerle con altri utenti.

Utilizza le AMI condivise a tuo rischio e pericolo. Amazon non può garantire l'integrità o la sicurezza delle AMI condivise da altri utenti Amazon EC2. Di conseguenza, ti consigliamo di trattare le AMI condivise come faresti con qualsiasi altro codice esterno che pensi di distribuire nel tuo data center con la dovuta cautela. Ti consigliamo di scaricare le AMI da un'origine attendibile, come un provider verificato.

Fornitore verificato

Nella console Amazon EC2, le AMI pubbliche di proprietà di Amazon o di un partner Amazon verificato sono contrassegnate dalla dicitura Verified provider (fornitore verificato).

Puoi anche utilizzare il AWS CLI comando describe-images per identificare le AMI pubbliche che provengono da un provider verificato. Le immagini pubbliche di Amazon o di un partner verificato hanno un proprietario con alias, `amazon` o `aws-marketplace`. Nell'output della CLI, vengono visualizzati questi valori per `ImageOwnerAlias`. Gli altri utenti non possono creare un alias per le proprie AMI. Ciò consente di cercare con facilità le AMI di Amazon o dei fornitori verificati.

Per diventare un fornitore verificato, è necessario registrarsi come venditore sul Marketplace AWS. Una volta effettuata la registrazione, è possibile inserire l'AMI nell'elenco di Marketplace AWS. Per

ulteriori informazioni, consulta Nozioni di base sui rivenditori e Prodotti basati su AMI nella Guida per i rivenditori di Marketplace AWS .

Argomenti sulle AMI condivise

- Trovare AMI condivise
- Rendere un'AMI pubblica
- Condivisione di un'AMI con organizzazioni o unità organizzative specifiche
- Condividere un'AMI con account AWS specifici
- Annulla la condivisione di un AMI con il tuo Account AWS
- Utilizzo dei segnalibri
- Linee guida per le AMI Linux condivise

Se stai cercando informazioni su altri argomenti

- Per informazioni sulla creazione di un'AMI, consulta the section called “Creazione di un'AMI Linux supportata da un instance store” othe section called “Crea un'AMI supportata da Amazon EBS”.
- Per ulteriori informazioni sulla creazione, la distribuzione e la gestione delle applicazioni in Marketplace AWS, consulta la Documentazione di Marketplace AWS.

Trovare AMI condivise

Per cercare le AMI condivise, puoi usare la console o la riga di comando di Amazon EC2.

Le AMI sono una risorsa basata sulla regione. Quindi, quando cerchi un'AMI condivisa (pubblica o privata), devi cercarla nella stessa regione da cui viene condivisa. Per rendere un'AMI disponibile in un'altra regione, copiala nella regione desiderata e condividila. Per ulteriori informazioni, consulta Copiare un'AMI.

Attività

- Ricerca di un'AMI condivisa (console)
- Cerca un'AMI condivisa (AWS CLI).
- Trova un'AMI condivisa (Strumenti per Windows PowerShell)
- Uso delle AMI condivise

Ricerca di un'AMI condivisa (console)

Per cercare un'AMI privata condivisa tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Nel primo filtro scegliere Private images (Immagini private). Vengono elencate tutte le AMI condivise con te. Per effettuare una ricerca granulare, scegliere la barra di ricerca e utilizzare le opzioni di filtro del menu.

Per cercare un'AMI pubblica condivisa tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Nel primo filtro scegliere Public images (Immagini pubbliche). Per effettuare una ricerca granulare, seleziona il campo Search (ricerca) e utilizza le opzioni di filtro del menu.

Cercare un'AMI pubblica condivisa Amazon utilizzando la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Nel primo filtro scegliere Public images (Immagini pubbliche).
4. Seleziona Search (ricerca), quindi, dalle opzioni di menu, seleziona Owner alias (alias del proprietario), quindi= e amazon per visualizzare solo immagini pubbliche di Amazon.

Cercare un'AMI pubblica condivisa di un fornitore verificato utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione seleziona AMI Catalog (catalogo AMI).
3. Scegli Community AMIs (AMI community).
4. L'etichetta Verified provider (fornitore verificato) indica le AMI provenienti da Amazon o da un partner verificato.

Cerca un'AMI condivisa (AWS CLI).

Utilizzare il comando describe-images (AWS CLI) per visualizzare un elenco delle AMI. Puoi definire l'ambito dell'elenco in base ai tipi di AMI di tuo interesse, come illustrato negli esempi seguenti.

Esempio: elencare tutte le AMI pubbliche

Il comando seguente consente di elencare tutte le AMI pubbliche, incluse quelle di tua proprietà.

```
aws ec2 describe-images --executable-users all
```

Esempio: elencare le AMI con permessi di avvio espliciti

Il comando seguente consente di elencare le AMI per le quali disponi di permessi di avvio espliciti. Questo elenco non include le AMI di tua proprietà.

```
aws ec2 describe-images --executable-users self
```

Esempio: elencare le AMI di proprietà di fornitori verificati

Il comando seguente consente di elencare le AMI di proprietà di fornitori verificati. Le AMI pubbliche di proprietà di fornitori verificati (sia Amazon che fornitori verificati) hanno un proprietario con alias, visualizzato come `amazon` o `aws-marketplace` nel campo dell'account. Ciò che consente di cercare con facilità le AMI di fornitori verificati. Gli altri utenti non possono creare un alias per le proprie AMI.

```
aws ec2 describe-images \
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

Esempio: elencare le AMI di proprietà di un account

Il comando seguente consente di elencare le AMI di proprietà dell' Account AWS specificato.

```
aws ec2 describe-images --owners 123456789012
```

Esempio: definire l'ambito delle AMI tramite un filtro

Per ridurre il numero delle AMI visualizzate, utilizza un filtro per visualizzare un elenco con soltanto i tipi di AMI desiderati. Ad esempio, utilizza il filtro seguente per visualizzare soltanto le AMI EBS-backed.

```
--filters "Name=root-device-type,Values=ebs"
```

Trova un'AMI condivisa (Strumenti per Windows PowerShell)

Usa il Get-EC2Imagecomando (Strumenti per Windows PowerShell) per elencare le AMI. Puoi definire l'ambito dell'elenco in base ai tipi di AMI di tuo interesse, come illustrato negli esempi seguenti.

Esempio: elencare tutte le AMI pubbliche

Il comando seguente consente di elencare tutte le AMI pubbliche, incluse quelle di tua proprietà.

```
PS C:\> Get-EC2Image -ExecutableUser all
```

Esempio: elencare le AMI con permessi di avvio espliciti

Il comando seguente consente di elencare le AMI per le quali disponi di permessi di avvio espliciti. Questo elenco non include le AMI di tua proprietà.

```
PS C:\> Get-EC2Image -ExecutableUser self
```

Esempio: elencare le AMI di proprietà di fornitori verificati

Il comando seguente consente di elencare le AMI di proprietà di fornitori verificati. Le AMI pubbliche di proprietà di fornitori verificati (sia Amazon che fornitori verificati) hanno un proprietario con alias, visualizzato come `amazon` o `aws-marketplace` nel campo dell'account. Ciò che consente di cercare con facilità le AMI di fornitori verificati. Gli altri utenti non possono creare un alias per le proprie AMI.

```
PS C:\> Get-EC2Image -Owner amazon aws-marketplace
```

Esempio: elencare le AMI di proprietà di un account

Il comando seguente consente di elencare le AMI di proprietà dell' Account AWS specificato.

```
PS C:\> Get-EC2Image -Owner 123456789012
```

Esempio: definire l'ambito delle AMI tramite un filtro

Per ridurre il numero delle AMI visualizzate, utilizza un filtro per visualizzare un elenco con soltanto i tipi di AMI desiderati. Ad esempio, utilizza il filtro seguente per visualizzare soltanto le AMI con supporto EBS.

```
-Filter @{ Name="root-device-type"; Values="ebs" }
```

Uso delle AMI condivise

Prima di utilizzare un'AMI condivisa, completa le fasi seguenti per verificare che non siano presenti credenziali preinstallate che consentirebbero l'accesso indesiderato di una terza parte all'istanza e che non sia stato preconfigurato l'accesso remoto che potrebbe consentire l'invio di dati sensibili a una terza parte. Controlla la documentazione della distribuzione Linux utilizzata dall'AMI per informazioni su come migliorare la sicurezza del sistema.

Per assicurarti di non perdere accidentalmente l'accesso all'istanza, ti consigliamo di avviare due sessioni SSH e di tenere la seconda sessione aperta finché non hai rimosso le credenziali che non riconosci e finché non hai verificato di poter accedere all'istanza tramite SSH.

1. Identificare e disabilitare le chiavi SSH pubbliche non autorizzate. L'unica chiave presente nel file deve essere quella utilizzata per avviare l'AMI. Il comando seguente consente di individuare i file `authorized_keys`:

   ```
   [ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
   ```

2. Disabilitare l'autenticazione basata su password per l'utente root. Aprire il file `sshd_config` e modificare la riga `PermitRootLogin` come segue:

   ```
   PermitRootLogin without-password
   ```

   In alternativa, è possibile disabilitare la funzione di accesso all'istanza come utente root:

   ```
   PermitRootLogin No
   ```

   Riavviare il servizio sshd.

3. Controllare la presenza di altri utenti in grado di accedere all'istanza. Gli utenti con privilegi superuser sono particolarmente pericolosi. Rimuovere o bloccare la password degli account sconosciuti.

4. Verificare la presenza di porte aperte inutilizzate e con in esecuzione servizi di rete in attesa di connessioni in entrata.
5. Per impedire la registrazione remota preconfigurata, elimina il file di configurazione esistente e riavviare il servizio `rsyslog`. Per esempio:

```
[ec2-user ~]$ sudo rm /etc/rsyslog.conf
[ec2-user ~]$ sudo service rsyslog restart
```

6. Verifica che tutti i processi cron siano legittimi.

Se rilevi un'AMI pubblica che ritieni rappresentare un rischio per la sicurezza, contatta il team di sicurezza AWS . Per ulteriori informazioni, visita il Centro di Sicurezza AWS.

Rendere un'AMI pubblica

Puoi rendere la tua AMI disponibile pubblicamente condividendola con tutti Account AWS.

Se desideri impedire la condivisione pubblica delle tue AMI, puoi abilitare il blocco dell'accesso pubblico per le AMI. Ciò blocca qualsiasi tentativo di rendere pubblica un'AMI, contribuendo a prevenire l'accesso non autorizzato e il potenziale uso improprio dei dati dell'AMI. Tieni presente che l'abilitazione del blocco dell'accesso pubblico non influisce sulle AMI che sono già disponibili pubblicamente, che rimarranno disponibili al pubblico.

Per consentire a solo determinati account di utilizzare l'AMI per avviare le istanze, consulta Condividere un'AMI con account AWS specifici.

Indice

Considerazioni

Considera quanto segue prima di rendere pubblica un'AMI.

- Proprietà: per rendere pubblica un'AMI, è Account AWS necessario possederla.
- Regione: le AMI sono una risorsa basata sulla regione. Quando un'AMI viene condivisa, questa sarà disponibile solo nella Regione da cui viene condivisa. Per rendere un'AMI disponibile in

un'altra regione, copiala nella regione desiderata e condividila. Per ulteriori informazioni, consulta Copiare un'AMI.

- Blocca l'accesso pubblico: per condividere pubblicamente un'AMI, il blocco dell'accesso pubblico per le AMI deve essere disabilitato in ogni Regione in cui l'AMI verrà condivisa pubblicamente. Dopo aver condiviso pubblicamente l'AMI, potrai riabilitare il blocco dell'accesso pubblico per le AMI e impedire un'ulteriore condivisione pubblica delle tue AMI.
- Alcune AMI non possono essere rese pubbliche: se l'AMI presenta una delle seguenti opzioni, non è possibile renderla pubblica (ma si può condividere l'AMI con Account AWS specifici):
  - Volumi crittografati
  - Snapshot di volumi crittografati
  - Codici di prodotto
- Evita di esporre dati sensibili: per evitare di esporre dati sensibili durante la condivisione di un'AMI, leggi le considerazioni di sicurezza in Linee guida per le AMI Linux condivise e segui le operazioni consigliate.
- Utilizzo: quando un'AMI viene condivisa, gli utenti possono soltanto avviare le istanze dall'AMI. Non possono eliminarle, condividerle o modificarle. Tuttavia, dopo l'avvio di un'istanza utilizzando l'AMI condivisa, potranno creare un'AMI dall'istanza di avvio.
- Obsolescenza automatica: per impostazione predefinita, la data di obsolescenza di tutte le AMI pubbliche è impostata a due anni dalla data di creazione dell'AMI. È possibile impostare la data di obsolescenza prima dei due anni. Per annullare la data di deprecazione o spostare la deprecazione a una data successiva, è necessario rendere privata l'AMI condividendola solo con utenti specifici. Account AWS
- Rimuovere le AMI obsolete: dopo che un'AMI pubblica raggiunge la data di obsolescenza, se non sono state lanciate nuove istanze dall'AMI per sei o più mesi, AWS rimuove la proprietà di condivisione pubblica in modo che le AMI obsolete non compaiano negli elenchi di AMI pubblici.
- Fatturazione: non ti viene addebitato alcun costo quando il tuo AMI viene utilizzato da altri Account AWS per avviare istanze. Agli account che avviano le istanze tramite l'AMI saranno addebitate solo le istanze avviate.

Condividi un'AMI con tutti gli AWS account (condividi pubblicamente)

Una volta resa pubblica, un'AMI sarà disponibile nelle AMI della community nella console, a cui si può accedere dal catalogo AMI nel riquadro di navigazione sulla sinistra della console EC2 o quando si avvia un'istanza utilizzando la console. Tieni presente che, dopo averla resa pubblica, potrebbe

essere necessario un po' di tempo prima che l'AMI venga visualizzata in Community AMIs (AMI della community).

Console

Per rendere un'AMI pubblica

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI nell'elenco e scegliere Actions (Operazioni), quindi Edit AMI permissions (Modifica autorizzazioni AMI).
4. In Disponibilità AMI, scegli Pubblica.
5. Seleziona Salvataggio delle modifiche.

AWS CLI

Ogni AMI ha una `launchPermission` proprietà che controlla chi Account AWS, oltre a quello del proprietario, può utilizzare quell'AMI per avviare le istanze. Modificando la `launchPermission` proprietà di un AMI, puoi renderlo pubblico (il che concede le autorizzazioni di avvio a tutti Account AWS) o condividerlo solo con Account AWS l'AMI specificato.

Puoi aggiungere o rimuovere gli ID account dall'elenco degli account che dispongono dei permessi di avvio per l'AMI. Per rendere un'AMI pubblica, specifica il gruppo `all`. Puoi specificare i permessi di avvio sia espliciti che pubblici.

Per rendere un'AMI pubblica

1. Utilizza il comando modify-image-attribute come riportato di seguito per aggiungere il gruppo `all` all'elenco `launchPermission` dell'AMI specificata.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{Group=all}]"
```

2. Per verificare le autorizzazioni di avvio dell'AMI, utilizza il comando describe-image-attribute.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

3. (Facoltativo) Per rendere nuovamente privata l'AMI, rimuovere il gruppo `all` dai relativi permessi di avvio. Tenere presente che il proprietario dell'AMI dispone sempre dei permessi di avvio e, di conseguenza, non è interessato da questo comando.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{Group=all}]"
```

PowerShell

Ogni AMI ha una `launchPermission` proprietà che controlla chi Account AWS, oltre a quello del proprietario, può utilizzare quell'AMI per avviare le istanze. Modificando la `launchPermission` proprietà di un AMI, puoi renderlo pubblico (il che concede le autorizzazioni di avvio a tutti Account AWS) o condividerlo solo con Account AWS l'AMI specificato.

Puoi aggiungere o rimuovere gli ID account dall'elenco degli account che dispongono dei permessi di avvio per l'AMI. Per rendere un'AMI pubblica, specifica il gruppo `all`. Puoi specificare i permessi di avvio sia espliciti che pubblici.

Per rendere un'AMI pubblica

1. Utilizza il comando Edit-EC2ImageAttribute come riportato di seguito per aggiungere il gruppo `all` all'elenco `launchPermission` dell'AMI specificata.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserGroup all
```

2. Per verificare le autorizzazioni di avvio dell'AMI, utilizza il seguente comando Get-EC2ImageAttribute.

```
PS C:\> Get-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

3. (Facoltativo) Per rendere nuovamente privata l'AMI, rimuovere il gruppo `all` dai relativi permessi di avvio. Tenere presente che il proprietario dell'AMI dispone sempre dei permessi di avvio e, di conseguenza, non è interessato da questo comando.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserGroup all
```

Blocca l'accesso pubblico alle tue AMI

Per impedire la condivisione pubblica delle AMI, è possibile abilitare il blocco dell'accesso pubblico per le AMI. Questa impostazione è abilitata a livello di account, ma è necessario abilitarla in tutti gli ambienti Regione AWS in cui si desidera impedire la condivisione pubblica delle AMI.

Quando il blocco dell'accesso pubblico è abilitato, qualsiasi tentativo di rendere pubblica un'AMI viene automaticamente bloccato. Tuttavia, se disponi già di AMI pubbliche, queste rimangono disponibili al pubblico.

Per condividere pubblicamente le AMI, devi disabilitare il blocco dell'accesso pubblico. Al termine della condivisione, è preferibile riabilitare il blocco dell'accesso pubblico per impedire la condivisione pubblica involontaria delle AMI.

È possibile limitare le autorizzazioni IAM a un utente amministratore in modo che solo lui possa abilitare o disabilitare il blocco dell'accesso pubblico per le AMI.

Indice

Impostazioni predefinite

L'impostazione Blocca l'accesso pubblico per le AMI è abilitata o disabilitata per impostazione predefinita a seconda che l'account sia nuovo o esistente e che disponga di AMI pubbliche. Nella tabella seguente vengono elencate le impostazioni predefinite:

AWS account	Blocco dell'accesso pubblico per le AMI per l'impostazione predefinita
Nuovi account	Abilitato
Account esistenti senza AMI pubbliche [1]	Abilitato

AWS account	Blocco dell'accesso pubblico per le AMI per l'impostazione predefinita
Account esistenti con una o più AMI pubbliche	Disabilitato

[1] Se il tuo account aveva una o più AMI pubbliche a partire dal 15 luglio 2023, l'opzione Blocca l'accesso pubblico alle AMI è disabilitata per impostazione predefinita per il tuo account, anche se successivamente hai reso private tutte le AMI.

Autorizzazioni IAM richieste

Per usare il blocco dell'accesso pubblico per le AMI, è necessario avere le seguenti autorizzazioni IAM:

- `EnableImageBlockPublicAccess`
- `DisableImageBlockPublicAccess`
- `GetImageBlockPublicAccessState`

Abilitazione del blocco dell'accesso pubblico per le AMI

Per impedire la condivisione pubblica delle AMI, abilita il blocco dell'accesso pubblico per le AMI a livello di account. È necessario abilitare il blocco dell'accesso pubblico per le AMI in ogni Regione AWS in cui si desidera impedire la condivisione pubblica delle AMI. Se si dispone già di AMI pubbliche, rimarranno disponibili al pubblico.

Console

Abilitazione del blocco dell'accesso pubblico per le AMI nella regione specificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, nella parte superiore della schermata, seleziona la regione in cui abilitare il blocco dell'accesso pubblico per le AMI.
3. Se il pannello di controllo non viene visualizzato, nel riquadro di navigazione scegli Pannello di controllo EC2.
4. In Attributi dell'account, scegli Protezione e sicurezza dei dati.
5. In Blocca l'accesso pubblico per le AMI, scegli Gestisci.

6. Seleziona la casella Blocca nuova condivisione pubblica quindi scegli Aggiorna.

> **Note**
>
> La configurazione di questa impostazione per l'API può richiedere fino a 10 minuti. Durante questo periodo, il valore sarà Nuova condivisione pubblica consentita. Una volta completata la configurazione dell'API, il valore cambierà automaticamente in Nuova condivisione pubblica bloccata.

AWS CLI

Per abilitare il blocco dell'accesso pubblico per le AMI

Usa il comando enable-image-block-public-access.

- Per una regione specifica

```
aws ec2 enable-image-block-public-access \
--region us-east-1 \
--image-block-public-access-state block-new-sharing
```

Output previsto

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

- Per tutte le regioni del tuo account

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 enable-image-block-public-access \
            --region $region \
```

```
            --image-block-public-access-state block-new-sharing \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Output previsto

```
Region           Public Access State
--------------   ---------------------
ap-south-1       block-new-sharing
eu-north-1       block-new-sharing
eu-west-3        block-new-sharing
...
```

> **Note**
>
> La configurazione di questa impostazione per l'API può richiedere fino a 10 minuti. Durante questo periodo, se si esegue il comando get-image-block-public-access-state, la risposta sarà. `unblocked` Quando l'API avrà completato la configurazione, la risposta sarà `block-new-sharing`.

Disabilitazione del blocco dell'accesso pubblico per le AMI

Per consentire agli utenti del tuo account di condividere pubblicamente le tue AMI, disabilita il blocco dell'accesso pubblico a livello di account. È necessario disabilitare l'accesso pubblico a blocco per le AMI in ognuna delle Regione AWS aree in cui si desidera consentire la condivisione pubblica delle AMI.

Console

Disabilitazione del blocco dell'accesso pubblico per le AMI nella Regione specificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, nella parte superiore della schermata, seleziona la Regione in cui abilitare il blocco dell'accesso pubblico per le AMI.

3. Se il pannello di controllo non viene visualizzato, nel riquadro di navigazione scegli Pannello di controllo EC2.
4. In Attributi dell'account, scegli Protezione e sicurezza dei dati.
5. In Blocca l'accesso pubblico per le AMI, scegli Gestisci.
6. Deseleziona la casella Blocca nuova condivisione pubblica quindi scegli Aggiorna.
7. Quando viene richiesta la conferma, inserisci **`confirm`** e seleziona Consenti condivisione pubblica.

> **Note**
>
> La configurazione di questa impostazione per l'API può richiedere fino a 10 minuti. Durante questo periodo, il valore sarà Nuova condivisione pubblica bloccata. Una volta completata la configurazione dell'API, il valore cambierà automaticamente in Nuova condivisione pubblica consentita.

AWS CLI

Per disabilitare l'accesso pubblico a blocchi per le AMI

Usa il comando disable-image-block-public-access.

- Per una regione specifica

```
aws ec2 disable-image-block-public-access --region us-east-1
```

Output previsto

```
{
   "ImageBlockPublicAccessState": "unblocked"
}
```

- Per tutte le regioni del tuo account

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
```

```
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 disable-image-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Output previsto

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
...
```

> **Note**
>
> La configurazione di questa impostazione per l'API può richiedere fino a 10 minuti. Durante questo periodo, se si esegue il comando get-image-block-public-access-state, la risposta sarà. `block-new-sharing` Quando l'API avrà completato la configurazione, la risposta sarà `unblocked`.

Visualizzazione dello stato di blocco dell'accesso pubblico per le AMI

Per vedere se la condivisione pubblica delle tue AMI è bloccata nel tuo account, puoi visualizzare lo stato per bloccare l'accesso pubblico alle AMI. È necessario visualizzare lo stato in ogni Regione AWS in cui desideri verificare se la condivisione pubblica delle AMI è bloccata.

Console

Visualizzazione dello stato del blocco dell'accesso pubblico per le AMI nella Regione specificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nella barra di navigazione, nella parte superiore della schermata, seleziona la Regione in cui visualizzare lo stato del blocco dell'accesso pubblico per le AMI.
3. Se il pannello di controllo non viene visualizzato, nel riquadro di navigazione scegli Pannello di controllo EC2.
4. In Attributi dell'account, scegli Protezione e sicurezza dei dati.
5. In Blocca l'accesso pubblico per le AMI, seleziona il campo Accesso pubblico. Il valore è Nuova condivisione pubblica bloccata o Nuova condivisione pubblica consentita.

AWS CLI

Per ottenere lo stato di blocco dell'accesso pubblico per le AMI

Usa il comando get-image-block-public-access-state.

- Per una regione specifica

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

Output previsto: il valore è `block-new-sharing` o `unblocked`.

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

- Per tutte le regioni del tuo account

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-image-block-public-access-state \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
```

```
done
```

Output previsto: il valore è `block-new-sharing` o `unblocked`.

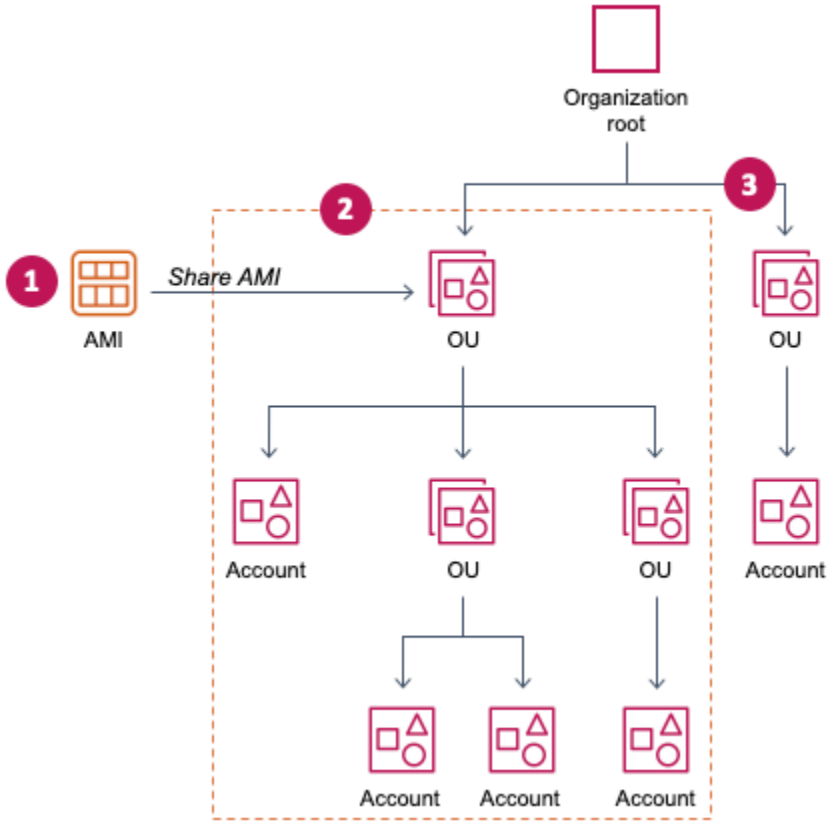
```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       unblocked
eu-west-3        block-new-sharing
...
```

Condivisione di un'AMI con organizzazioni o unità organizzative specifiche

AWS Organizationsè un servizio di gestione degli account che consente di consolidare più account Account AWS in un'organizzazione da creare e gestire centralmente. È possibile condividere un'AMI con un'organizzazione o un'unità organizzativa (UO) creata, oltre a condividerla con account specifici.

Un'organizzazione è un'entità che viene creata per consolidare e gestire centralmente i propri Account AWS. È possibile organizzare gli account in una struttura gerarchica strutturata ad albero con una radice nella parte superiore e unità organizzative sotto la radice dell'organizzazione. Ogni account può essere aggiunto direttamente alla radice o essere inserito in una delle UO nella gerarchia. Per ulteriori informazioni, consultare AWS Organizations terminology and concepts (Concetti e terminologia di AWS Organizations Organizations) nella Guida per l'utente di .

Quando un'AMI viene condivisa con un'organizzazione o un'unità organizzativa, tutti gli account figlio hanno accesso all'AMI. Ad esempio, nel diagramma seguente, l'AMI viene condivisa con un'unità organizzativa di primo livello (indicata dalla freccia sul numero 1). Anche tutte le unità organizzative e gli account nidificati sotto l'unità organizzativa di primo livello (indicata dalla linea tratteggiata sul numero 2) avranno accesso all'AMI. Gli account dell'organizzazione e dell'unità organizzativa al di fuori della linea tratteggiata (indicati dal numero 3) non avranno accesso all'AMI perché non sono figli dell'UO con cui l'AMI è condivisa.



Considerazioni

Considera le informazioni seguenti durante la condivisione delle AMI con organizzazioni o unità organizzative specifiche.

- Proprietà: per condividere un'AMI, il tuo Account AWS deve essere proprietario dell'AMI.
- Limiti di condivisione: il proprietario dell'AMI può condividere un'AMI con qualsiasi organizzazione o unità organizzativa, incluse le organizzazioni e le unità organizzative di cui non è membro.

  Per il numero massimo di entità con cui un'AMI può essere condivisa all'interno di una regione, consulta le quote di servizio di Amazon EC2.
- Tag: non puoi condividere tag definiti dall'utente (tag che colleghi a un'AMI). Quando condividi un'AMI, i tag definiti dall'utente non sono disponibili per nessuna Account AWS organizzazione o unità organizzativa con cui è condiviso l'AMI.
- Formato ARN: quando si specifica un'organizzazione o un'unità organizzativa in un comando, assicurarsi di utilizzare il formato ARN corretto. Se si specifica solo l'ID, ad esempio se si specifica solo `o-123example` o `ou-1234-5example`, viene restituito un errore.

Formati ARN corretti:

- ARN dell'organizzazione: `arn:aws:organizations::account-id:organization/organization-id`
- ARN dell'unità organizzativa: `arn:aws:organizations::account-id:ou/organization-id/ou-id`

Dove:

- *`account-id`* è il numero dell'account di gestione a 12 cifre, ad esempio, `123456789012`. Se non si conosce il numero dell'account di gestione, è possibile descrivere l'organizzazione o l'unità organizzativa in modo da ottenere l'ARN, che include il numero dell'account di gestione. Per ulteriori informazioni, consulta Ottenimento dell'ARN.
- *`organization-id`* è l'ID dell'organizzazione, ad esempio, `o-123example`.
- *`ou-id`* è l'ID dell'unità organizzativa, ad esempio, `ou-1234-5example`.

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Names (ARNs) nella IAM User Guide.

- Crittografia e chiavi: puoi condividere le AMI supportate da snapshot non crittografati e crittografati.
  - Gli snapshot crittografati devono essere crittografati con una chiave gestita dal cliente. Non puoi condividere AMI supportate da istantanee crittografate con la chiave gestita predefinita. AWS
  - Se condividi un'AMI supportata da istantanee crittografate, devi consentire alle organizzazioni o alle unità organizzative di utilizzare le chiavi gestite dal cliente utilizzate per crittografare le istantanee. Per ulteriori informazioni, consulta Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS.
- Regione: le AMI sono una risorsa basata sulla regione. Quando un'AMI viene condivisa, questa sarà disponibile solo nella Regione da cui viene condivisa. Per rendere un'AMI disponibile in un'altra regione, copiala nella regione desiderata e condividila. Per ulteriori informazioni, consulta Copiare un'AMI.
- Utilizzo: quando un'AMI viene condivisa, gli utenti possono soltanto avviare le istanze dall'AMI. Non possono eliminarle, condividerle o modificarle. Tuttavia, dopo l'avvio di un'istanza utilizzando l'AMI condivisa, potranno creare un'AMI dall'istanza di avvio.
- Fatturazione: non ti viene addebitato alcun costo quando il tuo AMI viene utilizzato da altri Account AWS per avviare istanze. Agli account che avviano le istanze tramite l'AMI saranno addebitate solo le istanze avviate.

Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS

Se condividi un'AMI supportata da istantanee crittografate, devi inoltre consentire alle organizzazioni o alle unità organizzative di utilizzare AWS KMS keys quelle utilizzate per crittografare le istantanee.

Utilizzate le `aws:PrincipalOrgPaths` chiavi `aws:PrincipalOrgID` and per confrontare il AWS Organizations percorso del principale che effettua la richiesta con il percorso indicato nella policy. Tale principale può essere un utente, un ruolo IAM, un utente federato o un utente Account AWS root. In una policy, questa chiave di condizione garantisce che il richiedente sia un membro dell'account all'interno della root dell'organizzazione specificata o delle unità organizzative (UO) in AWS Organizations. Per altri esempi di istruzioni delle condizioni, consulta aws:PrincipalOrgID e aws:PrincipalOrgPaths nella Guida per l'utente di IAM.

Per informazioni sulla modifica di una politica chiave, consulta Consentire agli utenti di altri account di utilizzare una chiave KMS nella Guida per gli AWS Key Management Service sviluppatori.

Per concedere a un'organizzazione o un'unità organizzativa l'autorizzazione a utilizzare una chiave KMS, aggiungere la seguente istruzione alla policy di chiavi.

```
{
    "Sid": "Allow access for organization root",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "kms:Describe*",
        "kms:List*",
        "kms:Get*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-123example"
        }
    }
}
```

Per condividere una chiave KMS con più unità organizzative, è possibile utilizzare una policy simile a quella riportata nell'esempio seguente.

```
{
        "Sid": "Allow access for specific OUs and their descendants",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "kms:Describe*",
            "kms:List*",
            "kms:Get*",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "o-123example"
            },
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-123example/r-ab12/ou-ab12-33333333/*",
                    "o-123example/r-ab12/ou-ab12-22222222/*"
                ]
            }
        }
}
```

Condivisione di un'AMI

Puoi utilizzare la console Amazon EC2 o AWS CLI condividere un'AMI con un'organizzazione o un'unità organizzativa.

Condivisione di un'AMI (console)

Come condividere un'AMI con un'organizzazione o una unità organizzativa tramite console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI nell'elenco e scegli Actions (Operazioni), quindi Edit AMI permissions (Modifica autorizzazioni AMI).
4. In AMI availability (Disponibilità AMI), scegliere Private (Privato).

5. Accanto a Shared organizations/OUs (Organizzazioni condivise/OUS), scegliere Add organization/OU ARN (Aggiungi ARN organizzazione/OU).
6. Per Organization/OU ARN (Organizzazione/OU ARN), inserire l'ARN o l'ARN OU dell'organizzazione con cui condividere l'AMI, quindi scegliere Share AMI (Condivisione di AMI). È necessario specificare l'ARN completo, non solo l'ID.

   Per condividere questa AMI con più utenti, ripetere questa fase fino a quando non sono stati aggiungere tutte le organizzazioni o unità organizzative (OU) desiderate.

   > **Note**
   >
   > Per condividere l'AMI, non è necessario condividere gli snapshot Amazon EBS a cui l'AMI fa riferimento. Occorre condividere soltanto l'AMI; il sistema fornisce automaticamente all'istanza l'accesso agli snapshot Amazon EBS a cui viene fatto riferimento per l'avvio. Tuttavia, è necessario condividere le chiavi KMS utilizzate per crittografare le istantanee a cui fa riferimento l'AMI. Per ulteriori informazioni, consulta Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS.
7. Al termine, scegli Save changes (Salva modifiche).
8. (Facoltativo) per visualizzare le organizzazioni o le unità organizzative con le quali è stata condivisa l'AMI, selezionare l'AMI nell'elenco, scegliere la scheda Permissions (Autorizzazioni) e scorrere verso il basso fino a Shared organizations/OUs (Organizzazioni condivise/OU). Per cercare le AMI che altri hanno condiviso con te, consulta Trovare AMI condivise.

Condivisione di un'AMI (Strumenti per Windows PowerShell)

Utilizzate il Edit-EC2ImageAttributecomando (Strumenti per Windows PowerShell) per condividere un'AMI, come illustrato negli esempi seguenti.

Come condividere un'AMI con un'organizzazione o una unità organizzativa

Il comando seguente concede all'organizzazione specificata le autorizzazioni di avvio per l'AMI selezionata.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType add -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

> **Note**
>
> Per condividere l'AMI, non è necessario condividere gli snapshot Amazon EBS a cui l'AMI fa riferimento. Occorre condividere soltanto l'AMI; il sistema fornisce automaticamente all'istanza l'accesso agli snapshot Amazon EBS a cui viene fatto riferimento per l'avvio. Tuttavia, è necessario condividere le chiavi KMS utilizzate per crittografare snapshot a cui l'AMI fa riferimento. Per ulteriori informazioni, consulta Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS.

Come interrompere la condivisione di un'AMI con un'organizzazione o una unità organizzativa

Il comando seguente rimuove le autorizzazioni di avvio per l'AMI specificata dall'organizzazione specificata:

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType remove -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

Per interrompere la condivisione di un'AMI con tutte le organizzazioni, le unità organizzative e Account AWS

Il comando seguente consente di rimuovere dall'AMI specificata tutte le autorizzazioni di avvio esplicite e pubbliche. Considera che il proprietario dell'AMI dispone sempre delle autorizzazioni di avvio e, di conseguenza, questo comando non ha alcun effetto su di lui.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Condividere un'AMI (AWS CLI)

Usa il comando modify-image-attribute (AWS CLI) per condividere un'AMI.

Per condividere un'AMI con un'organizzazione utilizzando AWS CLI

Il comando modify-image-attribute concede all'organizzazione specificata le autorizzazioni di avvio per l'AMI selezionata. È necessario specificare l'ARN completo, non solo l'ID.

```
aws ec2 modify-image-attribute \
```

```
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Per condividere un'AMI con un'unità organizzativa utilizzando AWS CLI

Il modify-image-attributecomando concede le autorizzazioni di avvio per l'AMI specificato all'unità organizzativa specificata. È necessario specificare l'ARN completo, non solo l'ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/
ou-1234-5example}]"
```

> **Note**
>
> Per condividere l'AMI, non è necessario condividere gli snapshot Amazon EBS a cui l'AMI fa riferimento. Occorre condividere soltanto l'AMI; il sistema fornisce automaticamente all'istanza l'accesso agli snapshot Amazon EBS a cui viene fatto riferimento per l'avvio. Tuttavia, è necessario condividere le chiavi KMS utilizzate per crittografare snapshot a cui l'AMI fa riferimento. Per ulteriori informazioni, consulta Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS.

Interruzione della condivisione di un'AMI

Puoi utilizzare la console Amazon EC2 o interrompere la condivisione AWS CLI di un'AMI con un'organizzazione o un'unità organizzativa.

Interruzione della condivisione di un'AMI (console)

Come condividere un'AMI con un'organizzazione o una unità organizzativa tramite console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Selezionare l'AMI nell'elenco e scegli Actions (Operazioni), quindi Edit AMI permissions (Modifica autorizzazioni AMI).

4. In Shared organizations/OUs (Organizzazioni condivise/OUs), selezionare le organizzazioni o le unità organizzative con cui si desideri interrompere la condivisione dell'AMI, quindi scegliere Remove selected (Rimuovi selezionati).
5. Al termine, scegli Save changes (Salva modifiche).
6. (Facoltativo) per confermare l'interruzione della condivisione dell'AMI con le organizzazioni o le unità organizzative, selezionare l'AMI nell'elenco, scegliere la scheda Permissions (Autorizzazioni) e scorrere verso il basso fino a Shared organizations/OUs (Organizzazioni condivise/OU).

Interruzione della condivisione di un'AMI (AWS CLI)

Usa i reset-image-attributecomandi modify-image-attributeo (AWS CLI) per interrompere la condivisione di un AMI.

Per interrompere la condivisione di un AMI con un'organizzazione o un'unità organizzativa utilizzando AWS CLI

Il modify-image-attributecomando rimuove le autorizzazioni di avvio per l'AMI specificato dall'organizzazione specificata. È necessario specificare l'ARN.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Per interrompere la condivisione di un'AMI con tutte le organizzazioni, le unità organizzative e l' Account AWS utilizzo di AWS CLI

Il comando reset-image-attribute consente di rimuovere dall'AMI specificata tutte le autorizzazioni di avvio esplicite e pubbliche. Considera che il proprietario dell'AMI dispone sempre delle autorizzazioni di avvio e, di conseguenza, questo comando non ha alcun effetto su di lui.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

> **Note**
>
> Non è possibile interrompere la condivisione di un'AMI con un account specifico se si trova in un'organizzazione o in una unità organizzativa con cui è condivisa un'AMI. Se si prova a interrompere la condivisione dell'AMI rimuovendo le autorizzazioni di avvio per l'account, Amazon EC2 restituirà un messaggio di riuscita dell'operazione. Tuttavia, l'AMI continuerà a essere condivisa con l'account.

Visualizzazione delle organizzazioni e delle unità organizzative con cui è condivisa un'AMI

Puoi utilizzare la console Amazon EC2 o la AWS CLI per verificare con quali organizzazioni e unità organizzative hai condiviso la tua AMI.

Visualizzazione delle organizzazioni e delle unità organizzative con cui è condivisa un'AMI (console)

Per verificare con quali organizzazioni e unità organizzative l'AMI è stata condivisa tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Selezionare l'AMI dall'elenco, scegliere la scheda Permissions (Autorizzazioni) e scorrere verso il basso fino a Shared organizations/OUs (Organizzazioni condivise/OU).

   Per cercare le AMI che altri hanno condiviso con te, consulta Trovare AMI condivise.

Visualizzazione delle organizzazioni e delle unità organizzative con cui è condivisa un'AMI (AWS CLI)

Puoi verificare con quali organizzazioni e unità organizzative l'AMI è stata condivisa utilizzando il comando describe-image-attribute (AWS CLI) e l'attributo `launchPermission`.

Per verificare con quali organizzazioni e unità organizzative hai condiviso la tua AMI utilizzando AWS CLI

Il comando describe-image-attribute descrive l'attributo `launchPermission` per l'AMI specificata e restituisce le organizzazioni e le unità organizzative l'AMI è stata condivisa.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
```

```
    --attribute launchPermission
```

Example response

```
{
    "ImageId": "ami-0abcdef1234567890",
    "LaunchPermissions": [
        {
            "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/
o-123example/ou-1234-5example"
        }
    ]
}
```

Ottenimento dell'ARN

Gli ARN delle organizzazioni e delle unità organizzative contengono il numero di account di gestione a 12 cifre. Se non si conosce il numero dell'account di gestione, è possibile descrivere l'organizzazione e l'unità organizzativa in modo da ottenere l'ARN. Negli esempi seguenti,`123456789012` è il numero dell'account di gestione.

Prima di poter ottenere gli ARN, occorre possedere l'autorizzazione per descrivere le organizzazioni e le unità organizzative. La seguente policy fornisce l'autorizzazione necessaria.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

Come ottenere l'ARN di un'organizzazione

Utilizza il comando describe-organization e il parametro `--query` impostato su `'Organization.Arn'` per restituire solo l'ARN dell'organizzazione.

```
aws organizations describe-organization --query 'Organization.Arn'
```

Example response

```
"arn:aws:organizations::123456789012:organization/o-123example"
```

Come ottenere l'ARN di una unità organizzativa

Utilizza il comando describe-organizational-unit, specifica l'ID UO e imposta il parametro `--query` su `'OrganizationalUnit.Arn'` per restituire solo l'ARN dell'unità organizzativa.

```
aws organizations describe-organizational-unit --organizational-unit-
id ou-1234-5example --query 'OrganizationalUnit.Arn'
```

Example response

```
"arn:aws:organizations::123456789012:ou/o-123example/ou-1234-5example"
```

Condividere un'AMI con account AWS specifici

È possibile condividere un'AMI con specifici utenti Account AWS senza renderla pubblica. Tutto ciò di cui hai bisogno sono gli Account AWS ID.

Un Account AWS ID è un numero di 12 cifre, ad esempio`012345678901`, che identifica in modo univoco un. Account AWS Per ulteriori informazioni, consulta la sezione Visualizzazione degli identificatori di Account AWS nella Guida di riferimento di AWS Account Management .

Considerazioni

Tieni presente quanto segue quando condividi AMI con utenti specifici. Account AWS

- Proprietà: per condividere un'AMI, il tuo Account AWS deve essere proprietario dell'AMI.
- Limiti di condivisione: per il numero massimo di entità con cui un'AMI può essere condivisa all'interno di una regione, consulta le quote di servizio di Amazon EC2.
- Tag: non puoi condividere tag definiti dall'utente (tag che colleghi a un'AMI). Quando condividi un'AMI, i tag definiti dall'utente non sono disponibili per nessuno con Account AWS cui l'AMI è condiviso.

- Crittografia e chiavi: puoi condividere le AMI supportate da snapshot non crittografati e crittografati.
  - Gli snapshot crittografati devono essere crittografati con una chiave KMS. Non è possibile condividere AMI supportate da snapshot crittografati con la chiave gestita da AWS di default.
  - Se condividi un'AMI supportata da istantanee crittografate, devi consentire loro di Account AWS utilizzare le chiavi KMS utilizzate per crittografare le istantanee. Per ulteriori informazioni, consultare Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS. Per configurare la policy chiave necessaria per avviare le istanze di Auto Scaling quando utilizzi una chiave gestita dal cliente per la crittografia, consulta la sezione AWS KMS key Politica richiesta per l'uso con volumi crittografati nella Guida per l'utente di Amazon EC2 Auto Scaling.
- Regione: le AMI sono una risorsa basata sulla regione. Quando un'AMI viene condivisa, questa sarà disponibile solo in quella Regione. Per rendere un'AMI disponibile in un'altra regione, copiala nella regione desiderata e condividila. Per ulteriori informazioni, consulta Copiare un'AMI.
- Utilizzo: quando un'AMI viene condivisa, gli utenti possono soltanto avviare le istanze dall'AMI. Non possono eliminarle, condividerle o modificarle. Tuttavia, dopo aver avviato un'istanza utilizzando l'AMI condivisa, potranno creare un'AMI dalla loro istanza.
- Copiare AMI condivise: Se gli utenti di un altro account vogliono copiare un'AMI condivisa, è necessario concedere loro le autorizzazioni di lettura per lo archiviazione che supporta l'AMI. Per ulteriori informazioni, consulta Copia tra account.
- Fatturazione: non ti viene addebitato alcun costo quando il tuo AMI viene utilizzato da altri Account AWS per avviare istanze. Agli account che avviano le istanze tramite l'AMI saranno addebitate solo le istanze avviate.

Condivisione di un'AMI (console)

Per concedere permessi di avvio espliciti tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Selezionare l'AMI nell'elenco e scegli Actions (Operazioni), quindi Edit AMI permissions (Modifica autorizzazioni AMI).
4. Scegli Private (Privato).
5. In Shared accounts (Account condivisi), scegliere Add account ID (Aggiungi ID account).
6. Per Account AWS ID, inserisci l' Account AWS ID con cui desideri condividere l'AMI, quindi scegli Condividi AMI.

Per condividere questa AMI con più account, ripetere le fasi 5 e 6 fino a quando sono stati aggiunti tutti gli account richiesti.

> **Note**
>
> Per condividere l'AMI, non serve condividere gli snapshot Amazon EBS a cui l'AMI fa riferimento. Occorre condividere soltanto l'AMI; il sistema fornisce automaticamente all'istanza l'accesso agli snapshot Amazon EBS a cui viene fatto riferimento per l'avvio. Tuttavia, è necessario condividere eventuali Chiavi KMS utilizzate per crittografare snapshot a cui l'AMI fa riferimento. Per ulteriori informazioni, consulta Share an Amazon EBS snapshot nella Amazon EBS User Guide.

7. Al termine, scegliere Save changes (Salva modifiche).
8. (Facoltativo) Per visualizzare gli Account AWS ID con cui hai condiviso l'AMI, seleziona l'AMI nell'elenco e scegli la scheda Autorizzazioni. Per cercare le AMI che altri hanno condiviso con te, consulta Trovare AMI condivise.

Condivisione di un'AMI (Strumenti per Windows PowerShell)

Utilizzate il Edit-EC2ImageAttributecomando (Strumenti per Windows PowerShell) per condividere un'AMI, come illustrato negli esempi seguenti.

Per concedere i permessi di avvio espliciti

Il comando seguente concede all' Account AWS specificato le autorizzazioni di avvio per l'AMI specificata. Nell'esempio seguente, sostituisci l'ID AMI di esempio con un ID AMI valido e sostituiscilo *account-id* con l'ID a 12 cifre Account AWS .

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserId "account-id"
```

> **Note**
>
> Per condividere l'AMI, non serve condividere gli snapshot Amazon EBS a cui l'AMI fa riferimento. Occorre condividere soltanto l'AMI; il sistema fornisce automaticamente all'istanza l'accesso agli snapshot Amazon EBS a cui viene fatto riferimento per l'avvio. Tuttavia, è necessario condividere eventuali Chiavi KMS utilizzate per crittografare snapshot

a cui l'AMI fa riferimento. Per ulteriori informazioni, consulta Share an Amazon EBS snapshot nella Amazon EBS User Guide.

Per rimuovere i permessi di avvio da un account

Il comando seguente consente di rimuovere dall' Account AWS specificato le autorizzazioni di avvio per l'AMI specificata. Nell'esempio seguente, sostituisci l'ID AMI di esempio con un ID AMI valido e sostituiscilo *account-id* con l'ID a 12 cifre Account AWS .

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserId "account-id"
```

Per rimuovere tutte le autorizzazioni di avvio

Il comando seguente consente di rimuovere tutti i permessi di avvio espliciti e pubblici dall'AMI specificata. Considera che il proprietario dell'AMI dispone sempre delle autorizzazioni di avvio e, di conseguenza, questo comando non ha alcun effetto su di lui. Nell'esempio seguente, sostituisci l'ID AMI di esempio con un ID AMI valido.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Condividere un'AMI (AWS CLI)

Utilizza il comando modify-image-attribute (AWS CLI) per condividere un'AMI come illustrato negli esempi seguenti.

Per concedere i permessi di avvio espliciti

Il comando seguente concede all' Account AWS specificato le autorizzazioni di avvio per l'AMI specificata. Nell'esempio seguente, sostituisci l'ID AMI di esempio con un ID AMI valido e sostituiscilo *account-id* con l'ID a 12 cifre Account AWS .

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{UserId=account-id}]"
```

> **Note**
>
> Per condividere l'AMI, non serve condividere gli snapshot Amazon EBS a cui l'AMI fa riferimento. Occorre condividere soltanto l'AMI; il sistema fornisce automaticamente all'istanza l'accesso agli snapshot Amazon EBS a cui viene fatto riferimento per l'avvio. Tuttavia, è necessario condividere eventuali Chiavi KMS utilizzate per crittografare snapshot a cui l'AMI fa riferimento. Per ulteriori informazioni, consulta Share an Amazon EBS snapshot nella Amazon EBS User Guide.

Per rimuovere i permessi di avvio da un account

Il comando seguente consente di rimuovere dall' Account AWS specificato le autorizzazioni di avvio per l'AMI specificata. Nell'esempio seguente, sostituisci l'ID AMI di esempio con un ID AMI valido e sostituiscilo *account-id* con l'ID a 12 cifre Account AWS .

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{UserId=account-id}]"
```

Per rimuovere tutte le autorizzazioni di avvio

Il comando seguente consente di rimuovere tutti i permessi di avvio espliciti e pubblici dall'AMI specificata. Considera che il proprietario dell'AMI dispone sempre delle autorizzazioni di avvio e, di conseguenza, questo comando non ha alcun effetto su di lui. Nell'esempio seguente, sostituisci l'ID AMI di esempio con un ID AMI valido.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Annulla la condivisione di un AMI con il tuo Account AWS

Un'Amazon Machine Image (AMI) può essere condivisa con Account AWS specifici aggiungendo gli account alle sue autorizzazioni di avvio. Se un'AMI è stata condivisa con il tuo Account AWS e non desideri più che venga condivisa con il tuo account, puoi rimuovere il tuo account dalle autorizzazioni di avvio dell'AMI. Puoi farlo eseguendo il `cancel-image-launch-permission` AWS CLI comando. Quando si esegue questo comando, le Account AWS autorizzazioni di avvio per l'AMI specificata vengono rimosse.

Potresti annullare la condivisione di un'AMI con il tuo account, ad esempio, per ridurre la probabilità di avviare un'istanza con un'AMI inutilizzata o obsoleta che è stata condivisa con te. Quando annulli la condivisione di un'AMI con il tuo account, questa non viene più visualizzata in nessun elenco di AMI della console EC2 o nell'output per describe-images.

Argomenti

Limitazioni

- Puoi rimuovere il tuo account dalle autorizzazioni di avvio di un'AMI condivisa Account AWS solo con te. Non puoi utilizzare `cancel-image-launch-permission` per rimuovere il tuo account dalle autorizzazioni di avvio di un'AMI condivisa con un'organizzazione o un'unità organizzativa (UO) o per rimuovere l'accesso alle AMI pubbliche.
- Non è possibile rimuovere definitivamente il tuo account dalle autorizzazioni di avvio di un'AMI. Il proprietario di un'AMI può condividerla nuovamente con il tuo account.
- Le AMI sono una risorsa basata sulla regione. Durante l'esecuzione di `cancel-image-launch-permission`, devi specificare la regione in cui si trova l'AMI. Specifica la regione nel comando oppure utilizza la variabile d'ambiente AWS_DEFAULT_REGION.
- Solo gli SDK AWS CLI e supportano la rimozione del tuo account dalle autorizzazioni di avvio di un'AMI. Al momento la console EC2 non supporta questa operazione.

Annullamento della condivisione di un'AMI con il tuo account

> **Note**
>
> L'annullamento della condivisione di un'AMI con il tuo account non è un'operazione annullabile. Per ottenere nuovamente l'accesso all'AMI, il proprietario dell'AMI dovrà condividerla con il tuo account.

AWS CLI

Per annullare la condivisione di un AMI con Account AWS

Utilizza il comando cancel-image-launch-permission e specifica l'ID dell'AMI.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0123456789example \
    --region us-east-1
```

Output previsto

```
{
    "Return": true
}
```

PowerShell

Per annullare la condivisione di un AMI con te Account AWS utilizzando il AWS Tools for PowerShell

Utilizza il comando Stop-EC2ImageLaunchPermission e specifica l'ID dell'AMI.

```
Stop-EC2ImageLaunchPermission `
    -ImageId ami-0123456789example `
    -Region us-east-1
```

Output previsto

```
True
```

Ricerca delle AMI condivise con un account

Per trovare le AMI condivise con le tue Account AWS, consultaTrovare AMI condivise.

Utilizzo dei segnalibri

Se hai creato un'AMI pubblica o l'hai condivisa con un'altra Account AWS, puoi creare un segnalibro che consenta a un utente di accedere all'AMI e avviare immediatamente un'istanza nel proprio account. È un modo semplice per condividere i riferimenti dell'AMI; in questo modo gli utenti non dovranno impiegare del tempo a cercare la tua AMI per utilizzarla.

Tieni presente che la tua AMI deve essere pubblica o che devi averla condivisa con l'utente al quale desideri inviare il segnalibro.

Per creare un segnalibro per la tua AMI

1. Digitare un URL con le informazioni seguenti, dove region è la regione in cui risiede l'AMI:

   ```
   https://console.aws.amazon.com/ec2/v2/home?
   region=region#LaunchInstanceWizard:ami=ami_id
   ```

   Ad esempio, questo URL avvia un'istanza dall'AMI ami-0abcdef1234567890 AMI nella regione `us-east-1` Stati Uniti orientali (Virginia settentrionale):

   ```
   https://console.aws.amazon.com/ec2/v2/home?region=us-
   east-1#LaunchInstanceWizard:ami=ami-0abcdef1234567890
   ```

2. Condividere il collegamento con gli utenti che desiderano utilizzare l'AMI.
3. Per utilizzare un segnalibro, selezionare il collegamento o copiarlo e incollarlo nel browser. Si aprirà la procedura guidata di avvio con l'AMI già selezionata.

Linee guida per le AMI Linux condivise

Utilizza le linee guida seguenti per ridurre la superficie di attacco e migliorare l'affidabilità delle AMI create.

> **Important**
>
> Nessun elenco delle linee guida di sicurezza può essere esaustivo. Crea le tue AMI condivise con attenzione considerando in quale posizione potresti esporre dati sensibili.

Indice

Se stai creando AMI per Marketplace AWS, consulta le migliori pratiche per la creazione di AMI nella Guida per il Marketplace AWS venditore per le linee guida, le politiche e le migliori pratiche.

Per ulteriori informazioni sulla condivisione sicura delle AMI, consulta gli articoli seguenti:

- Articolo relativo alla condivisione e all'utilizzo sicuri delle AMI pubbliche
- Articolo relativo ai requisiti di pulizia e ai controlli di base per la pubblicazione delle AMI pubbliche

Aggiornare gli Strumenti AMI prima di usarli

Per le AMI supportate da instance store, ti consigliamo di scaricare e aggiornare gli strumenti di creazione delle AMI Amazon EC2 prima di usarli. In questo modo, le nuove AMI basate sulle AMI condivise disporranno degli strumenti AMI più recenti.

Per Amazon Linux 2, installare il pacchetto `aws-amitools-ec2` e aggiungere gli strumenti AMI al PATH con il seguente comando. Per Amazon Linux AMI, `aws-amitools-ec2` il pacchetto è già stato installato per impostazione predefinita.

```
[ec2-user ~]$ sudo yum install -y aws-amitools-ec2 && export PATH=$PATH:/opt/aws/bin
 > /etc/profile.d/aws-amitools-ec2.sh && . /etc/profile.d/aws-amitools-ec2.sh
```

Aggiorna gli strumenti AMI con il comando seguente:

```
[ec2-user ~]$ sudo yum upgrade -y aws-amitools-ec2
```

Per altre distribuzioni, assicurati di disporre degli strumenti AMI più recenti.

Disabilitazione degli accessi remoti basati su password per l'utente root

L'uso di una password root fissa per le AMI pubbliche rappresenta un rischio per la sicurezza che può diventare noto rapidamente. Anche fare affidamento sul fatto che gli utenti modifichino la password dopo il primo accesso lascia aperta una piccola possibilità di potenziali usi illeciti.

Per risolvere questo problema, disabilita gli accessi remoti basati su password per l'utente root.

Per disabilitare gli accessi remoti basati su password per l'utente root

1. Aprire il file `/etc/ssh/sshd_config` con un editor di testo e individuare la riga seguente:

```
#PermitRootLogin yes
```

2. Modificare la riga in:

```
PermitRootLogin without-password
```

Il percorso di questo file di configurazione potrebbe essere diverso a seconda della distribuzione o se OpenSSH non è in esecuzione. In questo caso, consultare la relativa documentazione.

Disabilitazione dell'accesso root locale

Quando utilizzi AMI condivise, ti consigliamo, come best practice, di disabilitare gli accessi root diretti. Per farlo, accedi all'istanza in esecuzione ed esegui il comando seguente:

```
[ec2-user ~]$ sudo passwd -l root
```

> **Note**
>
> Questo comando non ha alcun impatto sull'uso di `sudo`.

Rimozione delle coppie di chiavi dell'host SSH

Se intendi condividere un'AMI derivata da un'AMI pubblica, rimuovi le coppie di chiavi dell'host SSH esistenti posizionate in `/etc/ssh`. Ciò costringe SSH a generare nuove coppie di chiavi SSH uniche quando qualcuno avvia un'istanza utilizzando la tua AMI, migliorando la sicurezza e riducendo la probabilità di attacchi "». man-in-the-middle

Rimuovi tutti i file di chiave seguenti presenti sul sistema.

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key

- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

Puoi rimuovere in sicurezza tutti questi file con il comando seguente.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

> **Warning**
>
> Le utilità di eliminazione sicura, come **`shred`**, potrebbero non rimuovere tutte le copie di un file dai supporti di archiviazione. I file system di journaling (tra cui il file system ext4 predefinito di Amazon Linux), snapshot, backup, RAID e la cache temporanea potrebbero creare delle copie nascoste dei file. Per ulteriori informazioni, consulta la documentazione di **`shred`**.

> **Important**
>
> Se dimentichi di rimuovere le coppie di chiavi dell'host SSH esistenti dall'AMI pubblica, il nostro processo di controllo di routine invia una notifica a te e a tutti gli utenti che eseguono le istanze della tua AMI informandovi del potenziale rischio per la sicurezza. Dopo un breve periodo di tolleranza, contrassegneremo l'AMI come privata.

Installazione delle credenziali di chiave pubblica

Dopo aver configurato l'AMI per impedire l'accesso tramite password, devi assicurarti che gli utenti possano accedervi mediante un altro meccanismo.

Amazon EC2 consente agli utenti di specificare un nome di coppia di chiavi pubblica-privata al momento dell'avvio dell'istanza. Se viene specificato un nome della coppia di chiavi valido alla chiamata API `RunInstances` (o tramite gli strumenti API della riga di comando), la chiave pubblica (la porzione della coppia di chiavi che Amazon EC2 conserva sul server in seguito alla chiamata a

`CreateKeyPair` o a `ImportKeyPair`) viene resa disponibile per l'istanza tramite una query HTTP sui metadati dell'istanza.

Per accedere tramite SSH, l'AMI deve recuperare il valore di chiave al momento dell'avvio e aggiungerlo a `/root/.ssh/authorized_keys` (o all'equivalente per gli altri account utente sull'AMI). Gli utenti possono avviare le istanze dell'AMI con una coppia di chiavi e accedere senza bisogno di una password root.

Molte distribuzioni, tra cui Amazon Linux e Ubuntu, utilizzano il pacchetto `cloud-init` per inserire le credenziali di chiave pubblica per un utente configurato. Se la distribuzione in uso non supporta `cloud-init`, puoi aggiungere il codice seguente a uno script di avvio del sistema (come `/etc/rc.local`) per inserire la chiave pubblica specificata al momento dell'avvio per l'utente root.

> **Note**
>
> Nell'esempio seguente, l'indirizzo IP http://169.254.169.254/ è un indirizzo locale del collegamento ed è valido solo dall'istanza.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
```

```
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

Questa procedura è applicabile a tutti gli utenti e non è necessario limitarla all'utente `root`.

> **Note**
>
> Il nuovo raggruppamento di un'istanza basata su tale AMI include la chiave con la quale è stata avviata. Per impedire l'inclusione della chiave, è necessario eliminare il file `authorized_keys` o escluderlo dal nuovo raggruppamento.

Disabilita i controlli DNS sshd (opzionale)

La disabilitazione dei controlli DNS sshd indebolisce leggermente la sicurezza sshd. Tuttavia, in caso di errori della risoluzione DNS, gli accessi SSH continueranno a funzionare. Se non disabiliti i controlli sshd, gli errori della risoluzione DNS impediranno tutti gli accessi.

Per disabilitare i controlli DNS sshd

1. Aprire il file `/etc/ssh/sshd_config` con un editor di testo e individuare la riga seguente:

   ```
   #UseDNS yes
   ```

2. Modificare la riga in:

   ```
   UseDNS no
   ```

> **Note**
>
> Il percorso di questo file di configurazione può essere diverso a seconda della distribuzione o se OpenSSH non è in esecuzione. In questo caso, consultare la relativa documentazione.

Protezione dell'utente

Ti sconsigliamo di archiviare dati sensibili o software sulle AMI che condividi. Gli utenti che avviano un'AMI condivisa potrebbero ricompilarla e registrarla come di loro proprietà. Segui queste linee guida per evitare rischi della sicurezza spesso sottovalutati:

- Ti consigliamo di utilizzare l'opzione `--exclude` *`directory`* su `ec2-bundle-vol` per saltare le directory e le sottodirectory contenenti informazioni segrete che non desideri includere nel bundle. In particolare, escludi tutte le coppie di chiavi SSH pubbliche/private di proprietà dell'utente e i file `authorized_keys` SSH durante il raggruppamento dell'immagine. Le AMI pubbliche di Amazon archiviano questi elementi in `/root/.ssh` per l'utente root e in `/home/`*`user_name`*`/.ssh/` per gli utente normali. Per ulteriori informazioni, consulta ec2-bundle-vol.
- Elimina sempre la cronologia della shell prima di effettuare il raggruppamento. Se tenti di effettuare più di un caricamento del bundle nella stessa AMI, la cronologia di shell (interprete di comandi) conterrà la tua chiave di accesso. L'esempio seguente riporta l'ultimo comando eseguito prima del raggruppamento effettuato dall'istanza.

  ```
  [ec2-user ~]$ shred -u ~/.*history
  ```

  > **Warning**
  >
  > Le limitazioni dell'utilità **`shred`** descritte nell'avviso riportato sopra si applicano anche in questo caso.
  > Tieni presente che bash scrive la cronologia della sessione corrente sul disco al momento dell'uscita. Se ti disconnetti dall'istanza dopo avere eliminato `~/.bash_history` e ripeti l'accesso, scoprirai che `~/.bash_history` è stato ricreato e contiene tutti i comandi eseguiti durante la sessione precedente.
  > Oltre a bash, anche altri programmi scrivono la cronologia sul disco; presta attenzione e rimuovi o escludi i file e le directory dot non necessari.

- Il raggruppamento di un'istanza in esecuzione richiede la chiave privata e il certificato X.509. Inserisci queste e altre credenziali in un percorso non incluso nel bundle (come l'instance store).

AMI a pagamento

Un AMI a pagamento è un AMI elencato in vendita nel Marketplace AWS. Marketplace AWS È un negozio online in cui è possibile acquistare software funzionante AWS, comprese le AMI che

è possibile utilizzare per avviare l'istanza EC2. Le Marketplace AWS AMI sono organizzate in categorie, ad esempio Developer Tools, per consentirti di trovare prodotti adatti alle tue esigenze. Per ulteriori informazioni in merito Marketplace AWS, consulta il Marketplace AWSsito Web.

Le AMI possono essere acquistate Marketplace AWS da terze parti, comprese le AMI fornite con contratti di servizio di organizzazioni come Red Hat. Puoi anche creare un'AMI e venderla Marketplace AWS ad altri utenti di Amazon EC2. La creazione di un'AMI sicura, protetta e utilizzabile per l'uso pubblico è un processo molto semplice se segui alcune semplici linee guida. Per ulteriori informazioni su come creare e utilizzare le AMI condivise, consulta AMI condivise.

L'avvio di un'istanza da un'AMI a pagamento è analogo all'avvio di un'istanza da qualsiasi altra AMI. Non sono necessari altri parametri. L'istanza viene addebitata in base alle tariffe stabilite dal proprietario dell'AMI, nonché alle tariffe di utilizzo standard per i servizi Web correlati, ad esempio la tariffa oraria per l'esecuzione di un tipo di istanza m5.small in Amazon EC2. Potrebbero essere applicate anche tasse aggiuntive. Il proprietario dell'AMI a pagamento può confermare se un'istanza specifica è stata avviata utilizzato l'AMI a pagamento indicata.

> **Important**
>
> Amazon DevPay non accetta più nuovi venditori o prodotti. Marketplace AWS è ora l'unica piattaforma di e-commerce unificata per la vendita di software e servizi tramite. AWS Per informazioni su come distribuire e vendere software da Marketplace AWS, consulta Selling in AWS Marketplace. Marketplace AWS supporta le AMI supportate da Amazon EBS.

Indice

Vendere un'AMI

Puoi vendere la tua AMI utilizzando Marketplace AWS. Marketplace AWS offre un'esperienza di acquisto organizzata. Inoltre, supporta Marketplace AWS anche AWS funzionalità come AMI supportate da Amazon EBS, istanze riservate e istanze Spot.

Per informazioni su come vendere la tua AMI su Marketplace AWS, consulta Selling in AWS Marketplace.

Trovare un'AMI a pagamento

Sono disponibili numerosi modi per cercare le AMI disponibili per l'acquisto. Ad esempio, puoi utilizzare Marketplace AWS, la console Amazon EC2 o la riga di comando. In alternativa, uno sviluppatore può personalmente comunicarti informazioni su un'AMI a pagamento specifica.

Trovare un'AMI a pagamento con la console

Per cercare un'AMI a pagamento con la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Nel primo filtro scegliere Public images (Immagini pubbliche).
4. Nella barra di ricerca scegli Owner alias (alias del proprietario), quindi = e aws-marketplace.
5. Se conosci il codice prodotto, seleziona Product code (codice prodotto), = e digita il codice.

Trova un AMI a pagamento utilizzando Marketplace AWS

Per trovare un'AMI a pagamento utilizzando Marketplace AWS

1. Aprire Marketplace AWS.
2. Inserisci il nome del sistema operativo nel campo di ricerca, seleziona il pulsante di ricerca (lente di ingrandimento).
3. Per definire ulteriormente l'ambito dei risultati, utilizzare una delle categorie o uno dei filtri disponibili.
4. Ogni prodotto viene etichettato con il proprio tipo di prodotto, ovvero `AMI` o `Software as a Service`.

Trova un AMI a pagamento utilizzando il AWS CLI

Puoi trovare un'AMI a pagamento utilizzando il seguente comando describe-images (AWS CLI).

```
aws ec2 describe-images
    --owners aws-marketplace
```

Questo comando restituisce numerosi dettagli che descrivono ciascuna AMI, compreso il codice prodotto di un'AMI a pagamento. L'output del comando `describe-images` include una voce relativa al codice prodotto, come nell'esempio seguente:

```
"ProductCodes": [
    {
        "ProductCodeId": "product_code",
        "ProductCodeType": "marketplace"
    }
],
```

Se si conosce il codice prodotto, è possibile filtrare i risultati in base a quel codice. L'esempio seguente restituisce l'AMI più recente con il codice prodotto specificato.

```
aws ec2 describe-images
    --owners aws-marketplace \
    --filters "Name=product-code,Values=product_code" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

Trova un'AMI a pagamento utilizzando gli Strumenti per Windows PowerShell

Puoi trovare un'AMI a pagamento usando il seguente Get-EC2Imagecomando.

```
PS C:\> Get-EC2Image -Owner aws-marketplace
```

L'output di un'AMI a pagamento include il codice prodotto.

```
ProductCodeId           ProductCodeType
-------------           ---------------
product_code            marketplace
```

Se si conosce il codice prodotto, è possibile filtrare i risultati in base a quel codice. L'esempio seguente restituisce l'AMI più recente con il codice prodotto specificato.

```
PS C:\> (Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-
code";"Value"="product_code"} | sort CreationDate -Descending | Select-Object -First
 1).ImageId
```

Acquistare un'AMI a pagamento

Devi registrarti per acquistare un'AMI a pagamento prima di poter avviare un'istanza utilizzando l'AMI.

In genere, il rivenditore di un'AMI a pagamento ti invia le informazioni sull'AMI, compresi il relativo prezzo e un collegamento associato alla pagina in cui puoi effettuare l'acquisto. Quando fai clic sul link, ti viene prima chiesto di accedere AWS e poi puoi acquistare l'AMI.

Acquistare un'AMI a pagamento con la console

Puoi acquistare un'AMI a pagamento utilizzando la procedura guidata di avvio di Amazon EC2. Per ulteriori informazioni, consulta Avvia un' Marketplace AWS istanza.

Abbonati a un prodotto utilizzando Marketplace AWS

Per utilizzare il Marketplace AWS, è necessario disporre di un AWS account. Per avviare istanze dai Marketplace AWS prodotti, devi essere registrato per utilizzare il servizio Amazon EC2 e devi essere abbonato al prodotto da cui avviare l'istanza. Ci sono due modi per sottoscrivere ai prodotti in Marketplace AWS:

- Marketplace AWS sito web: Puoi avviare rapidamente il software preconfigurato con la funzione di distribuzione 1-Click.
- Procedura guidata di avvio di Amazon EC2: puoi cercare un'AMI e avviare un'istanza direttamente dalla procedura guidata. Per ulteriori informazioni, consulta Avvia un' Marketplace AWS istanza.

Recupero del codice prodotto per l'istanza

Puoi recuperare il codice Marketplace AWS prodotto dell'istanza utilizzando i metadati dell'istanza. Se l'istanza dispone di un codice prodotto, Amazon EC2 restituisce tale valore. Per ulteriori informazioni sul recupero dei metadati, consulta Recupero dei metadati dell'istanza.

Per recuperare il codice di un prodotto, utilizza il comando relativo al sistema operativo dell'istanza.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/product-codes
```

Utilizzo del supporto a pagamento

Amazon EC2 consente inoltre agli sviluppatori di offrire supporto per il software (AMI derivate). Gli sviluppatori possono creare prodotti di supporto per il cui utilizzo è prevista la registrazione. Durante il processo di registrazione per un prodotto di supporto, lo sviluppatore ti invia un codice prodotto, che dovrai quindi associare all'AMI in tuo possesso. Ciò consente allo sviluppatore di verificare che la tua istanza ha diritto al supporto. Garantisce inoltre che quando esegui le istanze del prodotto ti vengano addebitati i costi corretti in base alle condizioni specificate per il prodotto dallo sviluppatore.

> **Important**
>
> Non puoi utilizzare un prodotto di supporto con le Istanze riservate. Ti verrà sempre addebitato il prezzo specificato dal rivenditore del prodotto di supporto.

Per associare un codice prodotto all'AMI, utilizzare uno dei seguenti comandi, dove ami_id rappresenta l'ID dell'AMI e product_code rappresenta il codice prodotto:

- modify-image-attribute (AWS CLI)

```
aws ec2 modify-image-attribute --image-id ami_id --product-codes "product_code"
```

- Edit-EC2ImageAttribute (AWS Tools for Windows PowerShell)

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami_id -ProductCode product_code
```

Dopo aver impostato l'attributo relativo al codice prodotto, non puoi più modificarlo o rimuoverlo.

Fatture per AMI a pagamento e supportate

Alla fine di ogni mese riceverai un messaggio e-mail contenente l'importo addebitato sulla tua carta di credito per l'utilizzo di qualsiasi AMI a pagamento o supportata durante il mese appena trascorso. Questa fattura è distinta rispetto alla normale fattura di Amazon EC2. Per ulteriori informazioni, consulta Pagamento dei prodotti nella Marketplace AWS Guida per gli acquirenti .

Gestisci i tuoi abbonamenti Marketplace AWS

Sul Marketplace AWS sito Web, puoi controllare i dettagli dell'abbonamento, visualizzare le istruzioni di utilizzo del fornitore, gestire gli abbonamenti e altro ancora.

Per controllare i dettagli della sottoscrizione

1. Accedi al Marketplace AWS.
2. Scegliere Your Marketplace Account (Account Marketplace personale).
3. Scegliere Manage your software subscriptions (Gestisci sottoscrizioni software).
4. Vengono elencate tutte le sottoscrizioni correnti. Scegliere Usage Instructions (Istruzioni di utilizzo) per visualizzare istruzioni specifiche relative all'utilizzo del prodotto, ad esempio un nome utente per la connessione all'istanza in esecuzione.

Per annullare un abbonamento Marketplace AWS

1. Assicurarsi di aver terminato tutte le istanze in esecuzione dalla sottoscrizione.
   a. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   b. Nel riquadro di navigazione, seleziona Istanze.
   c. Seleziona l'istanza e scegli Instance state (Stato istanza), Terminate instance (Termina istanza).
   d. Quando viene richiesta la conferma, seleziona Terminate (Interrompi).

2. Accedere al Marketplace AWS e scegliere Account Marketplace personale, quindi Gestisci sottoscrizioni software.
3. Scegliere Cancel subscription (Annulla sottoscrizione). Verrà richiesto di confermare l'annullamento.

> **Note**
>
> Dopo aver annullato la sottoscrizione, non sara più in possibile avviare istanze dall'AMI specifica. Per utilizzare nuovamente quell'AMI, devi abbonarti nuovamente, sul Marketplace AWS sito Web o tramite la procedura guidata di avvio nella console Amazon EC2.

Ciclo di vita di un'AMI

Puoi creare le tue AMI, copiarle, eseguirne il backup e conservarle fino a quando non sei pronto a deprecarle o annullarne la registrazione.

Indice

Creare un'AMI

Puoi creare AMI Linux o Windows supportate da volumi Amazon EBS. Puoi anche creare AMI Linux supportate da volumi di instance store (le AMI Windows non supportano l'instance store per il dispositivo root). È inoltre possibile utilizzare Windows Sysprep per creare AMI Windows.

Argomenti

Crea un'AMI supportata da Amazon EBS

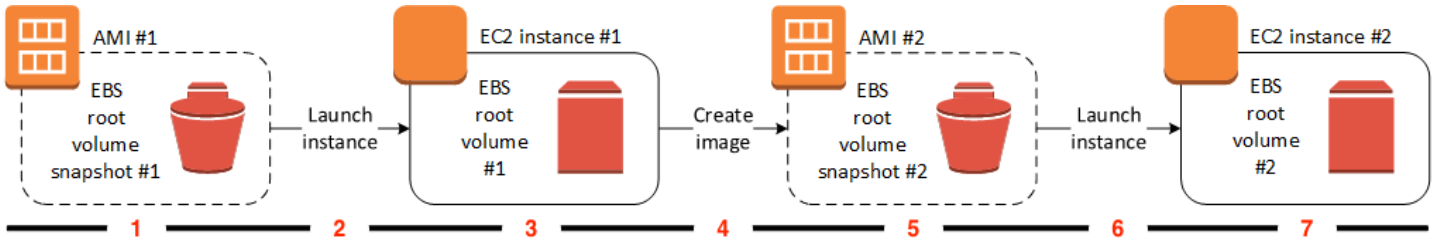
Per creare un'AMI supportata da Amazon EBS, inizia da un'istanza che hai lanciato da un'AMI esistente supportata da Amazon EBS. Può trattarsi di un AMI ottenuto da Marketplace AWS, di un AMI creato utilizzando AWS Server Migration Serviceo VM Import/Export o di qualsiasi altro AMI a cui è possibile accedere. Dopo aver personalizzato l'istanza in base alle tue esigenze, è necessario creare e registrare una nuova AMI, che puoi utilizzare per avviare nuove istanze con queste personalizzazioni.

Le procedure descritte di seguito sono valide per le istanze di Amazon EC2 supportate dai volumi Amazon Elastic Block Store (Amazon EBS) (incluso il volume root) e per i volumi non crittografati.

Il processo di creazione dell'AMI è diverso per le AMIs supportate da instance store. Per informazioni sulle differenze tra istanze supportate da Amazon EBS e istanze supportate da instance store e su come determinare il tipo di dispositivo root per l'istanza, consulta Archiviazione del dispositivo root. Per informazioni sulla creazione di un'AMI basata su instance store-backed, consulta. Creazione di un'AMI Linux supportata da un instance store

Panoramica sulla creazione di AMIs supportate da Amazon EBS

Il diagramma seguente riepiloga il processo di creazione di un'AMI Amazon EBS-backed da un'istanza EC2 in esecuzione: si inizia con un'AMI esistente, si avvia un'istanza, la si personalizza, si crea una nuova AMI da essa e infine si avvia un'istanza della nuova AMI. I numeri nel diagramma corrispondono ai numeri nella descrizione che segue.



1 — AMI #1: si inizia con un'AMI esistente

Individua un'AMI esistente simile all'AMI che si desidera creare. Può trattarsi di un AMI ottenuto da Marketplace AWS, di un AMI creato utilizzando AWS Server Migration Serviceo VM Import/Export o di qualsiasi altro AMI a cui è possibile accedere. Si personalizzerà questa AMI in base alle proprie esigenze.

Nel diagramma, lo snapshot del volume root EBS #1 indica che l'AMI è un'AMI Amazon EBS-backed e che le informazioni sul volume root sono memorizzate in questo snapshot.

2 — Si avvia l'istanza dall'AMI esistente

Il modo per configurare un'AMI consiste nel lanciare un'istanza dall'AMI su cui si desidera basare la nuova AMI, quindi personalizzare l'istanza (indicata all'indirizzo 3 nel diagramma). Quindi si creerà una nuova AMI che include le personalizzazioni (indicate all'indirizzo 4 nel diagramma).

3 — Istanza EC2 #1: si personalizza l'istanza

Connettersi all'istanza e personalizzarla in base alla proprie esigenze. La nuova AMI includerà queste personalizzazioni.

È possibile effettuare una delle operazioni seguenti sull'istanza per personalizzarla in base alle proprie esigenze:

- Installazione di software e applicazioni
- Copia dei dati
- Riduzione del tempo di avvio tramite l'eliminazione dei file temporanei e la deframmentazione del disco rigido
- Collegamento di volumi EBS aggiuntivi

4 — Si crea un'immagine

Quando un'AMI viene creata da un'istanza, Amazon EC2 spegne l'istanza prima di creare l'AMI per garantire che tutto ciò che è presente sull'istanza sia arrestato e mantenuto in uno stato coerente durante la procedura di creazione. Se sei sicuro che l'istanza sia in uno stato coerente, appropriato per la creazione dell'AMI, puoi indicare ad Amazon EC2 di non spegnere e riavviare l'istanza. Alcuni file system, come XFS, possono bloccare e sbloccare l'attività, consentendo la creazione sicura dell'immagine senza il riavvio dell'istanza.

Durante il processo di creazione dell'AMI, Amazon EC2 crea degli snapshot del volume root dell'istanza e di altri volumi EBS collegati alla tua istanza. Ti verrà addebitato il costo degli snapshot finché non annullerai la registrazione dell'AMI e non eliminerai gli snapshot. Se i volumi

collegati all'istanza sono crittografati, la nuova AMI viene avviata correttamente solo sulle istanze che supportano la crittografia Amazon EBS.

A seconda della dimensione dei volumi, potrebbero essere necessari diversi istanti per il completamento del processo di creazione dell'AMI (a volte fino a 24 ore). Si potrebbe ritenere più efficiente creare snapshot dei volumi prima della creazione dell'AMI. In questo modo, in seguito alla creazione dell'AMI, dovrai creare soltanto snapshot incrementali e di piccole dimensioni, e il processo verrà completato più rapidamente (il tempo totale per la creazione della snapshot rimane invariato).

5 — AMI #2: Una nuova AMI

Al termine del processo, si disporrà di una nuova AMI e di uno snapshot (snapshot #2) creati dal volume root dell'istanza. Se si aggiungono volumi di archivio istanza o volumi EBS all'istanza, oltre al volume dispositivo root, la mappatura dei dispositivi a blocchi per la nuova AMI conterrà informazioni su tali volumi.

Amazon EC2 registra automaticamente l'AMI

6 — Si avvia un'istanza da una nuova AMI.

È possibile utilizzare la nuova AMI per avviare un'istanza.

7 — Istanza EC2 #2: una nuova istanza

Quando si avvia un'istanza con la nuova AMI, Amazon EC2 crea un nuovo volume EBS per il relativo volume root tramite lo snapshot. Se si aggiungono volumi di archivio istanza o volumi EBS all'istanza, oltre al volume dispositivo root, la mappatura dei dispositivi a blocchi per la nuova AMI conterrà informazioni su tali volumi e le mappature dei dispositivi a blocchi per le istanze avviate dalla nuova AMI includeranno automaticamente le informazioni relative a tali volumi. I volumi instance store specificati nella mappatura dei dispositivi a blocchi per la nuova istanza sono nuovi e non contengono nessun dato sui volumi instance store dell'istanza utilizzata per creare l'AMI. I dati sui volumi EBS vengono conservati. Per ulteriori informazioni, consulta Mappatura dei dispositivi a blocchi.

Quando una nuova istanza da un'AMI EBS-backed viene creata, occorre inizializzare il relativo volume root e l'archiviazione EBS aggiuntiva prima di inserirla in produzione. Per ulteriori informazioni, consulta Initialize Amazon EBS Volumes nella Amazon EBS User Guide.

Creare un AMI da un'istanza

È possibile creare un AMI utilizzando AWS Management Console o la riga di comando.

Console

Per creare un AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza dalla quale creare l'AMI, quindi scegli Actions (Operazioni), Image and templates (Immagine e modelli), Create image (Crea immagine).

   > **Tip**
   >
   > Se questa opzione è disabilitata, l'istanza non è un'istanza supportata da Amazon EBS.

4. Nella pagina Create image (Crea immagine), specifica le seguenti informazioni:

   a. In Image name (Nome immagine), inserisci un nome univoco per l'immagine lungo al massimo 127 caratteri.

   b. In Image description (Descrizione immagine), inserisci una descrizione facoltativa dell'immagine lunga al massimo 255 caratteri.

   c. In No reboot (Nessun riavvio), lascia deselezionata la casella di controllo Enable (Abilita), che è l'impostazione predefinita, oppure selezionala.

      - Se la casella di controllo Abilita non è selezionata per Nessun riavvio, quando Amazon EC2 crea la nuova AMI, riavvia l'istanza in modo da poter acquisire snapshot dei volumi collegati mentre i dati sono a riposo, al fine di garantire uno stato coerente.
      - Se la casella di controllo Abilita è selezionata per Nessun riavvio, quando Amazon EC2 crea la nuova AMI, non chiude e non riavvia l'istanza.

      > **Warning**
      >
      > Se si sceglie di abilitare No reboot (Non riavviare), non possiamo garantire l'integrità del file system dell'immagine creata.

   d. Volumi istanza: puoi modificare il volume root e aggiungere altri volumi Amazon EBS e di archivio dell'istanza, come segue:

i. Il volume root è definito nella prima riga.

- Per modificare la dimensione del volume root, in Dimensione immetti il valore richiesto.
- Se selezioni Delete on Termination (Elimina al termine), quando termini l'istanza creata da questa AMI, il volume EBS viene eliminato. Se deselezioni Delete on Termination (Elimina al termine), quando termini l'istanza, il volume EBS non viene eliminato. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.

ii. Per aggiungere un volume EBS, seleziona Add New Volume (Aggiungi nuovo volume), che comporta l'aggiunta di una nuova riga. Per Tipo di archiviazione, scegli EBSe compilai campi nella riga. Quando avvii un'istanza dalla nuova AMI, questi volumi aggiuntivi vengono collegati automaticamente all'istanza. È necessario formattare e montare i volumi vuoti. È necessario montare i volumi basati su snapshot.

iii. Per aggiungere un volume instance store, consulta Aggiunta di volumi di instance store a un'AMI. Quando avvii un'istanza dalla nuova AMI, i volumi aggiuntivi vengono inizializzati e installati automaticamente. Questi volumi non contengono i dati dai volumi instance store dell'istanza in esecuzione sulla quale hai basato l'AMI.

e. Tags (Tag) - È possibile contrassegnare l'AMI e gli snapshot con gli stessi tag, oppure contrassegnarli con tag diversi.

- Per taggare l'AMI e gli snapshot con gli stessi tag, scegli Tag image and snapshots together. All'AMI e a ogni snapshot creato vengono applicati gli stessi tag.
- Per contrassegnare l'AMI e gli snapshot con tag diversi, scegli Tag image and snapshots separately. All'AMI e a ogni snapshot creato vengono applicati tag diversi. Tuttavia, tutti gli snapshot ricevono gli stessi tag; non è possibile contrassegnare ogni snapshot con un tag diverso.

Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore per il tag. Ripetere per ogni tag.

f. Quando è tutto pronto per creare l'AMI, scegli Create image (Crea immagine).

5. Per visualizzare lo stato dell'AMI durante la creazione:

a. Nel riquadro di navigazione scegliere AMIs (AMI).

b. Imposta il filtro su Owned by me (Di mia proprietà) e seleziona l'AMI dall'elenco.

   Inizialmente lo stato è `pending`, ma dovrebbe cambiare in `available` dopo pochi minuti.

6. (Facoltativo) Per visualizzare lo snapshot creato per la nuova AMI:

   a. Annota l'ID dell'AMI individuata nel passaggio precedente.

   b. Nel pannello di navigazione, selezionare Snapshots (Snapshot).

   c. Imposta il filtro su Owned by me (Di mia proprietà), quindi trova lo snapshot con il nuovo ID AMI nella colonna Description (Descrizione).

      Quando avvii un'istanza da quest'AMI, Amazon EC2 utilizza questo snapshot per creare il relativo volume dispositivo root.

AWS CLI

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- create-image (AWS CLI)
- New-EC2Image (AWS Tools for Windows PowerShell)

Creazione di un'AMI Linux da uno snapshot

Se disponi di un'istantanea del volume del dispositivo root di un'istanza, puoi creare un'AMI Linux da questa istantanea utilizzando AWS Management Console o la riga di comando. Questa funzionalità non è attualmente disponibile per le istanze Windows.

Console

Per creare un AMI da un'istantanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Snapshots (Snapshot).
3. Seleziona lo snapshot dal quale creare l'AMI e scegli Actions (Operazioni), Create image from snapshot (Crea un'immagine dallo snapshot).
4. Nella pagina Crea immagine da istantanea, specificate le seguenti informazioni:

a. In Image name (Nome immagine), inserire un nome descrittivo per l'immagine.

b. In Description (Descrizione) inserire una breve descrizione dell'immagine.

c. In Architecture (Architettura), scegliere l'architettura dell'immagine. Scegli i386 per 32 bit, x86_64 per 64 bit, arm64 per ARM a 64 bit o x86_64 per macOS a 64 bit.

d. In Root device name (Nome dispositivo root), inserire il nome del dispositivo da utilizzare per il volume del dispositivo di root. Per ulteriori informazioni, consulta Nomi dei dispositivi sulle istanze Amazon EC2.

e. Per Virtualization type (Tipo di virtualizzazione), scegliere il tipo di virtualizzazione da utilizzare dalle istanze avviate da questa AMI. Per ulteriori informazioni, consulta Tipi di virtualizzazione dell'AMI.

f. (Solo per la virtualizzazione paravirtuale) Per Kernel ID (ID kernel), selezionare il kernel del sistema operativo per l'immagine. Se si utilizza uno snapshot del volume del dispositivo di root di un'istanza, selezionare lo stesso ID kernel dell'istanza originale. Se non si è sicuri, utilizzare il kernel di default.

g. (Solo per la virtualizzazione paravirtuale) Per RAM disk ID (ID disco RAM), selezionare il disco RAM per l'immagine. Se è stato selezionato un kernel specifico, potrebbe essere necessario selezionare un disco RAM specifico con i driver che lo supportano.

h. Per la modalità di avvio, scegli la modalità di avvio per l'immagine o scegli Usa default in modo che quando un'istanza viene avviata con questa AMI, si avvii con la modalità di avvio supportata dal tipo di istanza. Per ulteriori informazioni, consulta Impostare la modalità di avvio di un'AMI.

i. (Facoltativo) In Block device mappings, personalizza il volume root e aggiungi volumi di dati aggiuntivi.

   Per ogni volume, si possono specificare le dimensioni, il tipo, le caratteristiche delle prestazioni, il comportamento dell'eliminazione alla terminazione e lo stato di crittografia. Per il volume root, la dimensione non può essere inferiore alla dimensione dello snapshot. Per il tipo di volume, SSD a uso generale `gp3` è la selezione predefinita.

j. (Facoltativo) In Tag, puoi aggiungere uno o più tag alla nuova AMI. Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore per il tag. Ripetere per ogni tag.

k. Quando è tutto pronto per creare l'AMI, scegli Create image (Crea immagine).

AWS CLI

Per creare un'AMI da una snapshot tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- register-image (CLI)AWS
- Register-EC2Image (AWS Tools for Windows PowerShell)

Avvia un'istanza da un'AMI che hai creato

È possibile avviare un'istanza da un'AMI creata da un'istanza o da uno snapshot.

Per avviare un'istanza dalla nuova AMI.

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di spostamento, in Images (Immagini), scegliere AMI.
3. Imposta il filtro su Owned by me (Di mia proprietà) e seleziona la tua AMI.
4. Scegli Avvia istanza dall'AMI.
5. Accettare i valori di default o specificare valori personalizzati nella procedura guidata di avvio dell'istanza. Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Creazione di un'AMI Linux supportata da un instance store

L'AMI specificata quando avvii l'istanza determina il tipo di volume dispositivo root.

Per creare un'AMI Linux supportata da instance store, inizia da un'istanza che hai avviato da un'AMI Linux supportata da instance store esistente. Dopo avere personalizzato l'istanza in base alle tue esigenze, è necessario creare un bundle del volume e registrare una nuova AMI, che puoi utilizzare per avviare nuove istanze con queste personalizzazioni.

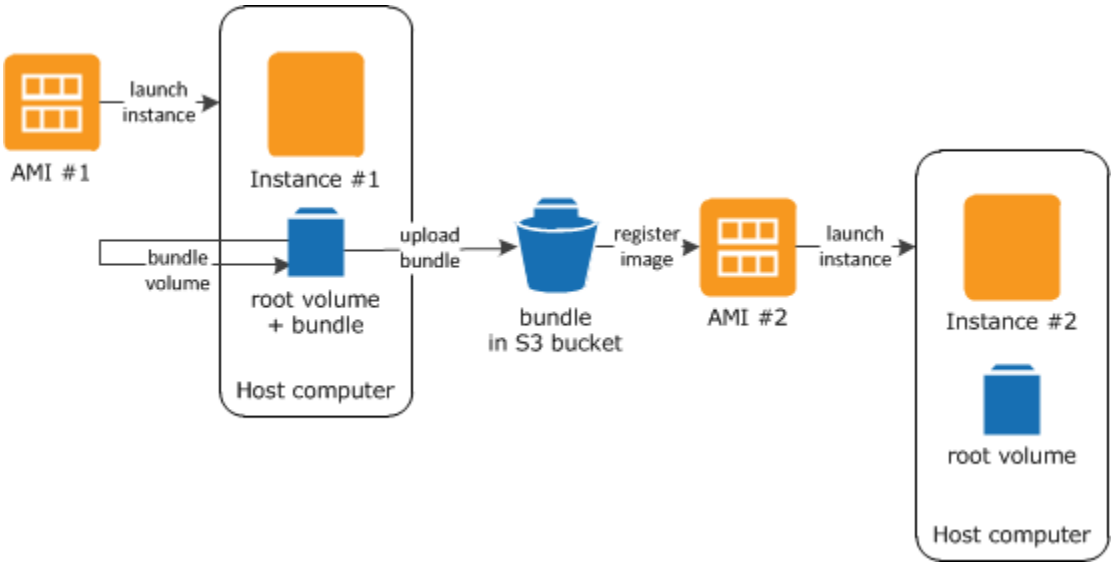
Non è possibile creare un'AMI Windows supportata da Instance-Store perché le AMI Windows non supportano l'Instance Store per il dispositivo root.

> **Important**
>
> Solo i seguenti tipi di istanza supportano un volume di instance store come dispositivo principale: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Il processo di creazione di AMI è diverso per le AMI Amazon EBS-backed. Per ulteriori informazioni sulle differenze tra istanze supportate da Amazon EBS e istanze supportate da instance store e su come determinare il tipo di dispositivo root per l'istanza, consulta Archiviazione del dispositivo root. Se devi creare un'AMI supportata da Amazon EBS, consulta. Crea un'AMI supportata da Amazon EBS

Panoramica del processo di creazione delle AMI supportate da instance store

Il diagramma seguente riepiloga le operazioni necessarie per la creazione di un'AMI a partire da un'istanza supportata da instance store.



Innanzitutto, avvia un'istanza da un'AMI che sia simile all'AMI che desideri creare. Puoi connetterti alla tua istanza e personalizzarla. Una volta che è configurata come desideri puoi creare un bundle dell'istanza. Per il completamento di questo processo sono richiesti vari minuti. Al termine del processo avrai un bundle, composto da un manifest delle immagini (`image.manifest.xml`) e da file (`image.part.xx`) contenenti un modello per il volume root. Successivamente, carica il bundle nel bucket Amazon S3 e registra l'AMI.

> **Note**
>
> Per caricare oggetti in un bucket S3 per l'AMI Linux supportata da archivi istanze, è necessario abilitare le ACL per il bucket. In caso contrario, Amazon EC2 non sarà in grado di impostare le ACL sugli oggetti da caricare. Se il bucket di destinazione utilizza l'impostazione applicata dal proprietario del bucket per S3 Object Ownership, ciò non funzionerà perché le ACL sono disabilitate. Per maggiori informazioni, consultare Controllo della proprietà degli oggetti caricati tramite S3 Object Ownership.

Quando avvii un'istanza con la nuova AMI, viene creato il volume root dell'istanza usando il bundle che hai caricato in Amazon S3. Finché non lo elimini, lo spazio di archiviazione utilizzato dal bundle in Amazon S3 comporta dei costi che vengono addebitati sul tuo account. Per ulteriori informazioni, consulta Annullare la registrazione (eliminare) un AMI.

Se aggiungi dei volumi instance store all'istanza, oltre al volume dispositivo root, la mappatura dei dispositivi a blocchi per la nuova AMI conterrà informazioni su tali volumi e le mappature dei dispositivi a blocchi per le istanze che avvii dalla nuova AMI conterranno automaticamente le informazioni relative a tali volumi. Per ulteriori informazioni, consulta Mappatura dei dispositivi a blocchi.

Prerequisiti

Prima di poter creare un AMI, devi completare le attività seguenti:

- Installazione degli strumenti AMI. Per ulteriori informazioni, consulta Configurazione degli strumenti dell'AMI.
- Installa il. AWS CLI Per ulteriori informazioni, consulta la sezione su come eseguire la configurazione con AWS Command Line Interface.
- Verificare di disporre di un bucket S3 per il bundle e che il bucket abbia le ACL abilitate. Per ulteriori informazioni sulla configurazione delle ACL, consulta la pagina Configurazione delle ACL.
  - Per creare un bucket S3 utilizzando AWS Management Console, apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/ e scegli Create Bucket.
  - Per creare un bucket S3 con AWS CLI, puoi usare il comando mb. Se la versione installata degli strumenti AMI è la 1.5.18 o successiva, per creare il bucket S3 puoi anche usare il comando `ec2-upload-bundle`. Per ulteriori informazioni, consulta ec2-upload-bundle.

- Assicurati di avere l'ID del tuo AWS account. Per ulteriori informazioni, consulta Visualizza Account AWS gli identificatori nella Guida di riferimento per la gestione degli AWS account.
- Assicurati di disporre delle credenziali per utilizzare la AWS CLI. Per ulteriori informazioni, consulta le migliori pratiche per AWS gli account nella Guida AWS Account Management di riferimento.
- Verifica della disponibilità di un certificato X.509 e della chiave privata corrispondente.
  - Per creare un certificato X.509, consultare Gestione dei certificati di firma. Il certificato X.509 e la chiave privata vengono utilizzati per codificare e decodificare l'AMI.
  - [Cina (Pechino)] Utilizza il certificato `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem`.
  - [AWS GovCloud (US-West)] Usa il `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem` certificato.
- Connessione all'istanza e relativa personalizzazione. Ad esempio, è possibile installare software e applicazioni, copiare i dati, eliminare i file temporanei e modificare la configurazione Linux.

Attività

- Configurazione degli strumenti dell'AMI
- Creazione di un'AMI da un'istanza Amazon Linux supportata da instance store
- Creazione di un'AMI da un'istanza Ubuntu supportata da instance store
- Conversione dell'AMI supportata da instance store in un'AMI Amazon EBS-backed

Configurazione degli strumenti dell'AMI

Puoi utilizzare gli strumenti AMI per creare e gestire le AMIs Linux supportate dall'instance store. Per usare gli strumenti, è necessario installarli sulla propria istanza Linux. Gli strumenti AMI sono disponibili sia come file RPM che come file .zip per le distribuzioni Linux che non supportano il formato RPM.

Per configurare gli strumenti AMI tramite il file RPM

1. Installare Ruby utilizzando il programma di gestione dei pacchetti per la distribuzione Linux in uso, come yum. Ad esempio:

   ```
   [ec2-user ~]$ sudo yum install -y ruby
   ```

2. Scaricare il file RPM utilizzando uno strumento come wget o curl. Ad esempio:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. Verificare la firma del file RPM tramite il seguente comando:

```
[ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
```

Questo comando deve indicare che gli hash SHA1 e MD5 del file sono nello stato `OK`. Se il comando indica che gli hash sono nello stato `NOT OK`, utilizzare il seguente comando per visualizzare gli hash Header SHA1 e MD5 del file:

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

Quindi, confrontare tali hash con i seguenti hash degli strumenti AMI verificati per confermare l'autenticità del file:

- Header SHA1: a1f662d6f25f69871104e6a62187fa4df508f880
- MD5: 9faff05258064e2f7909b66142de6782

Se gli hash Header SHA1 e MD5 del file corrispondono agli hash degli strumenti AMI verificati, continuare con la fase successiva.

4. Installare il file RPM utilizzando il seguente comando:

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. Verificare l'installazione degli strumenti AMI tramite il comando ec2- ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

> **Note**
>
> Se ricevi un errore di caricamento del tipo «cannot load such file -- ec2/amitools/version (LoadError)», completa il passaggio successivo per aggiungere la posizione dell'installazione degli strumenti AMI al tuo percorso. `RUBYLIB`

6. (Facoltativo) Se nella fase precedente si è ricevuto un errore, aggiungere la posizione dell'installazione degli strumenti AMI al percorso `RUBYLIB`.

a. Eseguire il seguente comando per determinare i percorsi da aggiungere.

```
[ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
/usr/lib/ruby/site_ruby/ec2/amitools/version.rb
/usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
```

Nell'esempio di cui sopra, il file mancante indicato nel precedente errore di caricamento si trova in `/usr/lib/ruby/site_ruby` e `/usr/lib64/ruby/site_ruby`.

b. Aggiungere le posizioni indicate nella fase precedente al percorso `RUBYLIB`.

```
[ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/
site_ruby
```

c. Verificare l'installazione degli strumenti AMI tramite il comando ec2- ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Per configurare gli strumenti AMI tramite il file .zip

1. Installare Ruby e decomprimerlo utilizzando il programma di gestione dei pacchetti per la distribuzione Linux in uso, come apt-get. Ad esempio:

```
[ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. Scaricare il file .zip utilizzando uno strumento come wget o curl. Ad esempio:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. Decomprimere i file in una directory di installazione adatta, come `/usr/local/ec2`.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

Si noti che il file .zip contiene una cartella ec2-ami-tools-*x.x.x*, in cui *x.x.x* è il numero della versione degli strumenti (ad esempio, `ec2-ami-tools-1.5.7`).

4. Impostare la variabile di ambiente `EC2_AMITOOL_HOME` sulla posizione directory di installazione degli strumenti. Ad esempio:

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Aggiungere gli strumenti alla variabile di ambiente PATH. Ad esempio:

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. È possibile verificare l'installazione degli strumenti AMI tramite il comando ec2- ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Gestione dei certificati di firma

Alcuni comandi negli strumenti AMI necessitano di un certificato di firma (noto anche come certificato X.509). È necessario creare il certificato e poi caricarlo su. AWS Ad esempio, per creare il certificato puoi utilizzare uno strumento di terza parte come OpenSSL.

Per creare un certificato di firma

1. Installare e configurare OpenSSL
2. Creare una chiave privata usando il comando `openssl genrsa` e salvare l'output in un file `.pem`. È consigliabile creare una chiave RSA a 2048 o 4096 bit.

```
openssl genrsa 2048 > private-key.pem
```

3. Generare un certificato usando il comando `openssl req`.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -
out certificate.pem
```

Per caricare il certificato su AWS, usa il upload-signing-certificatecomando.

```
aws iam upload-signing-certificate --user-name user-name --certificate-body
 file://path/to/certificate.pem
```

Per elencare i certificati per un utente, usa il list-signing-certificatescomando:

```
aws iam list-signing-certificates --user-name user-name
```

Per disabilitare o riattivare un certificato di firma per un utente, usa il update-signing-certificatecomando. Il seguente comando disattiva il certificato:

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE --
status Inactive --user-name user-name
```

Per eliminare un certificato, usa il delete-signing-certificatecomando:

```
aws iam delete-signing-certificate --user-name user-name --certificate-
id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE
```

Creazione di un'AMI da un'istanza supportata da instance store

Le procedure seguenti ti permettono di creare un'AMI supportata da instance store a partire da un'istanza supportata da instance store. Prima di iniziare, assicurati di leggere i Prerequisiti.

Argomenti

- Creazione di un'AMI da un'istanza Amazon Linux supportata da instance store
- Creazione di un'AMI da un'istanza Ubuntu supportata da instance store

Creazione di un'AMI da un'istanza Amazon Linux supportata da instance store

Questa sezione descrive la creazione di un'AMI da un'istanza Amazon Linux. Le procedure seguenti potrebbero non funzionare per le istanze eseguite su altre distribuzioni Linux. Per le procedure specifiche di Ubuntu, consultare Creazione di un'AMI da un'istanza Ubuntu supportata da instance store.

Per prepararsi a utilizzare gli strumenti AMI (solo istanze HVM)

1. Per essere avviati correttamente, gli strumenti AMI necessitano di GRUB Legacy. Utilizzare il comando seguente per installare GRUB:

   ```
   [ec2-user ~]$ sudo yum install -y grub
   ```

2. Installare i pacchetti di gestione delle partizioni usando il seguente comando:

```
[ec2-user ~]$ sudo yum install -y gdisk kpartx parted
```

Per creare un'AMI da un'istanza Amazon Linux supportata da instance store

Questa procedura presuppone che i prerequisiti indicati in Prerequisiti siano stati soddisfatti.

Nei comandi seguenti, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

1. Caricare le credenziali nell'istanza. Le credenziali servono a garantire l'accesso all'AMI solo da parte dell'utente e da Amazon EC2.

   a. Creare una directory temporanea sull'istanza per le credenziali, come segue:

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

   In questo modo è possibile escludere le proprie credenziali dall'immagine creata.

   b. Copiare il certificato X.509 e la chiave privata corrispondente dal proprio computer nella directory `/tmp/cert` sull'istanza utilizzando uno strumento di copia protetta come scp. L'opzione `-i` *`my-private-key`*`.pem` nel comando scp seguente è la chiave privata da utilizzare per connettersi all'istanza con SSH, non la chiave privata X.509. Ad esempio:

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
   path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
   ```

   In alternativa, poiché questi sono file di testo normale, è possibile aprire il certificato e la chiave in un editor di testo e copiarne il contenuto in nuovi file in `/tmp/cert`.

2. Preparare il bundle da caricare in Amazon S3 eseguendo il comando ec2-bundle-vol dall'istanza. Accertarsi di specificare l'opzione `-e` per escludere la directory in cui sono archiviate le proprie credenziali. Per impostazione predefinita, il processo di creazione di bundle esclude i file che possono contenere informazioni sensibili. Tali file includono `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` e

`*/.bash_history`. Per includere tutti questi file, utilizzare l'opzione `--no-filter`. Per includere alcuni di questi file, utilizzare l'opzione `--include`.

> **Important**
>
> Per impostazione predefinita, il processo di raggruppamento dell'AMI crea una raccolta codificata di file nella directory `/tmp` che rappresenta il volume root. Se non è disponibile sufficiente spazio libero sul disco in `/tmp` per archiviare il bundle, occorre specificare una posizione diversa per il bundle da archiviare con l'opzione `-d` *`/path/to/bundle/storage`*. Alcune istanze hanno uno storage temporaneo montato su `/mnt` o `/media/ephemeral0` che puoi utilizzare, oppure puoi anche creare, collegare e montare un nuovo volume Amazon (EBS) per archiviare il pacchetto. Per ulteriori informazioni, consulta Creare un volume Amazon EBS nella Guida per l'utente di Amazon EBS.

a. Il ec2-bundle-vol comando deve essere eseguito come root. Per la maggior parte dei comandi, è possibile utilizzare sudo per ottenere autorizzazioni elevate, ma in questo caso occorre eseguire sudo -E su per mantenere le variabili di ambiente.

```
[ec2-user ~]$ sudo -E su
```

Si noti che il prompt bash ora identifica l'utente come utente root e il simbolo del dollaro è stato sostituito da un tag hash, a segnalare che ci si trova in una shell root:

```
[root ec2-user]#
```

b. Per creare il bundle dell'AMI, eseguire il comando ec2-bundle-vol come segue:

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --
partition gpt
```

> **Note**
>
> Per le regioni Cina (Pechino) e AWS GovCloud (Stati Uniti occidentali), utilizza il `--ec2cert` parametro e specifica i certificati in base ai prerequisiti.

Possono essere necessari alcuni minuti per creare l'immagine. Al termine del comando, la directory `/tmp` (o quella non predefinita) contiene il bundle (`image.manifest.xml`, oltre a più file `image.part.xx`).

c. Uscire dalla shell root.

```
[root ec2-user]# exit
```

3. (Facoltativo) Per aggiungere altri volumi instance store, modificare le mappature dei dispositivi a blocchi nel file `image.manifest.xml` dell'AMI. Per ulteriori informazioni, consulta Mappatura dei dispositivi a blocchi.

a. Creare un backup del file `image.manifest.xml`.

```
[ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

b. Riformattare il file `image.manifest.xml` per renderne più semplice la lettura e la modifica.

```
[ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
image.manifest.xml
```

c. Modificare le mappature dei dispositivi a blocchi in `image.manifest.xml` con un editor di testo. Il seguente esempio mostra una nuova voce del volume instance store `ephemeral1`.

> **Note**
>
> Per un elenco dei file esclusi, consulta ec2-bundle-vol.

```
    <block_device_mapping>
      <mapping>
        <virtual>ami</virtual>
        <device>sda</device>
      </mapping>
      <mapping>
        <virtual>ephemeral0</virtual>
        <device>sdb</device>
      </mapping>
      <mapping>
        <virtual>ephemeral1</virtual>
```

```
        <device>sdc</device>
      </mapping>
      <mapping>
        <virtual>root</virtual>
        <device>/dev/sda1</device>
      </mapping>
    </block_device_mapping>
```

d. Salvare il file `image.manifest.xml` e uscire dall'editor di testo.

4. Per caricare il bundle su Amazon S3, eseguire il comando ec2-upload-bundle come segue.

```
[ec2-user ~]$ ec2-upload-bundle -b DOC-EXAMPLE-BUCKET/bundle_folder/bundle_name -
m /tmp/image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Per registrare l'AMI in una regione diversa da US East (N. Virginia), occorre specificare sia la regione di destinazione con l'opzione `--region` che un percorso del bucket esistente nella regione di destinazione oppure un percorso univoco del bucket che è possibile creare nella regione di destinazione.

5. (Facoltativo) Una volta caricato il bundle su Amazon S3, è possibile rimuoverlo dalla directory `/tmp` sull'istanza utilizzando il seguente comando rm:

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Se si è specificato un percorso con l'opzione `-d` */path/to/bundle/storage* in Step 2, utilizzare quel percorso invece di `/tmp`.

6. Per registrare l'AMI, eseguire il comando register-image come segue.

```
[ec2-user ~]$ aws ec2 register-image --image-location DOC-EXAMPLE-
BUCKET/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Se precedentemente si è specificata una regione per il comando ec2-upload-bundle, specificarla nuovamente per questo comando.

Creazione di un'AMI da un'istanza Ubuntu supportata da instance store

Questa sezione descrive la creazione di un AMI da un'istanza Ubuntu Linux con un volume instance store come volume radice. Le procedure seguenti potrebbero non funzionare per le istanze eseguite su altre distribuzioni Linux. Per le procedure specifiche di Amazon Linux, consultare Creazione di un'AMI da un'istanza Amazon Linux supportata da instance store.

Per prepararsi a utilizzare gli strumenti AMI (solo istanze HVM)

Per essere avviati correttamente, gli strumenti AMI necessitano di GRUB Legacy. Tuttavia, Ubuntu è configurato per l'utilizzo di GRUB 2. Devi verificare che l'istanza utilizzi GRUB Legacy e, diversamente, installarlo e configurarlo.

Le istanze HVM richiedono inoltre l'installazione degli strumenti di partizionamento perché gli strumenti AMI funzionino correttamente.

1. GRUB Legacy (versione 0.9*x* o inferiore) deve essere installato sull'istanza. Verificare se GRUB Legacy è presente e se necessario installarlo.

   a. Verificare la versione dell'installazione GRUB.

   ```
   ubuntu:~$ grub-install --version
   grub-install (GRUB) 1.99-21ubuntu3.10
   ```

   In questo esempio, la versione GRUB è superiore a 0.9*x*, pertanto è necessario installare GRUB Legacy. Passa a Step 1.b. Se GRUB Legacy è già presente, passare alla Step 2.

   b. Installa il pacchetto `grub` utilizzando il seguente comando.

   ```
   ubuntu:~$ sudo apt-get install -y grub
   ```

2. Installare i seguenti pacchetti di gestione delle partizioni utilizzando il programma di gestione dei pacchetti per la distribuzione in uso.

- `gdisk` (alcune distribuzioni potrebbero chiamare questo pacchetto `gptfdisk`)
- `kpartx`
- `parted`

Utilizzare il seguente comando.

```
ubuntu:~$ sudo apt-get install -y gdisk kpartx parted
```

3. Verificare i parametri del kernel dell'istanza.

```
ubuntu:~$ cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-3.2.0-54-virtual root=UUID=4f392932-ed93-4f8f-
aee7-72bc5bb6ca9d ro console=ttyS0 xen_emul_unplug=unnecessary
```

Si notino le opzioni che seguono i parametri del kernel e del dispositivo root: `ro`, `console=ttyS0` e `xen_emul_unplug=unnecessary`. Le opzioni in uso potrebbero essere diverse.

4. Verificare le voci del kernel in `/boot/grub/menu.lst`.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=hvc0
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
kernel  /boot/memtest86+.bin
```

Si noti che il parametro `console` punta a `hvc0` invece di `ttyS0` e che il parametro `xen_emul_unplug=unnecessary` manca. Anche in questo caso, le opzioni in uso potrebbero essere diverse.

5. Modificare il file `/boot/grub/menu.lst` con l'editor di testo preferito (ad esempio vim o nano) per cambiare la console e aggiungere i parametri individuati precedentemente alle voci di avvio.

```
title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual
root            (hd0)
kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs
 ro console=ttyS0 xen_emul_unplug=unnecessary
initrd          /boot/initrd.img-3.2.0-54-virtual

title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual (recovery mode)
```

```
root            (hd0)
kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro
 single console=ttyS0 xen_emul_unplug=unnecessary
initrd          /boot/initrd.img-3.2.0-54-virtual

title           Ubuntu 12.04.3 LTS, memtest86+
root            (hd0)
kernel          /boot/memtest86+.bin
```

6. Verificare che le voci del kernel ora contengano i parametri corretti.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=ttyS0
 xen_emul_unplug=unnecessary
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
 console=ttyS0 xen_emul_unplug=unnecessary
kernel  /boot/memtest86+.bin
```

7. [Solo per Ubuntu 14.04 e versioni successive] A partire da Ubuntu 14.04, le AMI Ubuntu supportate da instance store utilizzano una tabella di partizione GPT e una partizione EFI separata montata su `/boot/efi`. Il comando ec2-bundle-vol non implica la creazione di un bundle della partizione di avvio, pertanto occorre commentare la voce `/etc/fstab` per la partizione EFI come mostrato nel seguente esempio.

```
LABEL=cloudimg-rootfs   /        ext4   defaults        0 0
#LABEL=UEFI     /boot/efi       vfat    defaults        0 0
/dev/xvdb       /mnt    auto    defaults,nobootwait,comment=cloudconfig 0       2
```

Per creare un'AMI da un'istanza Ubuntu supportata da instance store

Questa procedura presuppone che i prerequisiti indicati in Prerequisiti siano stati soddisfatti.

Nei comandi seguenti, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

1. Caricare le credenziali nell'istanza. Le credenziali servono a garantire l'accesso all'AMI solo da parte dell'utente e da Amazon EC2.

   a. Creare una directory temporanea sull'istanza per le credenziali, come segue:

   ```
   ubuntu:~$ mkdir /tmp/cert
   ```

In questo modo è possibile escludere le proprie credenziali dall'immagine creata.

b. Copiare il certificato X.509 e la chiave privata dal proprio computer alla directory `/tmp/cert` sull'istanza utilizzando uno strumento di copia protetta come scp. L'opzione `-i` *`my-private-key`*`.pem` nel comando scp seguente è la chiave privata da utilizzare per connettersi all'istanza con SSH, non la chiave privata X.509. Ad esempio:

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
```

In alternativa, poiché questi sono file di testo normale, è possibile aprire il certificato e la chiave in un editor di testo e copiarne il contenuto in nuovi file in `/tmp/cert`.

2. Preparare il bundle da caricare in Amazon S3 eseguendo il comando ec2-bundle-vol dall'istanza. Accertarsi di specificare l'opzione `-e` per escludere la directory in cui sono archiviate le proprie credenziali. Per impostazione predefinita, il processo di creazione di bundle esclude i file che possono contenere informazioni sensibili. Tali file includono `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` e `*/.bash_history`. Per includere tutti questi file, utilizzare l'opzione `--no-filter`. Per includere alcuni di questi file, utilizzare l'opzione `--include`.

> **Important**
>
> Per impostazione predefinita, il processo di raggruppamento dell'AMI crea una raccolta codificata di file nella directory `/tmp` che rappresenta il volume root. Se non è disponibile sufficiente spazio libero sul disco in `/tmp` per archiviare il bundle, occorre specificare una posizione diversa per il bundle da archiviare con l'opzione `-d` *`/path/to/bundle/storage`*. Alcune istanze hanno uno storage temporaneo montato su `/mnt` o `/media/ephemeral0` che puoi utilizzare, oppure puoi anche creare, collegare e montare un nuovo volume Amazon (EBS) per archiviare il pacchetto. Per ulteriori informazioni, consulta Creare un volume Amazon EBS nella Guida per l'utente di Amazon EBS.

a. Il comando ec2-bundle-vol deve essere eseguito come root. Per la maggior parte dei comandi, è possibile utilizzare sudo per ottenere autorizzazioni elevate, ma in questo caso occorre eseguire sudo -E su per mantenere le variabili di ambiente.

```
ubuntu:~$ sudo -E su
```

Si noti che il prompt bash ora identifica l'utente come utente root e il simbolo del dollaro è stato sostituito da un tag hash, a segnalare che ci si trova in una shell root:

```
root@ubuntu:#
```

b. Per creare il bundle dell'AMI, eseguire il comando ec2-bundle-vol come segue.

```
root@ubuntu:# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u your_aws_account_id -r x86_64 -e /tmp/
cert --partition gpt
```

> **Important**
>
> Per Ubuntu 14.04 e versioni successive delle istanze HVM, aggiungere il contrassegno `--partition mbr` per creare correttamente il bundle delle istruzioni di avvio; altrimenti, l'AMI appena creata non si avvierà.

Possono essere necessari alcuni minuti per creare l'immagine. Al termine del comando, la directory `tmp` contiene il bundle (`image.manifest.xml`, oltre a più file `image.part.xx`).

c. Uscire dalla shell root.

```
root@ubuntu:# exit
```

3. (Facoltativo) Per aggiungere altri volumi instance store, modificare le mappature dei dispositivi a blocchi nel file `image.manifest.xml` dell'AMI. Per ulteriori informazioni, consulta Mappatura dei dispositivi a blocchi.

a. Creare un backup del file `image.manifest.xml`.

```
ubuntu:~$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

b. Riformattare il file `image.manifest.xml` per renderne più semplice la lettura e la modifica.

```
ubuntu:~$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
image.manifest.xml
```

c. Modificare le mappature dei dispositivi a blocchi in `image.manifest.xml` con un editor di testo. Il seguente esempio mostra una nuova voce del volume instance store *`ephemeral1`*.

```
    <block_device_mapping>
      <mapping>
        <virtual>ami</virtual>
        <device>sda</device>
      </mapping>
      <mapping>
        <virtual>ephemeral0</virtual>
        <device>sdb</device>
      </mapping>
      <mapping>
        <virtual>ephemeral1</virtual>
        <device>sdc</device>
      </mapping>
      <mapping>
        <virtual>root</virtual>
        <device>/dev/sda1</device>
      </mapping>
    </block_device_mapping>
```

d. Salvare il file `image.manifest.xml` e uscire dall'editor di testo.

4. Per caricare il bundle su Amazon S3, eseguire il comando ec2-upload-bundle come segue.

```
ubuntu:~$ ec2-upload-bundle -b DOC-EXAMPLE-BUCKET/bundle_folder/bundle_name -m /
tmp/image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Se si prevede di registrare l'AMI in una regione diversa da US East (N. Virginia), occorre specificare sia la regione di destinazione con l'opzione `--region` che un percorso del

bucket esistente nella regione di destinazione oppure un percorso univoco del bucket che è possibile creare nella regione di destinazione.

5. (Facoltativo) Una volta caricato il bundle su Amazon S3, è possibile rimuoverlo dalla directory `/tmp` sull'istanza utilizzando il seguente comando rm:

```
ubuntu:~$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Se si è specificato un percorso con l'opzione `-d` */path/to/bundle/storage* in Step 2, utilizzare lo stesso percorso riportato sotto invece di `/tmp`.

6. Per registrare l'AMI, eseguire il comando register-image AWS CLI come segue.

```
ubuntu:~$ aws ec2 register-image --image-location DOC-EXAMPLE-
BUCKET/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Se precedentemente si è specificata una regione per il comando ec2-upload-bundle, specificarla nuovamente per questo comando.

7. [Ubuntu 14.04 e versioni successive] Annullare il commento della voce EFI in `/etc/fstab`; altrimenti l'istanza in esecuzione non potrà riavviarsi.

Conversione dell'AMI supportata da instance store in un'AMI Amazon EBS-backed

Puoi convertire un'AMI Linux supportata da instance store di tua proprietà in un'AMI Linux supportata da Amazon EBS.

> **Important**
>
> Non puoi convertire un AMI che non possiedi.

Per convertire un'AMI supportata da instance store in un'AMI Amazon EBS-backed

1. Avviare un'istanza Amazon Linux da un'AMI Amazon EBS-backed. Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza. Le istanze Amazon Linux hanno gli strumenti AWS CLI e AMI preinstallati.
2. Caricare la chiave privata X.509 utilizzata per creare il bundle dell'AMI supportata da instance store sull'istanza. Questa chiave serve a garantire l'accesso all'AMI solo da parte dell'utente e da Amazon EC2.

   a. Creare una directory temporanea sull'istanza per la chiave privata X.509, come segue:

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

   b. Copiare la chiave privata X.509 dal proprio computer nella directory `/tmp/cert` sull'istanza utilizzando uno strumento di copia protetta come scp. Il *my-private-key*parametro nel comando seguente è la chiave privata che usi per connetterti alla tua istanza con SSH. Per esempio:

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   ```

3. Configura le tue variabili ambiente per usare la AWS CLI. Per ulteriori informazioni, consulta Creare una coppia di chiavi.

   a. (Consigliato) Imposta le variabili di ambiente per la chiave di AWS accesso, la chiave segreta e il token di sessione.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   [ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
   ```

   b. Imposta le variabili di ambiente per la chiave di AWS accesso e la chiave segreta.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   ```

4. Preparare un volume Amazon Elastic Block Store (Amazon EBS) per la nuova AMI.

a. Creare un volume EBS vuoto nella stessa zona di disponibilità dell'istanza utilizzando il comando create-volume. Prendere nota dell'ID del volume nell'output del comando.

> **Important**
>
> Questo volume EBS deve essere uguale o maggiore delle dimensioni del volume root instance store originale.

```
[ec2-user ~]$ aws ec2 create-volume --size 10 --region us-west-2 --
availability-zone us-west-2b
```

b. Collegare il volume all'istanza supportata da Amazon EBS utilizzando il comando attach-volume.

```
[ec2-user ~]$ aws ec2 attach-volume --volume-id volume_id --instance-
id instance_id --device /dev/sdb --region us-west-2
```

5. Creare una cartella per il bundle.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Scaricare il bundle dell'AMI basata su instance store in `/tmp/bundle` utilizzando il comando ec2-download-bundle.

```
[ec2-user ~]$ ec2-download-bundle -b DOC-EXAMPLE-BUCKET/bundle_folder/bundle_name -
m image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --privatekey /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Ricostruire il file di immagine dal bundle utilizzando il comando ec2-unbundle.

a. Cambiare directory nella cartella del bundle.

```
[ec2-user ~]$ cd /tmp/bundle/
```

b. Esegui il comando ec2-unbundle.

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. Copiare i file dall'immagine disaggregata nel nuovo volume EBS.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Esaminare il volume cercando eventuali partizioni disaggregate.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Elencare i dispositivi a blocchi per individuare il nome del dispositivo da montare.

```
[ec2-user bundle]$ lsblk
NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
##/dev/sda1 202:1    0   8G  0 part /
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

In questo esempio, la partizione da montare è `/dev/sdb1`, ma il nome del dispositivo probabilmente sarà diverso. Se il volume non è partizionato, il dispositivo da montare sarà simile a `/dev/sdb` (senza una cifra finale della partizione del dispositivo).

11. Creare un punto di montaggio per il nuovo volume EBS e montare il volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Aprire il file `/etc/fstab` sul volume EBS con l'editor di testo preferito (ad esempio vim o nano) e rimuovere tutte le voci dei volumi instance store (temporanei). Poiché il volume EBS è montato su `/mnt/ebs`, il file `fstab` si trova in `/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/     /           ext4    defaults,noatime  1   1
tmpfs       /dev/shm    tmpfs   defaults        0   0
devpts      /dev/pts    devpts  gid=5,mode=620  0   0
sysfs       /sys        sysfs   defaults        0   0
proc        /proc       proc    defaults        0   0
/dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
```

In questo esempio, l'ultima riga deve essere rimossa.

13. Smontare il volume e distaccarlo dall'istanza.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id volume_id --region us-west-2
```

14. Creare un'AMI dal nuovo volume EBS come segue:

    a. Creare uno snapshot del nuovo volume EBS.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
 "your_snapshot_description" --volume-id volume_id
```

    b. Controllare se la snapshot è completa.

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
id snapshot_id
```

    c. Identificare l'architettura del processore, il tipo di virtualizzazione e l'immagine del kernel (`aki`) utilizzati sull'AMI originale tramite il comando describe-images. Per questa fase, è necessario l'ID AMI dell'AMI originale supportata da instance store.

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-id ami-id
 --output text
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
 available public machine aki-fc8f11cc instance-store paravirtual xen
```

    In questo esempio, l'architettura è `x86_64` e l'ID dell'immagine del kernel è `aki-fc8f11cc`. Utilizzare questi valori nella fase seguente. Se l'output del comando sopra include anche un ID `ari`, prenderne nota.

    d. Registrare la nuova AMI con l'ID dello snapshot del nuovo volume EBS e i valori della fase precedente. Se nell'output del comando precedente è incluso un ID `ari`, includerlo nel seguente comando con `--ramdisk-id` *ari_id*.

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
name your_new_ami_name --block-device-mappings DeviceName=device-
name,Ebs={SnapshotId=snapshot_id} --virtualization-type paravirtual --
architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Facoltativo) Dopo avere verificato di poter avviare un'istanza dalla nuova AMI, è possibile eliminare il volume EBS creato per questa procedura.

```
aws ec2 delete-volume --volume-id volume_id
```

Riferimento strumenti AMI

È possibile utilizzare i comandi degli strumenti AMI per creare e gestire le AMI Linux supportate dall'instance store. Per impostare gli strumenti, consultare Configurazione degli strumenti dell'AMI.

Per informazioni sulle chiavi di accesso, consulta Managing access keys for IAM users nella IAM User Guide.

Comandi

- ec2- ami-tools-version
- ec2-bundle-image
- ec2-bundle-vol
- ec2-delete-bundle
- ec2-download-bundle
- ec2-migrate-manifest
- ec2-unbundle
- ec2-upload-bundle
- Opzioni comuni per gli strumenti AMI

ec2- ami-tools-version

Descrizione

Descrive la versione degli strumenti AMI.

Sintassi

`ec2-ami-tools-version`

Output

Informazioni relative alla versione.

Esempio

Questo comando di esempio mostra le informazioni relative alla versione degli strumenti AMI che si stanno utilizzando.

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

ec2-bundle-image

Descrizione

Crea un'AMI Linux supportata dall'instance store da un'immagine del sistema operativo creata in un file di loopback.

Sintassi

ec2-bundle-image -c *path* -k *path* -u *account* -i *path* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [-p *prefix*]

Opzioni

`-c, --cert` path

Il file del certificato a chiave pubblica RSA codificato PEM dell'utente.

Campo obbligatorio: sì

`-k, --privatekey` path

Il percorso di un file chiave RSA codificato PEM. Sarà necessario specificare questa chiave per separare questo bundle, quindi conservarla in un posto sicuro. Tieni presente che la chiave non deve essere registrata sul tuo AWS account.

Campo obbligatorio: sì

`-u, --user` account

L'ID dell' AWS account dell'utente, senza trattini.

Campo obbligatorio: sì

`-i, --image` path

Il percorso dell'immagine da aggiungere al bundle.

Campo obbligatorio: sì

`-d, --destination` path

La directory in cui creare il bundle.

Default: `/tmp`

Campo obbligatorio: no

`--ec2cert` path

Il percorso del certificato della chiave pubblica X.509 Amazon EC2 utilizzato per crittografare il manifest dell'immagine.

Le regioni `us-gov-west-1` e `cn-north-1` utilizzano un certificato di chiave pubblico non predefinito e il percorso di tale certificato deve essere specificato con questa opzione. Il percorso del certificato varia in base al metodo di installazione degli strumenti AMI. Per Amazon Linux, i certificati si trovano in `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se gli strumenti AMI sono stati installati dal file RPM o ZIP in Configurazione degli strumenti dell'AMI, i certificati si trovano in `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obbligatorio: Solo per le regioni `us-gov-west-1` e `cn-north-1`.

`-r, --arch` architecture

Architettura dell'immagine. Se non si fornisce l'architettura sulla riga di comando, verrà richiesta durante l'avvio del raggruppamento.

Valori validi: `i386` | `x86_64`

Campo obbligatorio: no

`--productcodes` code1,code2,...

I codici prodotto da collegare all'immagine al momento della registrazione, separati da virgole.

Campo obbligatorio: no

`-B, --block-device-mapping` mapping

Definisce come i dispositivi a blocchi sono esposti a un'istanza di questa AMI se il suo tipo di istanza supporta il dispositivo specificato.

Specificare un elenco di coppie chiave-valore separato da virgole, in cui ogni chiave è un nome virtuale e ogni valore è il nome del dispositivo corrispondente. Tra i nomi virtuali sono inclusi i seguenti:

- `ami` – Il dispositivo di sistema del file radice visto dall'istanza
- `root` – Il dispositivo di sistema del file radice visto dal kernel
- `swap` – Il dispositivo di scambio visto dall'istanza
- `ephemeralN` – Il volume Nesimo dell'instance store

Campo obbligatorio: no

`-p, --prefix` prefix

Il prefisso del nome del file per i file AMI raggruppati.

Predefinito: Il nome del file immagine. Per esempio, se il percorso dell'immagine è `/var/spool/my-image/version-2/debian.img`, il prefisso predefinito è `debian.img`.

Campo obbligatorio: no

`--kernel` kernel_id

Obsoleta. Utilizzare register-image per impostare il kernel.

Campo obbligatorio: no

`--ramdisk` ramdisk_id

Obsoleta. Utilizzare register-image per impostare il disco RAM se necessario.

Campo obbligatorio: no

Output

Messaggi di stato che descrivono le fasi e lo stato del processo di raggruppamento.

Esempio

Questo esempio crea un'AMI raggruppata da un'immagine del sistema operativo creata in un file di loopback.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
```

```
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

Descrizione

Crea un'AMI Linux supportata dall'instance store comprimendo, crittografando e firmando una copia del volume dispositivo root per l'istanza.

Amazon EC2 tenta di ereditare codici prodotto, impostazioni del kernel, impostazioni del disco RAM e mappature dei dispositivi a blocchi dall'istanza.

Per impostazione predefinita, il processo di raggruppamento esclude i file che possono contenere informazioni sensibili. Tali file includono `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` e `*/.bash_history`. Per includere tutti questi file, utilizzare l'opzione `--no-filter`. Per includere alcuni di questi file, utilizzare l'opzione `--include`.

Per ulteriori informazioni, consulta Creazione di un'AMI Linux supportata da un instance store.

Sintassi

ec2-bundle-vol -c *path* -k *path* -u *account* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [--all] [-e

directory1,_directory2_,...] [-i _file1_,_file2_,...] [--no-filter] [-p _prefix_] [-s _size_] [--[no-]inherit] [-v _volume_] [-P _type_] [-S _script_] [--fstab _path_] [--generate-fstab] [--grub-config _path_]

Opzioni

`-c, --cert` path

Il file del certificato a chiave pubblica RSA codificato PEM dell'utente.

Campo obbligatorio: sì

`-k, --privatekey` path

Il percorso del file chiave RSA codificato PEM dell'utente.

Campo obbligatorio: sì

`-u, --user` account

L'ID dell' AWS account dell'utente, senza trattini.

Campo obbligatorio: sì

`-d, --destination` destination

La directory in cui creare il bundle.

Default: `/tmp`

Campo obbligatorio: no

`--ec2cert` path

Il percorso del certificato della chiave pubblica X.509 Amazon EC2 utilizzato per crittografare il manifest dell'immagine.

Le regioni `us-gov-west-1` e `cn-north-1` utilizzano un certificato di chiave pubblico non predefinito e il percorso di tale certificato deve essere specificato con questa opzione. Il percorso del certificato varia in base al metodo di installazione degli strumenti AMI. Per Amazon Linux, i certificati si trovano in `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se gli strumenti AMI sono stati installati dal file RPM o ZIP in Configurazione degli strumenti dell'AMI, i certificati si trovano in `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obbligatorio: Solo per le regioni `us-gov-west-1` e `cn-north-1`.

`-r, --arch` architecture

L'architettura dell'immagine. Se non la si fornisce sulla riga di comando, verrà richiesto di fornirla durante l'avvio del raggruppamento.

Valori validi: `i386` | `x86_64`

Campo obbligatorio: no

`--productcodes` code1,code2,...

I codici prodotto da collegare all'immagine al momento della registrazione, separati da virgole.

Campo obbligatorio: no

`-B, --block-device-mapping` mapping

Definisce come i dispositivi a blocchi sono esposti a un'istanza di questa AMI se il suo tipo di istanza supporta il dispositivo specificato.

Specificare un elenco di coppie chiave-valore separato da virgole, in cui ogni chiave è un nome virtuale e ogni valore è il nome del dispositivo corrispondente. Tra i nomi virtuali sono inclusi i seguenti:

- `ami` – Il dispositivo di sistema del file radice visto dall'istanza
- `root` – Il dispositivo di sistema del file radice visto dal kernel
- `swap` – Il dispositivo di scambio visto dall'istanza
- `ephemeralN` – Il volume Nesimo dell'instance store

Campo obbligatorio: no

`-a, --all`

Raggruppare tutte le directory, comprese quelle su sistemi di file montati in remoto.

Campo obbligatorio: no

`-e, --exclude` directory1,directory2,...

Un elenco di percorsi e file di directory assoluti da escludere dall'operazione di creazione di bundle. Questo parametro sostituisce l'opzione `--all` . Quando si specifica l'opzione di

esclusione, le directory e sottodirectory elencate con il parametro non verranno raggruppate con il volume.

Campo obbligatorio: no

`-i, --include` file1,file2,...

Un elenco dei file da includere nell'operazione di creazione di bundle. I file specificati sarebbero altrimenti esclusi dall'AMI in quanto potrebbero contenere informazioni sensibili.

Campo obbligatorio: no

`--no-filter`

Se specificato, non verranno esclusi file dall'AMI in quanto potrebbero contenere informazioni sensibili.

Campo obbligatorio: no

`-p, --prefix` prefix

Il prefisso del nome del file per i file AMI raggruppati.

Impostazione predefinita: `image`

Campo obbligatorio: no

`-s, --size` size

La dimensione, in MB (1024 x 1024 byte), del file di immagine da creare. La dimensione massima è 10240 MB.

Impostazione predefinita: 10240

Campo obbligatorio: no

`--[no-]inherit`

Indica se l'immagine deve ereditare i metadati dell'istanza (l'impostazione predefinita è ereditare). Il raggruppamento non va a buon fine se si attiva `--inherit` ma i metadati dell'istanza non sono accessibili.

Campo obbligatorio: no

`-v, --volume` volume

Il percorso assoluto del volume montato da cui creare il bundle.

Impostazione predefinita: la directory radice (/)

Campo obbligatorio: no

`-P, --partition` type

Indica se l'immagine del disco deve utilizzare una tabella di partizione. Se non si specifica un tipo di tabella di partizione, quello predefinito è il tipo utilizzato dal principale dispositivo a blocchi del volume, se applicabile, altrimenti quello predefinito è `gpt`.

Valori validi: `mbr` | `gpt` | `none`

Campo obbligatorio: no

`-S, --script` script

Uno script di personalizzazione da eseguire appena prima del raggruppamento. Lo script deve aspettarsi un argomento singolo, il punto di montaggio del volume.

Campo obbligatorio: no

`--fstab` path

Il percorso di fstab da aggiungere in bundle all'immagine. Se questo non viene specificato, Amazon EC2 raggruppa /etc/fstab.

Campo obbligatorio: no

`--generate-fstab`

Raggruppa il volume tramite un fstab fornito da Amazon EC2.

Campo obbligatorio: no

`--grub-config`

Il percorso di un file di configurazione di sgombero alternato da aggiungere in bundle all'immagine. Per impostazione predefinita, `ec2-bundle-vol` si aspetta che `/boot/grub/menu.lst` o `/boot/grub/grub.conf` esistano nell'immagine clonata. Questa opzione consente di indicare un percorso di un file di configurazione di sgombero alternato che poi verrà copiato sui predefiniti (se presenti).

Campo obbligatorio: no

`--kernel` kernel_id

Obsoleta. Utilizzare register-image per impostare il kernel.

Campo obbligatorio: no

`--ramdisk`ramdisk_id

Obsoleta. Utilizzare register-image per impostare il disco RAM se necessario.

Campo obbligatorio: no

Output

Messaggi di stato che descrivono le fasi e lo stato del raggruppamento.

Esempio

Questo esempio crea un'AMI raggruppata comprimendo, crittografando e firmando uno snapshot del sistema di file radice della macchina locale.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c
 cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
  Copying / into the image file /mnt/image...
  Excluding:
       sys
       dev/shm
       proc
       dev/pts
       proc/sys/fs/binfmt_misc
       dev
       media
       mnt
       proc
       sys
       tmp/image
       mnt/img-mnt
  1+0 records in
  1+0 records out
  mke2fs 1.38 (30-Jun-2005)
  warning: 256 blocks unused.

  Splitting /mnt/image.gz.crypt...
  Created image.part.00
```

```
Created image.part.01
Created image.part.02
Created image.part.03
...
Created image.part.22
Created image.part.23
Generating digests for each part...
Digests generated.
Creating bundle manifest...
Bundle Volume complete.
```

ec2-delete-bundle

Descrizione

Elimina il bundle specificato dall'archiviazione Amazon S3. Dopo aver eliminato un bundle, non è possibile avviare istanze dall'AMI corrispondente.

Sintassi

ec2-delete-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* [-t *token*] [--url *url*] [--region *region*] [--sigv *version*] [-m *path*] [-p *prefix*] [--clear] [--retry] [-y]

Opzioni

`-b, --bucket` bucket

Il nome del bucket Amazon S3 che contiene l'AMI raggruppata, seguito da un prefisso facoltativo di percorso delimitato da "/"

Campo obbligatorio: sì

`-a, --access-key` access_key_id

L'ID della chiave di AWS accesso.

Campo obbligatorio: sì

`-s, --secret-key` secret_access_key

La chiave di accesso AWS segreta.

Campo obbligatorio: sì

`-t, --delegation-token` token

Il token di delega da passare alla AWS richiesta. Per ulteriori informazioni, consulta Utilizzo di credenziali di sicurezza temporanee.

Obbligatorio: Solo quando si utilizzano credenziali di sicurezza temporanee.

Predefinito: Il valore della variabile ambientale `AWS_DELEGATION_TOKEN` (se impostata).

`--region`region

La regione da utilizzare nella firma di richiesta.

Impostazione predefinita: `us-east-1`

Obbligatorio: Obbligatorio se si utilizza la versione 4 di firma

`--sigv`version

La versione della firma da utilizzare durante la firma della richiesta.

Valori validi: `2` | `4`

Default: `4`

Campo obbligatorio: no

`-m, --manifest`path

Il percorso del file manifest.

Obbligatorio: È necessario specificare `--prefix` o `--manifest`.

`-p, --prefix` prefix

Il prefisso del nome del file AMI raggruppato. Fornire il prefisso completo. Per esempio, se il prefisso è image.img, utilizzare `-p image.img` e non `-p image`.

Obbligatorio: È necessario specificare `--prefix` o `--manifest`.

`--clear`

Cancella il bucket Amazon S3 se è vuoto dopo aver eliminato il bundle specificato.

Campo obbligatorio: no

`--retry`

Ripete automaticamente i tentativi su tutti gli errori Amazon S3, fino a cinque volte per operazione.

Campo obbligatorio: no

`-y, --yes`

Suppone automaticamente che la risposta a tutte le richieste sia sì.

Campo obbligatorio: no

Output

Amazon EC2 visualizza i messaggi di stato che indicano gli stadi e lo stato del processo di eliminazione.

Esempio

In questo esempio viene eliminato un bundle da Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b DOC-EXAMPLE-BUCKET -a your_access_key_id -
s your_secret_access_key
Deleting files:
DOC-EXAMPLE-BUCKET/image.manifest.xml
DOC-EXAMPLE-BUCKET/image.part.00
DOC-EXAMPLE-BUCKET/image.part.01
DOC-EXAMPLE-BUCKET/image.part.02
DOC-EXAMPLE-BUCKET/image.part.03
DOC-EXAMPLE-BUCKET/image.part.04
DOC-EXAMPLE-BUCKET/image.part.05
DOC-EXAMPLE-BUCKET/image.part.06
Continue? [y/n]
y
Deleted DOC-EXAMPLE-BUCKET/image.manifest.xml
Deleted DOC-EXAMPLE-BUCKET/image.part.00
Deleted DOC-EXAMPLE-BUCKET/image.part.01
Deleted DOC-EXAMPLE-BUCKET/image.part.02
Deleted DOC-EXAMPLE-BUCKET/image.part.03
Deleted DOC-EXAMPLE-BUCKET/image.part.04
Deleted DOC-EXAMPLE-BUCKET/image.part.05
Deleted DOC-EXAMPLE-BUCKET/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Descrizione

Scarica le AMIs Linux supportate dall'archivio istanza specificato dall'archiviazione Amazon S3.

Sintassi

ec2-download-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* -k *path* [--url *url*] [--region *region*] [--sigv *version*] [-m *file*] [-p *prefix*] [-d *directory*] [--retry]

Opzioni

`-b, --bucket` bucket

Il nome del bucket Amazon S3 dove è posizionato il bundle, seguito da un prefisso facoltativo di percorso delimitato da "/".

Campo obbligatorio: sì

`-a, --access-key` access_key_id

L'ID della chiave di AWS accesso.

Campo obbligatorio: sì

`-s, --secret-key` secret_access_key

La chiave di accesso AWS segreta.

Campo obbligatorio: sì

`-k, --privatekey` path

La chiave privata utilizzata per decrittografare il manifest.

Campo obbligatorio: sì

`--url` url

L'URL di servizio Amazon S3.

Default: `https://s3.amazonaws.com/`

Campo obbligatorio: no

`--region` region

La regione da utilizzare nella firma di richiesta.

Impostazione predefinita: `us-east-1`

Obbligatorio: Obbligatorio se si utilizza la versione 4 di firma

`--sigv` Versione

La versione della firma da utilizzare durante la firma della richiesta.

Valori validi: `2` | `4`

Default: `4`

Campo obbligatorio: no

`-m, --manifest` file

Il nome del file manifest (senza il percorso). Si consiglia di specificare il manifest (`-m`) o un prefisso (`-p`).

Campo obbligatorio: no

`-p, --prefix` prefix

Il prefisso del nome del file per i file AMI raggruppati.

Impostazione predefinita: `image`

Campo obbligatorio: no

`-d, --directory` directory

La directory dove viene salvato il bundle scaricato. La directory deve esistere.

Predefinito: La directory di lavoro corrente.

Campo obbligatorio: no

`--retry`

Ripete automaticamente i tentativi su tutti gli errori Amazon S3, fino a cinque volte per operazione.

Campo obbligatorio: no

Output

Vengono visualizzati i messaggi di stato che indicano le varie fasi del processo di download.

Esempio

Questo esempio crea la directory `bundled` (tramite il comando di Linux mkdir) e scarica il bundle dal bucket Amazon S3 `DOC-EXAMPLE-BUCKET`.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b DOC-EXAMPLE-BUCKET/bundles/bundle_name
 -m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from DOC-EXAMPLE-BUCKET to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from DOC-EXAMPLE-BUCKET/bundles/bundle_name to mybundle/
image.part.00 ...
Downloaded image.part.00 from DOC-EXAMPLE-BUCKET
Downloading part image.part.01 from DOC-EXAMPLE-BUCKET/bundles/bundle_name to mybundle/
image.part.01 ...
Downloaded image.part.01 from DOC-EXAMPLE-BUCKET
Downloading part image.part.02 from DOC-EXAMPLE-BUCKET/bundles/bundle_name to mybundle/
image.part.02 ...
Downloaded image.part.02 from DOC-EXAMPLE-BUCKET
Downloading part image.part.03 from DOC-EXAMPLE-BUCKET/bundles/bundle_name to mybundle/
image.part.03 ...
Downloaded image.part.03 from DOC-EXAMPLE-BUCKET
Downloading part image.part.04 from DOC-EXAMPLE-BUCKET/bundles/bundle_name to mybundle/
image.part.04 ...
Downloaded image.part.04 from DOC-EXAMPLE-BUCKET
Downloading part image.part.05 from DOC-EXAMPLE-BUCKET/bundles/bundle_name to mybundle/
image.part.05 ...
Downloaded image.part.05 from DOC-EXAMPLE-BUCKET
Downloading part image.part.06 from DOC-EXAMPLE-BUCKET/bundles/bundle_name to mybundle/
image.part.06 ...
Downloaded image.part.06 from DOC-EXAMPLE-BUCKET
```

ec2-migrate-manifest

Descrizione

Modifica un'AMI Linux supportata da instance store (per esempio, il suo certificato, il kernel o il disco RAM) in modo che essa supporti una regione diversa.

Sintassi

```
ec2-migrate-manifest -c path -k path -m path {(-a access_key_id -
s secret_access_key --region region) | (--no-mapping)} [--ec2cert
ec2_cert_path] [--kernel kernel-id] [--ramdisk ramdisk_id]
```

Opzioni

`-c, --cert` path

Il file del certificato a chiave pubblica RSA codificato PEM dell'utente.

Campo obbligatorio: sì

`-k, --privatekey` path

Il percorso del file chiave RSA codificato PEM dell'utente.

Campo obbligatorio: sì

`--manifest` path

Il percorso del file manifest.

Campo obbligatorio: sì

`-a, --access-key` access_key_id

L'ID della chiave di AWS accesso.

Obbligatorio: Obbligatorio se si utilizza la mappatura automatica.

`-s, --secret-key` secret_access_key

La chiave di accesso AWS segreta.

Obbligatorio: Obbligatorio se si utilizza la mappatura automatica.

`--region` region

La regione da cercare nel file di mappatura.

Obbligatorio: Obbligatorio se si utilizza la mappatura automatica.

`--no-mapping`

Disattiva la mappatura automatica dei kernel e dei dischi RAM.

Durante la migrazione, Amazon EC2 sostituisce il kernel e il disco RAM nel file manifest con un kernel e un disco RAM progettati per la regione di destinazione. A meno che non venga fornito il parametro `--no-mapping`, `ec2-migrate-bundle` deve utilizzare le operazioni `DescribeRegions` e `DescribeImages` per eseguire le mappature automatiche.

Obbligatorio: Obbligatorio se non si forniscono le opzioni `-a`, `-s` e `--region` utilizzate per la mappatura automatica.

`--ec2cert` path

Il percorso del certificato della chiave pubblica X.509 Amazon EC2 utilizzato per crittografare il manifest dell'immagine.

Le regioni `us-gov-west-1` e `cn-north-1` utilizzano un certificato di chiave pubblico non predefinito e il percorso di tale certificato deve essere specificato con questa opzione. Il percorso del certificato varia in base al metodo di installazione degli strumenti AMI. Per Amazon Linux, i certificati si trovano in `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se gli strumenti AMI sono stati installati dal file ZIP in Configurazione degli strumenti dell'AMI, i certificati si trovano in `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obbligatorio: Solo per le regioni `us-gov-west-1` e `cn-north-1`.

`--kernel` kernel_id

L'ID del kernel da selezionare.

> **Important**
>
> È consigliabile utilizzare PV-GRUB invece dei kernel e dei dischi RAM. Per ulteriori informazioni, consulta Kernel forniti dall'utente nella Guida per l'utente di Amazon Linux 2.

Campo obbligatorio: no

`--ramdisk` ramdisk_id

L'ID del disco RAM da selezionare.

> **Important**
>
> È consigliabile utilizzare PV-GRUB invece dei kernel e dei dischi RAM. Per ulteriori informazioni, consulta Kernel forniti dall'utente nella Guida per l'utente di Amazon Linux 2.

Campo obbligatorio: no

Output

Messaggi di stato che descrivono le fasi e lo stato del processo di raggruppamento.

Esempio

Questo esempio copia l'AMI specificata nel manifest `my-ami.manifest.xml` dagli Stati Uniti all'Unione Europea.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml
 --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --region eu-west-1

Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

Descrizione

Ricrea il bundle da un'AMI Linux supportata dall'instance store.

Sintassi

ec2-unbundle -k *path* -m *path* [-s *source_directory*] [-d *destination_directory*]

Opzioni

`-k, --privatekey` path

Il percorso del file chiave RSA codificato PEM.

Campo obbligatorio: sì

`-m, --manifest` path

Il percorso del file manifest.

Campo obbligatorio: sì

`-s, --source` source_directory

La directory che contiene il bundle.

Predefinita: La directory attuale.

Campo obbligatorio: no

`-d, --destination` destination_directory

La directory in cui disaggregare l'AMI. La directory di destinazione deve esistere.

Predefinita: La directory attuale.

Campo obbligatorio: no

Esempio

Questo esempio Linux e UNIX disaggrega l'AMI specificata nel file `image.manifest.xml`.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

Output

Vengono visualizzati i messaggi di stato che indicano le varie fasi del processo di disaggregazione.

ec2-upload-bundle

Descrizione

Carica il bundle per un'AMI Linux supportata da un archivio istanza in Amazon S3 e imposta le liste di controllo accessi (ACL) appropriate sugli oggetti caricati. Per ulteriori informazioni, consulta Creazione di un'AMI Linux supportata da un instance store.

> **Note**
>
> Per caricare oggetti in un bucket S3 per l'AMI Linux supportata da archivi istanze, è necessario abilitare le ACL per il bucket. In caso contrario, Amazon EC2 non sarà in grado di

impostare le ACL sugli oggetti da caricare. Se il bucket di destinazione utilizza l'impostazione applicata dal proprietario del bucket per S3 Object Ownership, ciò non funzionerà perché le ACL sono disabilitate. Per maggiori informazioni, consultare Controllo della proprietà degli oggetti caricati tramite S3 Object Ownership.

Sintassi

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t
token] -m path [--url url] [--region region] [--sigv version] [--acl acl]
[-d directory] [--part part] [--retry] [--skipmanifest]
```

Opzioni

`-b, --bucket` bucket

Il nome del bucket Amazon S3 dove memorizzare il bundle, seguito da un prefisso facoltativo di percorso delimitato da "/". Se il bucket non esiste, viene creato se il nome del bucket è disponibile. Inoltre, se il bucket non esiste e la versione degli strumenti AMI è 1.5.18 o successiva, questo comando imposta le ACL per il bucket.

Campo obbligatorio: sì

`-a, --access-key` access_key_id

L'ID della tua chiave di AWS accesso.

Campo obbligatorio: sì

`-s, --secret-key` secret_access_key

La tua chiave di accesso AWS segreta.

Campo obbligatorio: sì

`-t, --delegation-token` token

Il token di delega da passare alla AWS richiesta. Per ulteriori informazioni, consulta Utilizzo di credenziali di sicurezza temporanee.

Obbligatorio: Solo quando si utilizzano credenziali di sicurezza temporanee.

Predefinito: Il valore della variabile ambientale `AWS_DELEGATION_TOKEN` (se impostata).

`-m, --manifest` path

Il percorso del file manifest. Il file manifest viene creato durante il processo di raggruppamento e si può trovare nella directory che contiene il bundle.

Campo obbligatorio: sì

`--url` url

Obsoleta. Invece, utilizzare l'opzione `--region` a meno che il bucket non sia limitato alla posizione EU (e non `eu-west-1`). Il contrassegno `--location` è l'unico modo per mirare a quella specifica limitazione di posizione.

L'URL di servizio endpoint Amazon S3.

Default: `https://s3.amazonaws.com/`

Campo obbligatorio: no

`--region` region

La regione da utilizzare nella firma di richiesta per il bucket S3 di destinazione.

- Se il bucket non esiste e non si specifica una regione, lo strumento crea il bucket senza un vincolo di posizione (in `us-east-1`).
- Se il bucket non esiste e si specifica una regione, lo strumento crea il bucket nella regione specificata.
- Se il bucket esiste e non si specifica una regione, lo strumento utilizza la posizione del bucket.
- Se il bucket esiste e si specifica `us-east-1` come regione, lo strumento utilizza la posizione reale del bucket senza alcun messaggio di errore e senza che i file corrispondenti esistenti vengano sovrascritti.
- Se il bucket esiste e si specifica una regione (diversa da `us-east-1`) che non corrisponde alla posizione reale del bucket, lo strumento dà un errore.

Se il bucket è limitato alla posizione EU (e non `eu-west-1`), utilizzare il contrassegno `--location`. Il contrassegno `--location` è l'unico modo per mirare a quella specifica limitazione di posizione.

Impostazione predefinita: `us-east-1`

Obbligatorio: Obbligatorio se si utilizza la versione 4 di firma

`--sigv` Versione

La versione della firma da utilizzare durante la firma della richiesta.

Valori validi: `2` | `4`

Default: `4`

Campo obbligatorio: no

`--acl` acl

La policy della lista di controllo accessi dell'immagine raggruppata.

Valori validi: `public-read` | `aws-exec-read`

Default: `aws-exec-read`

Campo obbligatorio: no

`-d, --directory` directory

La directory che contiene le parti dell'AMI raggruppata.

Predefinito: La directory che contiene il file manifest (consultare l'opzione `-m`).

Campo obbligatorio: no

`--part` part

Inizia a caricare la parte specificata e tutte le parti successive. Ad esempio, `--part 04`.

Campo obbligatorio: no

`--retry`

Ripete automaticamente i tentativi su tutti gli errori Amazon S3, fino a cinque volte per operazione.

Campo obbligatorio: no

`--skipmanifest`

Non carica il manifest.

Campo obbligatorio: no

`--location` location

Obsoleta. Invece, utilizzare l'opzione `--region`, a meno che il bucket non sia limitato alla posizione EU (e non `eu-west-1`). Il contrassegno `--location` è l'unico modo per mirare a quella specifica limitazione di posizione.

La limitazione di posizione del bucket Amazon S3 di destinazione. Se il bucket esiste e si specifica una posizione che non corrisponde alla posizione reale del bucket, lo strumento dà un errore. Se il bucket esiste e non si specifica una posizione, lo strumento utilizza la posizione del bucket. Se il bucket non esiste e si specifica una posizione, lo strumento crea il bucket nella posizione specificata. Se il bucket non esiste e non si specifica una posizione, lo strumento crea il bucket senza un vincolo di posizione (in `us-east-1`).

Predefinito: Se `--region` viene specificato, viene impostata la posizione per quella regione specificata. Se `--region` non viene specificata, la posizione predefinita è `us-east-1`.

Campo obbligatorio: no

Output

Amazon EC2 visualizza i messaggi di stato che indicano gli stadi e lo stato del processo di caricamento.

Esempio

Questo esempio carica il bundle specificato dal manifest `image.manifest.xml`.

```
[ec2-user ~]$ ec2-upload-bundle -b DOC-EXAMPLE-BUCKET/bundles/bundle_name -m
 image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket DOC-EXAMPLE-BUCKET ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
```

```
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

Opzioni comuni per gli strumenti AMI

La maggior parte degli strumenti AMI accettano i parametri facoltativi seguenti.

`--help, -h`

Visualizza il messaggio di aiuto.

`--version`

Visualizza la versione e l'avviso di copyright.

`--manual`

Visualizza l'immissione manuale.

`--batch`

Funziona in modalità batch, sopprimendo le richieste interattive.

`--debug`

Visualizza le informazioni che possono essere utili durante la risoluzione dei problemi.

Creare un'AMI con Windows Sysprep

Lo strumento System Preparation (Sysprep) di Microsoft semplifica il processo di duplicazione di un'installazione personalizzata di Windows. È possibile utilizzare Sysprep per creare un'immagine Amazon Machine Image (AMI) standardizzata. Da tale immagine standardizzata, sarà quindi possibile creare nuove istanze Amazon EC2 per Windows.

Ti consigliamo di utilizzare EC2 Image Builder per automatizzare la creazione, la gestione e l'implementazione di immagini server personalizzate up-to-date, sicure e «dorate» preinstallate e preconfigurate con software e impostazioni.

Se si utilizza Windows Sysprep per creare un'AMI standardizzata, si consiglia di eseguire Sysprep con. EC2Launch v2 Se usi ancora gli agenti EC2config (Windows Server 2012 R2 e versioni precedenti) o EC2Launch (Windows Server 2016 e 2019), consulta la documentazione relativa all'utilizzo di Sysprep con EC2config e EC2Launch riportata di seguito.

> **Important**
>
> Non si deve utilizzare Sysprep per creare il backup di un'istanza. Sysprep rimuove le informazioni specifiche di sistema. La rimozione di tali informazioni può avere conseguenze indesiderate sul backup di un'istanza.

Per risolvere i problemi relativi a Sysprep, vedere Risolvi i problemi di Sysprep con le istanze di Windows.

Indice

Prima di iniziare

- Prima di eseguire Sysprep, ti consigliamo di rimuovere tutti gli account utente locali e tutti i profili account diversi da un account amministratore singolo in cui Sysprep verrà eseguito. Se esegui Sysprep con account e profili aggiuntivi, si può verificare un comportamento imprevisto, inclusi perdita di dati del profilo o errore di completamento Sysprep.
- Scopri di più su Sysprep in Microsoft. TechNet
- Informazioni sui ruoli server supportati per Sysprep.

Esecuzione di Sysprep con EC2Launch v2

Questa sezione contiene dettagli sulle diverse fasi di esecuzione di Sysprep e sulle attività eseguite dal servizio EC2Launch v2 durante la preparazione dell'immagine. Include anche le fasi per creare un'AMI standardizzata utilizzando Sysprep con il servizio EC2Launch v2.

Sysprep con argomenti EC2Launch v2

Fasi di Sysprep

L'esecuzione di Sysprep avviene nelle fasi seguenti:

- Generalize (Generalizzazione): lo strumento rimuove le informazioni e le configurazioni specifiche dell'immagine. Per esempio, Sysprep rimuove l'identificatore di sicurezza (SID), il nome del computer, i log di eventi e i driver specifici, per citarne alcune. Dopo il completamento di questa fase, il sistema operativo (SO) è pronto a creare un'AMI.

  > **Note**
  >
  > Quando esegui Sysprep con il servizio EC2Launch v2, il sistema impedisce la rimozione dei driver perché `PersistAllDeviceInstalls` è impostato su true per impostazione predefinita.

- Specialize (Specializzazione): Plug and Play esegue un'analisi del computer e installa i driver per ogni dispositivo rilevato. Lo strumento genera i requisiti del SO, quali il nome del computer e il SID. Facoltativamente, è possibile eseguire comandi in questa fase.
- Out-of-Box Experience (OOBE): il sistema esegue una versione abbreviata della configurazione di Windows e ti richiede utente di inserire informazioni come la lingua di sistema, il fuso orario e un'organizzazione registrata. Quando esegui Sysprep con EC2Launch v2, il file di risposta automatizza questa fase.

Azioni di Sysprep

Sysprep ed EC2Launch v2 eseguono le seguenti operazioni durante la preparazione di un'immagine.

1. Quando scegli Shutdown with Sysprep (Arresta con Sysprep) nella finestra di dialogo EC2Launch Service Properties (Proprietà servizio EC2), il sistema esegue il comando `ec2launch sysprep`.
2. EC2Launch v2 modifica il contenuto del file `unattend.xml` leggendo il valore del Registro di sistema in `HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName`. Il file si trova nella directory seguente: `C:\ProgramData\Amazon\EC2Launch\sysprep`.

3. Il sistema esegue il comando `BeforeSysprep.cmd`. Tale comando crea una chiave di registro come indicato di seguito:

   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f

   La chiave di registro disattiva le connessioni RDP fino a che non vengono riattivate. La disattivazione delle connessioni RDP è una misura di sicurezza necessaria in quanto, nella prima sessione di avvio dopo l'esecuzione di Sysprep, RDP consente le connessioni per un breve periodo di tempo in cui la password dell'Amministratore è vuota.
4. Il servizio EC2Launch v2 chiama Sysprep attraverso l'esecuzione dei comandi seguenti:

   sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml"

Fase di generalizzazione

- EC2Launch v2 rimuove le informazioni e le configurazioni specifiche dell'immagine, quali il nome del computer e l'SID. Se l'istanza è un membro di un dominio, essa viene rimossa dal dominio. Il file di risposta `unattend.xml` include le impostazioni seguenti che riguardano questa fase:
  - PersistAllDeviceInstalls: questa impostazione impedisce a Windows Setup di rimuovere e riconfigurare i dispositivi, il che accelera il processo di preparazione delle immagini perché le AMI Amazon richiedono l'esecuzione di determinati driver e il nuovo rilevamento di tali driver richiederebbe tempo.
  - DoNotCleanUpNonPresentDevices: questa impostazione conserva le informazioni Plug and Play per i dispositivi attualmente non presenti.
- Sysprep arresta l'SO quando si prepara alla creazione dell'AMI. Il sistema avvia una nuova istanza o avvia l'istanza originale.

Fase di specializzazione

Il sistema genera i requisiti specifici del SO, come un nome del computer e un SID. Il sistema esegue anche le azioni seguenti, in base alle configurazioni specificate nel file di risposta `unattend.xml`.

- CopyProfile: Sysprep può essere configurato per eliminare tutti i profili utente, incluso il profilo Administrator integrato. Questa impostazione mantiene l'account Amministratore integrato cosicché

qualsiasi personalizzazione effettuata su tale account venga trasferita alla nuova immagine. Il valore predefinito è `True`.

CopyProfilesostituisce il profilo predefinito con il profilo di amministratore locale esistente. Tutti gli account connessi dopo l'esecuzione di Sysprep riceveranno una copia del profilo e del suo contenuto al primo accesso.

Se non si dispone di personalizzazioni specifiche del profilo utente che si desidera trasferire alla nuova immagine, modificare questa impostazione in `False`. Sysprep rimuoverà tutti i profili utente, risparmiando tempo e spazio su disco.

- TimeZone: per impostazione predefinita, il fuso orario è impostato su Coordinate Universal Time (UTC).
- Synchronous command with order 1 (Comando sincrono con ordine 1): il sistema esegue il comando seguente che abilita l'account amministratore e specifica il requisito della password:

```
net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /
PASSWORDREQ:YES
```

- Synchronous command with order 2 (Comando sincrono con ordine 2): il sistema codifica la password dell'amministratore. Questa misura di sicurezza è progettata per impedire che l'istanza sia accessibile dopo il completamento di Sysprep se non è stata configurata l'attività. `setAdminAccount`

  Il sistema esegue il comando seguente dalla directory locale del Launch Agent (). `C:\Program Files\Amazon\EC2Launch\`

```
EC2Launch.exe internal randomize-password --username Administrator
```

- Per abilitare le connessioni desktop remote, il sistema imposta la chiave di `fDenyTSConnections` registro di Terminal Server su false.

Fase Configurazione guidata

1. Il sistema specifica le seguenti configurazioni utilizzando il file di risposta di EC2Launch v2:
   - `<InputLocale>en-US</InputLocale>`
   - `<SystemLocale>en-US</SystemLocale>`
   - `<UILanguage>en-US</UILanguage>`

- `<UserLocale>en-US</UserLocale>`
- `<HideEULAPage>true</HideEULAPage>`
- `<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>`
- `<ProtectYourPC>3</ProtectYourPC>`
- `<BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>`
- `<TimeZone>UTC</TimeZone>`
- `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`
- `<RegisteredOwner>EC2</RegisteredOwner>`

> **Note**
>
> Durante le fasi di generalizzazione e di specializzazione, EC2Launch v2 monitora lo stato del SO. Se EC2Launch v2 rileva che il SO si trova in una fase di Sysprep, pubblica il messaggio seguente al log di sistema:
> Windows è in fase di configurazione. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Il sistema esegue EC2Launch v2.

Dopo Sysprep

Al termine di Sysprep, EC2Launch v2 invia il seguente messaggio all'output della console:

```
Windows sysprep configuration complete.
```

Quindi EC2Launch v2 effettua le seguenti operazioni:

1. Legge il contenuto del file `agent-config.yml` ed esegue le attività configurate.
2. Esegue tutte le attività della fase `preReady`.
3. Al termine, invia un messaggio `Windows is ready` ai log di sistema dell'istanza.
4. Esegue tutte le attività della fase `PostReady`.

Per ulteriori informazioni su EC2Launch v2, consulta Configurare un'istanza Windows tramite EC2Launch v2.

Esecuzione di Sysprep con EC2Launch v2

Utilizza la procedura seguente per creare un'AMI standardizzata utilizzando Sysprep con EC2Launch v2.

1. Nella console Amazon EC2, individua un'AMI che desideri duplicare.
2. Avviare l'istanza Windows e connettersi a essa.
3. Personalizzarla.
4. Dal menu Start di Windows, cerca e scegli le impostazioni di Amazon EC2Launch. Per ulteriori informazioni sulle opzioni e sulle impostazioni della finestra di dialogo Amazon EC2Launch settings (Impostazioni di Amazon EC2Launch), consulta Impostazioni di EC2Launch v2.
5. Seleziona Shutdown with Sysprep (Arresto con Sysprep) o Shutdown without Sysprep (Arresto senza Sysprep).

Quando viene chiesto di confermare l'esecuzione di Sysprep e l'arresto dell'istanza, fare clic su Sì. EC2Launch v2 esegue Sysprep. Quindi verrai disconnesso dall'istanza e l'istanza verrà arrestata. Se si controlla la pagina Instances (Istanze) nella console Amazon EC2, lo stato dell'istanza cambia da `Running` a `Stopping` a `Stopped`. A questo punto, è opportuno creare un'AMI da questa istanza.

È possibile richiamare manualmente lo strumento Sysprep dalla riga di comando con il comando seguente:

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Utilizzare Sysprep con EC2Launch

EC2Launch offre un file di risposta predefinito e dei file batch per Sysprep che automatizzano e proteggono il processo di preparazione delle immagini sull'AMI. La modifica di tali file è facoltativa. Per impostazione predefinita, questi file si trovano nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.

> **Important**
>
> Non si deve utilizzare Sysprep per creare il backup di un'istanza. Sysprep rimuove le informazioni specifiche di sistema. La rimozione di tali informazioni può avere conseguenze indesiderate sul backup di un'istanza.

Argomenti di Sysprep con EC2Launch

- File batch e di risposta EC2Launch per Sysprep
- Utilizzo di Sysprep con EC2Launch
- Aggiornamento di routing KMS/metadati per il Server 2016 o versione successiva quando si lancia un'AMI personalizzata

File batch e di risposta EC2Launch per Sysprep

Il file di risposta e i file batch di EC2Launch per Sysprep includono quanto segue:

`Unattend.xml`

Si tratta del file di risposta predefinito. Se esegui `SysprepInstance.ps1` o scegli ShutdownWithSysprepnell'interfaccia utente, il sistema legge l'impostazione da questo file.

`BeforeSysprep.cmd`

Personalizzare questo file batch per eseguire i comandi prima che EC2Launch esegua Sysprep.

`SysprepSpecialize.cmd`

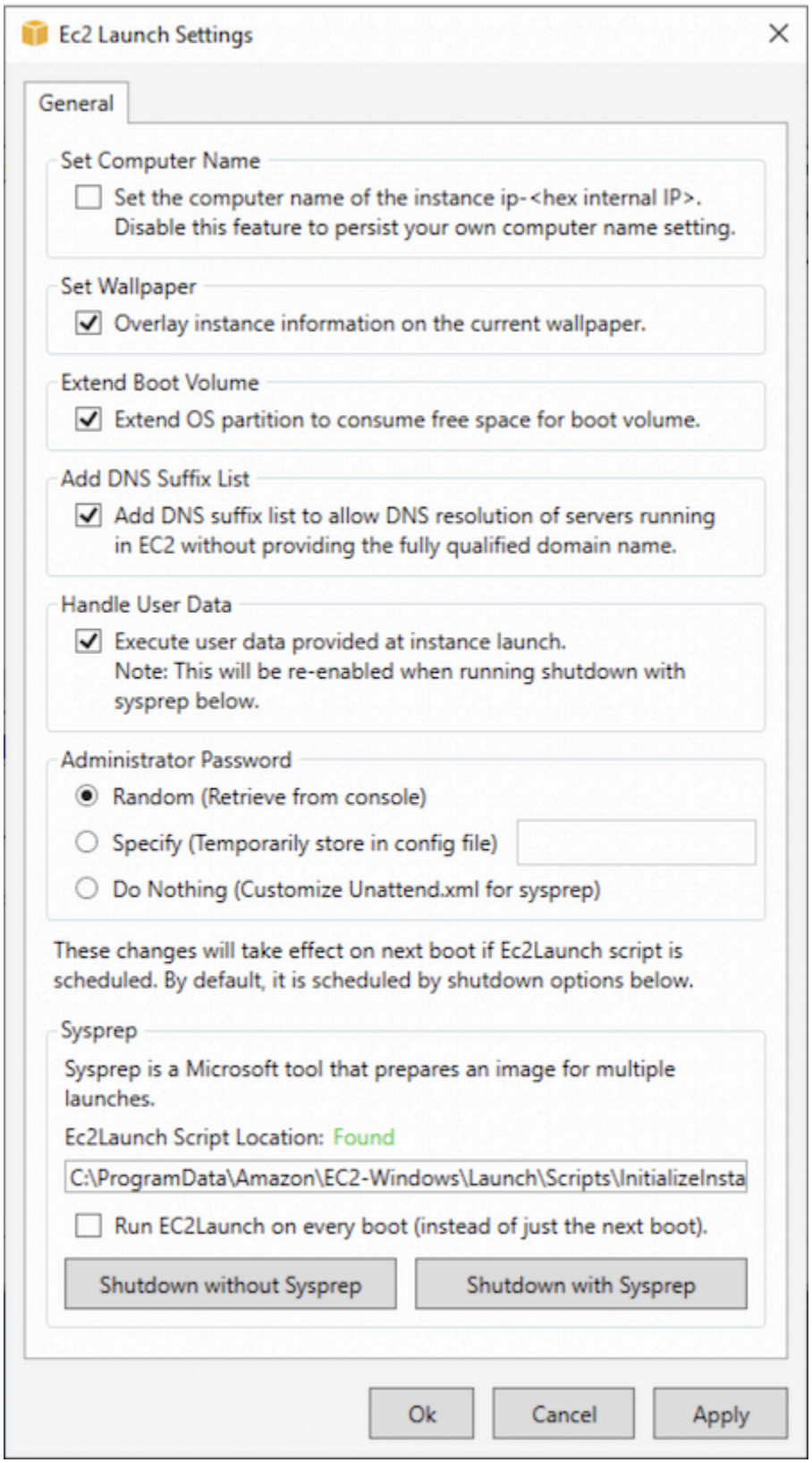
Personalizzare questo file batch per eseguire i comandi durante la fase di specializzazione di Sysprep.

Utilizzo di Sysprep con EC2Launch

Durante l'installazione completa di Windows Server 2016 o versione successiva (con un'esperienza desktop), è possibile eseguire Sysprep con EC2Launch manualmente o utilizzando l'applicazione EC2 Launch Settings (Impostazioni di avvio EC2) .

Eseguire Sysprep tramite l'applicazione EC2Launch Settings

1. Nella console Amazon EC2, identificare o creare un'AMI di Windows Server 2016 o versione successiva.
2. Avviare un'istanza Windows dall'AMI.
3. Collegarsi all'istanza Windows e personalizzarla.
4. Cerca ed esegui l'applicazione EC2 LaunchSettings. Per impostazione predefinita, si trova nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.



5. Selezionare o deselezionare le opzioni in base alle esigenze. Tali impostazioni vengono memorizzate nel file `LaunchConfig.json`.

6. Per Administrator Password (Password amministratore), eseguire una delle seguenti operazioni:

   - Scegliere Random (Casuale). EC2Launch genera una password e la crittografa utilizzando la chiave dell'utente. Il sistema disattiva questa impostazione dopo l'avvio dell'istanza in modo che questa password rimanga se l'istanza viene riavviata o arrestata e avviata.
   - Scegliere Specify (Specifica) e digitare una password che soddisfi i requisiti di sistema. La password viene memorizzata in `LaunchConfig.json` come testo non crittografato e viene cancellata dopo che Sysprep ha impostato la password amministratore. Se si esegue l'arresto in questo momento, la password viene impostata immediatamente. EC2Launch crittografa la password utilizzando la chiave dell'utente.
   - Scegli DoNothinge specifica una password nel `unattend.xml` file. Se non si indica una password in `unattend.xml`, l'account amministratore viene disattivato.
7. Selezionare Shutdown with Sysprep (Arresta con Sysprep).

Eseguire Sysprep manualmente tramite EC2Launch

1. Nella console Amazon EC2 identificare o creare un'AMI di Windows Server 2016 o versione successiva, edizione Datacenter, che si desidera duplicare.
2. Avviare l'istanza Windows e connettersi a essa.
3. Personalizzare l'istanza.
4. Specificare le impostazioni nel file `LaunchConfig.json`. Per impostazione predefinita, questo file si trova nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

   Per `adminPasswordType`, indicare uno dei valori seguenti:

   `Random`

   EC2Launch genera una password e la crittografa utilizzando la chiave dell'utente. Il sistema disattiva questa impostazione dopo l'avvio dell'istanza in modo che questa password rimanga se l'istanza viene riavviata o arrestata e avviata.

   `Specify`

   EC2Launch utilizza la password specificata in `adminPassword`. Se la password non soddisfa i requisiti di sistema, EC2Launch genera invece una password casuale. La password viene memorizzata in `LaunchConfig.json` come testo non crittografato e viene cancellata dopo che Sysprep ha impostato la password amministratore. EC2Launch crittografa la password utilizzando la chiave dell'utente.

`DoNothing`

EC2Launch utilizza la password specificata nel file `unattend.xml`. Se non si indica una password in `unattend.xml`, l'account amministratore viene disattivato.

5. (Facoltativo) Specificare le impostazioni nel file `unattend.xml` e in altri file di configurazione. Se si prevede di partecipare all'installazione, non è necessario apportare modifiche a questi file. Per impostazione predefinita, i file si trovano nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. In Windows PowerShell, esegui `./InitializeInstance.ps1 -Schedule`. Per impostazione predefinita, lo script si trova nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`. Lo script programma l'istanza da inizializzare durante l'avvio seguente. Bisogna eseguire questo script prima di eseguire lo script `SysprepInstance.ps1` durante la fase successiva.
7. In Windows PowerShell, esegui `./SysprepInstance.ps1`. Per impostazione predefinita, lo script si trova nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Si verrà disconnessi dall'istanza e l'istanza verrà arrestata. Se si controlla la pagina Instances (Istanze) nella console Amazon EC2, lo stato dell'istanza cambia da `Running` a `Stopping`, quindi in `Stopped`. A questo punto è sicuro creare un'AMI da questa istanza.

Aggiornamento di routing KMS/metadati per il Server 2016 o versione successiva quando si lancia un'AMI personalizzata

Per aggiornare routing KMS/metadati per il Server 2016 o versione successiva quando si lancia un'AMI personalizzata, effettuare una delle seguenti operazioni:

- Esegui la LaunchSettings GUI EC2 (C:\\ ProgramData Amazon\ EC2-Windows\ Launch\ Settings\ Ec2 LaunchSettings .exe) e seleziona l'opzione per chiudere con Sysprep.
- Esegui EC2 LaunchSettings e spegni senza Sysprep prima di creare l'AMI. Questo fa in modo che le attività di inizializzazione dell'avvio di EC2 vengano eseguite all'avvio successivo che imposta i routing in base alla sottorete per l'instanza.
- Riprogramma manualmente le attività di inizializzazione di EC2 Launch prima di creare un'AMI da. PowerShell

> **Important**
>
> Prendere nota del comportamento predefinito di reimpostazione della password prima di riprogrammare le attività.

- Per aggiornare le route su un'istanza in esecuzione in cui si verifica l'attivazione di Windows o la comunicazione con errori dei metadati dell'istanza, vedere "Impossibile attivare Windows".

Utilizzo di Sysprep con EC2Config

Questa sezione include i dettagli sulle diverse fasi di esecuzione di Sysprep e sulle attività eseguite dal servizio EC2Config durante la preparazione dell'immagine. Include anche le fasi per creare un'AMI standardizzata utilizzando Sysprep con il servizio EC2config.

Argomenti di Sysprep con EC2config

- Fasi di Sysprep
- Azioni di Sysprep
- Dopo Sysprep
- Eseguire Sysprep con il servizio EC2Config

Fasi di Sysprep

L'esecuzione di Sysprep avviene nelle fasi seguenti:

- Generalize (Generalizzazione): lo strumento rimuove le informazioni e le configurazioni specifiche dell'immagine. Per esempio, Sysprep rimuove l'identificatore di sicurezza (SID), il nome del computer, i log di eventi e i driver specifici, per citarne alcune. Dopo il completamento di questa fase, il sistema operativo (SO) è pronto a creare un'AMI.

> **Note**
>
> Quando si esegue Sysprep con il servizio EC2Config, il sistema impedisce la rimozione dei driver perché l'impostazione è impostata su true per impostazione predefinita. PersistAllDeviceInstalls

- Specialize (Specializzazione): Plug and Play esegue un'analisi del computer e installa i driver per ogni dispositivo rilevato. Lo strumento genera i requisiti del SO, quali il nome del computer e l'SID. Facoltativamente, è possibile eseguire comandi in questa fase.
- Out-of-Box Experience (OOBE) (Configurazione guidata): il sistema esegue una versione abbreviata della Configurazione di Windows e richiede all'utente di inserire informazioni come la lingua del sistema, il fuso orario e un'organizzazione registrata. Quando si esegue Sysprep con EC2Config, il file di risposta automatizza questa fase.

Azioni di Sysprep

Durante la preparazione di un'immagine, Sysprep e il servizio EC2Config eseguono le azioni seguenti.

1. Quando si sceglie Arresta con Sysprep nella finestra di dialogo Proprietà del servizio EC2, il sistema esegue il comando ec2config.exe –sysprep.
2. Il servizio EC2Config legge il contenuto del file `BundleConfig.xml`. Per impostazione predefinita, questo file si trova nella directory seguente: `C:\Program Files\Amazon \Ec2ConfigService\Settings`.

   Il file `BundleConfig.xml` include le seguenti impostazioni. È possibile modificare tali impostazioni:

   - AutoSysprep: Indica se utilizzare Sysprep automaticamente. Non si deve modificare tale valore se Sysprep è in esecuzione dalla finestra di dialogo EC2 Service Properties (Proprietà servizio EC2). Il valore predefinito è `No`.
   - SetRDPCertificate: imposta un certificato autofirmato per il server Remote Desktop. Questo consente di utilizzare il Remote Desktop Protocol (RDP) in modo sicuro per connettersi all'istanza. Modifica il valore in `Yes` se le nuove istanze devono utilizzare un certificato. Questa impostazione non viene utilizzata con le istanze di Windows Server 2012 perché questi sistemi operativi possono generare i propri certificati. Il valore predefinito è `No`.
   - SetPasswordAfterSysprep: imposta una password casuale su un'istanza appena avviata, la crittografa con la chiave di avvio dell'utente e invia la password crittografata alla console. Modifica il valore in `No` se le nuove istanze non devono essere impostate su una password casuale crittografata. Il valore predefinito è `Yes`.
   - PreSysprepRunCmd: la posizione del comando da eseguire. Per impostazione predefinita il comando si trova nella seguente directory: `C:\Program Files\Amazon \Ec2ConfigService\Scripts\BeforeSysprep.cmd`

3. Il sistema esegue `BeforeSysprep.cmd`. Tale comando crea una chiave di registro come indicato di seguito:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
 fDenyTSConnections /t REG_DWORD /d 1 /f
```

   La chiave di registro disattiva le connessioni RDP fino a che non vengono riattivate. La disattivazione delle connessioni RDP è una misura di sicurezza necessaria in quanto, nella prima sessione di avvio dopo l'esecuzione di Sysprep, RDP consente le connessioni per un breve periodo di tempo in cui la password dell'Amministratore è vuota.

4. Il servizio EC2Config chiama Sysprep attraverso l'esecuzione dei comandi seguenti:

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /
oobe /generalize /shutdown
```

Fase di generalizzazione

- Lo strumento rimuove le informazioni e le configurazioni specifiche dell'immagine, quali il nome del computer e l'SID. Se l'istanza è un membro di un dominio, essa viene rimossa dal dominio. Il file di risposta `sysprep2008.xml` include le impostazioni seguenti che riguardano questa fase:
  - PersistAllDeviceInstalls: questa impostazione impedisce a Windows Setup di rimuovere e riconfigurare i dispositivi, il che accelera il processo di preparazione delle immagini perché le AMI Amazon richiedono l'esecuzione di determinati driver e il nuovo rilevamento di tali driver richiederebbe tempo.
  - DoNotCleanUpNonPresentDevices: questa impostazione conserva le informazioni Plug and Play per i dispositivi attualmente non presenti.
- Sysprep arresta l'SO quando si prepara alla creazione dell'AMI. Il sistema avvia una nuova istanza o avvia l'istanza originale.

Fase di specializzazione

Il sistema genera i requisiti specifici del SO, come un nome del computer e un SID. Il sistema esegue anche le azioni seguenti, in base alle configurazioni specificate nel file di risposta sysprep2008.xml.

- CopyProfile: Sysprep può essere configurato per eliminare tutti i profili utente, incluso il profilo Administrator integrato. Questa impostazione mantiene l'account Amministratore integrato cosicché

qualsiasi personalizzazione effettuata su tale account venga trasferita alla nuova immagine. Il valore predefinito è True.

CopyProfilesostituisce il profilo predefinito con il profilo di amministratore locale esistente. Tutti gli account connessi dopo l'esecuzione di Sysprep riceveranno una copia di tale profilo e del suo contenuto al primo accesso.

Se non si dispone di personalizzazioni specifiche del profilo utente che si desidera trasferire alla nuova immagine, modificare questa impostazione in False. Sysprep rimuoverà tutti i profili utente, risparmiando tempo e spazio su disco.

- TimeZone: per impostazione predefinita, il fuso orario è impostato su Coordinate Universal Time (UTC).
- Synchronous command with order 1 (Comando sincrono con ordine 1): il sistema esegue il comando seguente che abilita l'account amministratore e specifica il requisito della password.

  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER / PASSWORDREQ:YES
- Synchronous command with order 2 (Comando sincrono con ordine 2): il sistema codifica la password dell'amministratore. Questa misura di sicurezza è progettata per impedire che l'istanza sia accessibile dopo il completamento di Sysprep se non è stata attivata l'impostazione ec2setpassword.

  C:\Program Files\ Amazon\ Ec2ConfigService\ ScramblePassword .exe» -u Amministratore
- Synchronous command with order 3 (Comando sincrono con ordine 3): il sistema esegue il comando seguente:

  C:\Program Files\ Amazon\ Ec2\ ScriptsConfigService\ .cmd SysprepSpecializePhase

  Questo comando aggiunge la seguente chiave di registro, che riattiva l'RDP:

  reg aggiungi «HKEY_LOCAL_MACHINE\ SYSTEM\\ ControlCurrentControlSet\ Terminal Server» /v fdenytsConnections /t REG_DWORD /d 0 /f

Fase Configurazione guidata

1. Con l'utilizzo del file di risposta del servizio EC2Config, il sistema specifica le configurazioni seguenti:
   - InputLocale< InputLocale >it-IT</ >

- < SystemLocale >it-IT</ SystemLocale >
- <UILanguage>en-US</UILanguage>
- < UserLocale >it-IT</ UserLocale >
- <HideEULAPage>true</HideEULAPage>
- < HideWirelessSetupIn OOBE>True</ HideWirelessSetupIn OOBE>
- < NetworkLocation >Altro</ NetworkLocation >
- < PC>3</ PC> ProtectYour ProtectYour
- < BluetoothTaskbarIconEnabled >falso</ BluetoothTaskbarIconEnabled >
- < TimeZone >UTC</ TimeZone >
- < RegisteredOrganization > Amazon.com</ RegisteredOrganization >
- < RegisteredOwner RegisteredOwner >Amazon</ >

> **Note**
>
> Durante le fasi di generalizzazione e di specializzazione, il servizio EC2Config monitora lo stato del SO. Se EC2Config rileva che il SO si trova in una fase di Sysprep, pubblica il messaggio seguente nel log di sistema:
> EC2ConfigMonitorState: 0 Windows è in fase di configurazione.
> SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Al termine della fase OOBE, il sistema esegue `SetupComplete.cmd` dal seguente percorso: `C:\Windows\Setup\Scripts\SetupComplete.cmd`. Nelle AMI pubbliche di Amazon, prima dell'aprile 2015 questo file era vuoto e non eseguiva nulla sull'immagine. Nelle AMI pubbliche datate dopo l'aprile 2015, il file include il seguente valore: call "C:\Program Files\Amazon\Ec2ConfigService\Scripts\PostSysprep.cmd".
3. Il sistema esegue `PostSysprep.cmd`, che esegue le seguenti operazioni:
   - Imposta la password Amministratore locale in modo che non scada. Se la password è scaduta, l'Amministratore potrebbe non essere in grado di effettuare l'accesso.
   - Imposta il nome della macchina MSSQLServer (se installata) in modo che sia sincronizzato con l'AMI.

Dopo Sysprep

Al termine di Sysprep, i servizi EC2Config inviano il messaggio seguente all'uscita della console:

```
Windows sysprep configuration complete.
   Message: Sysprep Start
   Message: Sysprep End
```

Quindi EC2Config effettua le seguenti azioni:

1. Legge il contenuto del file config.xml ed elenca tutti i plug-in attivati.
2. Esegue tutti i plug-in "Prima che Windows sia pronto" contemporaneamente.
   - Ec2 SetPassword
   - Ec2 SetComputerName
   - Ec2 InitializeDrives
   - Ec2 EventLog
   - Ec2ConfigureRDP
   - Ec2OutputRDPCert
   - Ec2 SetDriveLetter
   - Ec2 WindowsActivate
   - Ec2 DynamicBootVolumeSize
3. Al termine, invia un messaggio "Windows è pronto" ai log del sistema di istanza.
4. Esegue tutti i plug-in "Dopo che Windows è pronto" contemporaneamente.
   - CloudWatch Registri Amazon
   - UserData
   - AWS Systems Manager (Systems Manager)

Per ulteriori informazioni sui plug-in di Windows, consulta Configurare un'istanza di Windows utilizzando il servizio EC2Config (legacy).

Eseguire Sysprep con il servizio EC2Config

Per creare un'AMI standardizzata utilizzando Sysprep e il servizio EC2Config, utilizzare la procedura seguente.

1. Nella console Amazon EC2 individuare o creare un'AMI che si desidera duplicare.
2. Avviare l'istanza Windows e connettersi a essa.
3. Personalizzarla.

4. Specificare le impostazioni di configurazione nel file di risposta del servizio EC2Config:

   `C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml`

5. Dal menu Start di Windows, scegli Tutti i programmi, quindi scegli ConfigServiceImpostazioni EC2.
6. Selezionare la scheda Image (Immagine) nella finestra di dialogo Ec2 Service Properties (Proprietà servizio Ec2). Per ulteriori informazioni sulle opzioni e sulle impostazioni nella finestra di dialogo Proprietà servizio Ec2, consultare Proprietà servizio Ec2.
7. Selezionare un'opzione per la password Amministratore, quindi scegliere Shutdown with Sysprep (Arresta con Sysprep) o Shutdown without Sysprep (Arresta senza Sysprep). EC2Config modifica i file delle impostazioni in base all'opzione della password selezionata.
   - Random (Casuale): EC2Config genera una password, la crittografa con la chiave dell'utente e mostra la password crittografata alla console. Questa impostazione si disattiva dopo il primo avvio, in modo che questa password persista se l'istanza viene riavviata o arrestata e avviata.
   - Specify (Specifica): la password viene memorizzata nel file di risposta Sysprep in un modulo non crittografato (testo normale). Quando Sysprep viene eseguito, imposta la password Amministratore. Se si esegue l'arresto in questo momento, la password viene impostata immediatamente. Quando il servizio viene avviato nuovamente, la password Amministratore viene rimossa. È importante ricordare la password, poiché non sarà più possibile recuperarla in seguito.
   - Keep Existing (Mantenere quella esistente): la password esistente dell'account Amministratore non cambia durante l'esecuzione di Sysprep o il riavvio di EC2Config. È importante ricordare la password, poiché non sarà più possibile recuperarla in seguito.
8. Seleziona OK.

Quando viene chiesto di confermare l'esecuzione di Sysprep e l'arresto dell'istanza, fare clic su Sì. EC2Config esegue Sysprep. Successivamente, si verrà disconnessi dall'istanza e l'istanza verrà arrestata. Se si controlla la pagina Instances (Istanze) nella console Amazon EC2, lo stato dell'istanza cambia da `Running` a `Stopping` e infine in `Stopped`. A questo punto, è opportuno creare un'AMI da questa istanza.

È possibile richiamare manualmente lo strumento Sysprep dalla riga di comando con il comando seguente:

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep""
```

> **Note**
>
> Le virgolette doppie nel comando non sono necessarie se la shell CMD è già nella directory C:\Program Files\ Amazon\ EC2ConfigService\.

Tuttavia, è necessario controllare bene che le opzioni dei file XML specificate nella cartella `Ec2ConfigService\Settings` siano corrette; in caso contrario, potrebbe non essere possibile connettersi all'istanza. Per ulteriori informazioni sui file delle impostazioni, consultare File delle impostazioni di EC2Config. Per avere un esempio della configurazione e dell'esecuzione di Sysprep dalla riga di comando, consulta `Ec2ConfigService\Scripts\InstallUpdates.ps1`.

Modificare un'AMI

Puoi modificare un set limitato di attributi Amazon Machine Image (AMI), come la descrizione e le proprietà di condivisione dell'AMI. Tuttavia, il contenuto dell'AMI (dati binari del volume) non può essere modificato. Per modificare il contenuto dell'AMI, è necessario creare una nuova AMI.

> **Important**
>
> Non puoi modificare il contenuto (dati binari del volume) di un'AMI supportata da EBS perché gli snapshot che lo supportano sono immutabili. Inoltre, non puoi modificare il contenuto (dati binari di volume) di un'AMI Linux basata sull'archivio di istanze (supportata da S3) perché il contenuto è firmato e l'avvio dell'istanza avrà esito negativo se le firme non corrispondono.

Per gli attributi AMI che possono essere modificati, consulta ModifyImageAttributeil riferimento alle API di Amazon EC2.

I seguenti argomenti forniscono istruzioni per l'uso della console Amazon EC2 e AWS CLI per modificare gli attributi di un'AMI:

- Rendere un'AMI pubblica
- Condivisione di un'AMI con organizzazioni o unità organizzative specifiche
- Condividere un'AMI con account AWS specifici
- Utilizzo del supporto a pagamento
- Configurazione dell'AMI

Copiare un'AMI

Puoi copiare un'Amazon Machine Image (AMI) all'interno o tra AWS regioni diverse. Puoi copiare sia AMI supportate da Amazon EBS che AMI supportate da Instance Storage. Puoi copiare le AMI supportate da EBS con istantanee crittografate e modificare lo stato della crittografia durante il processo di copia. Puoi copiare le AMI condivise da altri.

La copia di un'AMI di origine produce una nuova AMI identica ma distinta, denominata anche AMI di destinazione. L'AMI di destinazione ha il proprio ID AMI univoco. Puoi modificare o annullare la registrazione dell'AMI di origine senza alcun effetto sull'AMI di destinazione. È vero anche il contrario.

Con un'AMI supportata da EBS, ciascuna delle relative istantanee di backup viene copiata in un'istantanea di destinazione identica ma distinta. Se si copia un AMI in una nuova regione, gli snapshot saranno copie complete (non incrementali). Se si crittografano gli snapshot di backup non crittografati o li si crittografa in una nuova chiave KMS, gli snapshot saranno copie complete (non incrementali). Operazioni di copia successive di un AMI restituiscono copie incrementali degli snapshot di backup.

Indice

Considerazioni

- Autorizzazione a copiare le AMI: puoi utilizzare le policy IAM per concedere o negare agli utenti l'autorizzazione a copiare le AMI. Le autorizzazioni a livello di risorsa specificate per l'operazione `CopyImage` si applicano solo alla nuova AMI. Non è possibile specificare autorizzazioni a livello di risorsa per l'AMI di origine.
- Autorizzazioni di avvio e autorizzazioni per bucket Amazon S3 AWS : non copia le autorizzazioni di avvio o le autorizzazioni del bucket Amazon S3 dall'AMI di origine alla nuova AMI. Al

completamento dell'operazione di copia, è possibile applicare i permessi di avvio e le autorizzazioni del bucket Amazon S3 alla nuova AMI.

- Tag: puoi copiare solo i tag AMI definiti dall'utente che hai collegato all'AMI di origine. I tag di sistema (con il prefisso `aws:`) e i tag definiti dall'utente che sono collegati da altri Account AWS non verranno copiati. Quando si copia un'AMI, è possibile allegare nuovi tag all'AMI di destinazione e alle relative istantanee di supporto.

Costi

Non sono previsti addebiti per la copia di un'AMI. Tuttavia, vengono applicati i costi standard di archiviazione e trasferimento dati. Se si copia un'AMI EBS-backed, saranno addebitati i costi per lo archiviazione di eventuali snapshot EBS aggiuntivi.

Autorizzazioni IAM

Per copiare un'AMI supportata da EBS o da instance store-backed, sono necessarie le seguenti autorizzazioni IAM:

- `ec2:CopyImage`— Per copiare l'AMI. Per le AMI supportate da EBS, concede anche l'autorizzazione a copiare le istantanee di supporto dell'AMI.
- `ec2:CreateTags`— Per etichettare l'AMI di destinazione. Per le AMI supportate da EBS, concede anche l'autorizzazione a taggare le istantanee di supporto dell'AMI di destinazione.

Se stai copiando un'AMI supportata da un'istanza archiviata, hai bisogno delle seguenti autorizzazioni IAM aggiuntive:

- `s3:CreateBucket`— Per creare il bucket S3 nella regione di destinazione per la nuova AMI
- `s3:GetBucketAcl`— Per leggere le autorizzazioni ACL per il bucket di origine
- `s3:ListAllMyBuckets`— Per trovare un bucket S3 esistente per le AMI nella regione di destinazione
- `s3:GetObject`— Per leggere gli oggetti nel bucket di origine
- `s3:PutObject`— Per scrivere gli oggetti nel bucket di destinazione
- `s3:PutObjectAcl`— Per scrivere i permessi per i nuovi oggetti nel bucket di destinazione

Esempio di policy IAM per copiare un AMI supportato da EBS e etichettare l'AMI e le istantanee di destinazione

La seguente politica di esempio ti concede l'autorizzazione a copiare qualsiasi AMI supportato da EBS e taggare l'AMI di destinazione e le relative istantanee di supporto.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "PermissionToCopyAllImages",
        "Effect": "Allow",
        "Action": [
            "ec2:CopyImage",
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:*::image/*"
    }]
}
```

Esempio di policy IAM per copiare un'AMI supportata da EBS ma negare l'etichettatura delle nuove istantanee

L'`ec2:CopySnapshot`autorizzazione viene concessa automaticamente quando si ottiene l'autorizzazione. `ec2:CopyImage` Ciò include l'autorizzazione a etichettare le nuove istantanee di supporto dell'AMI di destinazione. L'autorizzazione a etichettare le nuove istantanee di supporto può essere negata esplicitamente.

La seguente politica di esempio ti concede l'autorizzazione a copiare qualsiasi AMI supportata da EBS, ma ti impedisce di taggare le nuove istantanee di supporto dell'AMI di destinazione.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Deny",
```

```
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:::snapshot/*"
        }
    ]
}
```

Esempio di policy IAM per copiare un AMI basato su storage di un'istanza e etichettare l'AMI di destinazione

La seguente politica di esempio concede l'autorizzazione a copiare qualsiasi AMI memorizzato nello storage di istanza nel bucket di origine specificato nella regione specificata e contrassegnare l'AMI di destinazione.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "PermissionToCopyAllImages",
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::ami-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
```

```
                "s3:PutObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-account-in-region-hash"
            ]
        }
    ]
}
```

Per trovare il nome della risorsa Amazon (ARN) del bucket di origine AMI, apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2, nel pannello di navigazione seleziona AMIs (AMI) e individua il nome del bucket nella colonna Source (Origine).

> **Note**
>
> L'`s3:CreateBucket`autorizzazione è necessaria solo la prima volta che si copia un'AMI basata su instance store-backed in una singola regione. Successivamente, il bucket Amazon S3 già creato nella regione viene utilizzato per archiviare tutte le AMIs future copiate in quella regione.

Copiare un'AMI

Puoi copiare un'AMI utilizzando AWS Management Console, the AWS Command Line Interface o SDK o l'API Amazon EC2, che supportano `CopyImage` tutti l'azione.

Console

Per copiare un AMI

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione della console, selezionare la regione che contiene l'AMI.
3. Nel pannello di navigazione, scegli AMI per visualizzare l'elenco delle AMI disponibili nella regione.
4. Se non vedi l'AMI che desideri copiare, scegli un filtro diverso. Puoi filtrare per AMI di mia proprietà, immagini private, immagini pubbliche e immagini disattivate.
5. Seleziona l'AMI da copiare, quindi scegli Azioni, Copia AMI.
6. Nella pagina Copy AMI (Copia AMI), specificare le seguenti informazioni:

a. AMI copy name (Nome copia AMI): un nome per la nuova AMI. Puoi includere le informazioni sul sistema operativo nel nome perché Amazon EC2 non fornisce queste informazioni quando visualizza i dettagli sull'AMI.

b. AMI copy description (Descrizione copia AMI): per impostazione predefinita, la descrizione include informazioni relative all'AMI di origine in modo da distinguere una copia dall'originale. È possibile modificare questa descrizione se necessario.

c. Destination region (Regione di destinazione): la Regione in cui copiare l'AMI. Per ulteriori informazioni, consulta Copia tra regioni.

d. Copy tags (Copia tag): seleziona questa casella di controllo per includere i tag AMI definiti dall'utente durante la copia dell'AMI. I tag di sistema (con il prefisso `aws:`) e i tag definiti dall'utente che sono collegati da altri Account AWS non verranno copiati.

e. (Solo AMI supportate da EBS) Crittografa le istantanee EBS della copia AMI: seleziona questa casella di controllo per crittografare le istantanee di destinazione o per crittografarle nuovamente utilizzando una chiave diversa. Se la crittografia è abilitata per impostazione predefinita, la casella di controllo Encrypt EBS snapshot of AMI copy è selezionata e non può essere deselezionata. Per ulteriori informazioni, consulta Crittografia e copia.

f. (Solo AMI supportate da EBS) Chiave KMS: la chiave KMS da utilizzare per crittografare le istantanee di destinazione.

g. Tag: puoi etichettare la nuova AMI e le nuove istantanee con gli stessi tag oppure puoi etichettarli con tag diversi.

   - Per etichettare la nuova AMI e le nuove istantanee con gli stessi tag, scegli Tagga immagine e istantanee insieme. Gli stessi tag vengono applicati alla nuova AMI e a tutte le istantanee create.
   - Per etichettare la nuova AMI e le nuove istantanee con tag diversi, scegli Tagga immagine e istantanee separatamente. Tag diversi vengono applicati alla nuova AMI e alle istantanee create. Nota, tuttavia, che tutte le nuove istantanee create hanno gli stessi tag; non puoi etichettare ogni nuova istantanea con un tag diverso.

   Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore per il tag. Ripetere per ogni tag.

h. Quando sei pronto a copiare l'AMI, scegli Copia AMI.

Lo stato iniziale della nuova AMI è `Pending`. L'operazione di copia AMI è completata quando lo stato è `Available`.

AWS CLI

Per copiare un AMI utilizzando il AWS CLI

È possibile copiare un'AMI tramite il comando copy-image. È necessario specificare la regione di origine e quella di destinazione, la prima tramite il parametro `--source-region`, mentre la seconda va specificata tramite il parametro `--region` o una variabile ambientale. Per ulteriori informazioni, vedere Configurazione dell'interfaccia a riga di AWS comando.

(Solo AMI supportate da EBS) Quando si crittografa uno snapshot di destinazione durante la copia, è necessario specificare questi parametri aggiuntivi: e. `--encrypted --kms-key-id`

Per i comandi di esempio, consulta la sezione Examples (Esempi) sotto copy-image nella Guida di riferimento ai comandi della AWS CLI .

PowerShell

Per copiare un'AMI utilizzando gli strumenti per Windows PowerShell

È possibile copiare un AMI utilizzando il Copy-EC2Imagecomando. È necessario specificare la regione di origine e quella di destinazione, la prima tramite il parametro `-SourceRegion`, mentre la seconda va specificata tramite il parametro `-Region` o il comando `Set-AWSDefaultRegion`. Per ulteriori informazioni, vedere Specificazione AWS delle regioni.

(Solo AMI supportate da EBS) Quando si crittografa uno snapshot di destinazione durante la copia, è necessario specificare questi parametri aggiuntivi: e. `-Encrypted -KmsKeyId`

Arrestare un'operazione di copia AMI in sospeso

Puoi interrompere una copia AMI in sospeso utilizzando AWS Management Console o la riga di comando.

Console

Arrestare un'operazione di copia di AMI tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Dalla barra di navigazione, selezionare la regione di destinazione dal selettore di regione.
3. Nel riquadro di navigazione scegliere AMIs (AMI).
4. Seleziona l'AMI per interrompere la copia, quindi scegli Azioni, Annulla registrazione AMI.
5. Quando viene richiesta la conferma, scegliere Deregister AMI (Annulla registrazione AMI).

Command line

Arrestare un'operazione di copia AMI tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

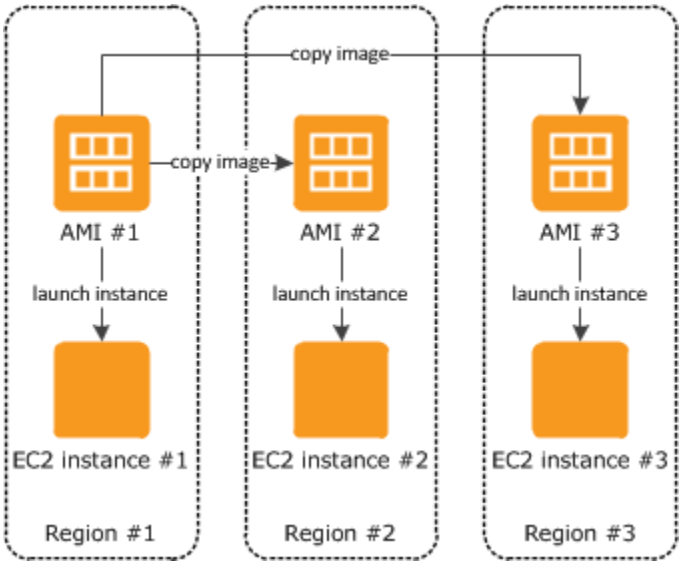
- deregister-image (AWS CLI)
- Unregister-EC2Image (AWS Tools for Windows PowerShell)

Copia tra regioni

Copiare un'AMI tra regioni geograficamente diverse offre i seguenti vantaggi:

- Distribuzione globale coerente: la copia di un'AMI da una regione all'altra consente di avviare istanze coerenti in regioni diverse in base alla stessa AMI.
- Scalabilità: è possibile progettare e creare più facilmente applicazioni di livello mondiale che soddisfino le esigenze degli utenti, indipendentemente dalla loro posizione.
- Prestazioni: è possibile aumentare le prestazioni distribuendo l'applicazione e localizzandone i componenti critici nelle vicinanze degli utenti. Puoi anche sfruttare le funzionalità specifiche della regione, come i tipi di istanze o altri servizi. AWS
- Elevata disponibilità: progettare e distribuire applicazioni nelle regioni AWS consente di aumentare la disponibilità.

Il diagramma seguente mostra la relazione tra un'AMI di origine e due AMI copiate in regioni diverse, nonché le istanze EC2 lanciate da ciascuna di esse. Quando avvii un'istanza da un'AMI, questa risiede nella stessa regione in cui risiede l'AMI. Se modifichi l'AMI di origine e desideri che tali modifiche si riflettano nelle AMIs delle regioni di destinazione, devi copiare nuovamente le AMI di origine nelle regioni di destinazione.



Quando copi per la prima volta un'AMI supportata da instance store in una regione, viene creato un bucket Amazon S3 per le AMIs copiate in quella regione. Tutte le AMIs supportate da instance store che vengono copiate in quella regione vengono memorizzate in questo bucket. I nomi del bucket hanno il formato seguente: amis-for-*account*-in-*regione*-*hash*. Ad esempio: `amis-for-123456789012-in-us-east-2-yhjmxvp6`.

Prerequisito

Prima di copiare un'AMI devi assicurarti che il contenuto dell'AMI di origine sia aggiornato per supportare l'esecuzione in un'altra regione. Ad esempio è necessario aggiornare tutte le stringhe di connessione al database o i dati di configurazione dell'applicazione simili per individuare le risorse appropriate. In caso contrario, le istanze avviate dalla nuova AMI nella regione di destinazione potrebbero continuare a utilizzare le risorse della regione di origine, il che può influire sulle prestazioni e sui costi.

Limitazioni

- Per le regioni di destinazione è previsto un limite di 100 copie di AMI simultanee.
- Non puoi copiare un'AMI paravirtuale (PV) in una regione che non supporta le AMI PV. Per ulteriori informazioni, consulta Tipi di virtualizzazione dell'AMI.

Copia tra account

Se un AMI di un altro utente Account AWS è condiviso con il tuo Account AWS, puoi copiare l'AMI condiviso. Questa operazione è nota come copia su più account. L'AMI condivisa con te è l'AMI di

origine. Quando si copia l'AMI di origine, si crea una nuova AMI. La nuova AMI viene spesso definita AMI di destinazione.

Costi AMI

- Per un'AMI condivisa, all'account dell'AMI condivisa viene addebitato lo spazio di archiviazione nella regione.
- Se copi un AMI condiviso con il tuo account, sei il proprietario dell'AMI di destinazione nel tuo account.
  - Al proprietario dell'AMI di origine vengono addebitate le tariffe di trasferimento standard di Amazon EBS o Amazon S3.
  - Ti viene addebitato il costo dello storage dell'AMI di destinazione nella regione di destinazione.

Autorizzazioni a livello di risorsa

Per copiare un'AMI condivisa con te da un altro account, il proprietario dell'AMI di origine deve concedere le autorizzazioni di lettura per l'archiviazione che supporta l'AMI. L'archiviazione è lo snapshot EBS associato (per un'AMI supportata da Amazon EBS) o un bucket S3 associato (per un'AMI supportata da archivio dell'istanza). Se l'AMI condivisa dispone di snapshot crittografati, il proprietario deve condividere anche la chiave o le chiavi. Per ulteriori informazioni sulla concessione delle autorizzazioni alle risorse, per gli snapshot EBS, consulta Share an Amazon EBS snapshot nella Amazon EBS User Guide e per i bucket S3, consulta Identity and access management in Amazon S3 nella Amazon Simple Storage Service User Guide.

> **Note**
>
> I tag collegati all'AMI di origine non vengono copiati tra account sull'AMI di destinazione.

Crittografia e copia

La tabella seguente mostra il supporto di crittografia in vari scenari di copia di AMI. Sebbene sia possibile copiare uno snapshot non crittografato per produrne uno crittografato, non è possibile copiare uno snapshot crittografato per produrne uno non crittografato.

Scenario	Descrizione	Supportata
1	U nencrypted-to-unencrypted	Sì

Scenario	Descrizione	Supportata
2	E ncrypted-to-encrypted	Sì
3	U nencrypted-to-encrypted	Sì
4	E ncrypted-to-unencrypted	No

> **Note**
>
> La crittografia durante l'operazione `CopyImage` si applica solo ad AMIs supportate da Amazon EBS. Poiché un'AMI supportata da instance store non si basa sugli snapshot, non puoi utilizzare la copia per modificare il suo stato di crittografia.

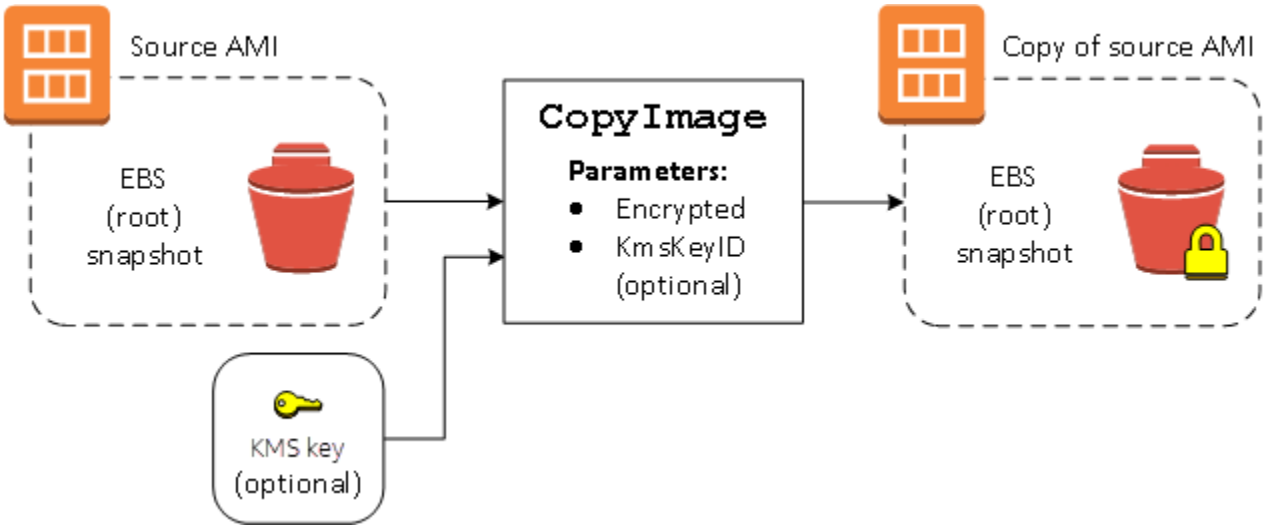
Per impostazione predefinita (ovvero, senza specificare i parametri di crittografia), lo snapshot di supporto di un'AMI viene copiato con il proprio stato di crittografia originario. Copiare un'AMI supportata da uno snapshot non crittografato consente di ottenere uno snapshot di destinazione identico, anch'esso non crittografato. Se l'AMI di origine è supportata da un'istantanea crittografata, copiandola si ottiene un'istantanea di destinazione identica crittografata con la stessa chiave. AWS KMS Copiare un'AMI supportata da più snapshot mantiene, per impostazione predefinita, lo stato di crittografia di origine in ogni snapshot di destinazione.

Se durante la copia di un'AMI si specificano i parametri di crittografia, puoi crittografare o crittografare di nuovo i suoi snapshot di supporto. L'esempio seguente mostra un caso non predefinito che fornisce parametri di crittografia all'operazione `CopyImage` per modificare lo stato di crittografia dell'AMI di destinazione.

Copia di un'AMI di origine non crittografata in un'AMI di destinazione crittografata

In questo scenario, un'AMI supportata da uno snapshot di root non crittografato viene copiato in un'AMI con uno snapshot di root crittografato. L'operazione `CopyImage` viene richiamata con due parametri di crittografia, inclusa una chiave gestita dal cliente. Di conseguenza, lo stato di crittografia dello snapshot root cambia, in modo che l'AMI di destinazione sia supportata da uno snapshot root contenente gli stessi dati dello snapshot di origine, ma crittografato utilizzando la chiave specificata. Ti verranno addebitati costi di archiviazione per gli snapshot in entrambe le AMI, nonché addebiti per tutte le istanze avviate da entrambe le AMI.

> **Note**
>
> L'abilitazione della crittografia per impostazione predefinita ha lo stesso effetto dell'impostazione del `Encrypted` parametro su `true` per tutte le istantanee nell'AMI.



L'impostazione del parametro `Encrypted` consente di crittografare il singolo snapshot per questa istanza. Se non specifichi il parametro `KmsKeyId`, per crittografare la copia snapshot viene utilizzata la chiave gestita dal cliente di default.

Per ulteriori informazioni sulla copia di AMIs con snapshot crittografati, consulta Utilizzo della crittografia con le AMI EBS-backed.

Archiviazione e ripristino di un'AMI utilizzando S3

Puoi archiviare un'Amazon Machine Image (AMI) in un bucket Amazon S3, copiare l'AMI in un altro bucket S3 e quindi ripristinarla dal bucket S3. Archiviando e ripristinando un'AMI utilizzando i bucket S3, puoi copiare le AMI da una AWS partizione all'altra, ad esempio dalla partizione commerciale principale alla partizione. AWS GovCloud (US) Potrai inoltre creare copie di archiviazione delle AMI memorizzandole in un bucket S3.

Le API supportate per la memorizzazione e il ripristino di un'AMI utilizzando S3 sono `CreateStoreImageTask`, `DescribeStoreImageTasks` e `CreateRestoreImageTask`.

`CopyImage`è l'API consigliata da utilizzare per copiare le AMI all'interno di una partizione. AWS Tuttavia, `CopyImage` non potrà copiare un'AMI in un'altra partizione.

Per informazioni sulle AWS partizioni, consulta *partition* nella pagina Amazon Resource Names (ARNs) nella IAM User Guide.

> **Warning**
>
> Assicurati di rispettare tutte le leggi e i requisiti aziendali applicabili quando sposti dati tra AWS partizioni o AWS regioni, inclusi, a titolo esemplificativo, le normative governative applicabili e i requisiti di residenza dei dati.

Argomenti

Casi d'uso

Utilizza le API di archiviazione e ripristino per effettuare le seguenti operazioni:

- Copiare un AMI da una AWS partizione all'altra AWS
- Creazione di copie di archiviazione delle AMI

Copiare un AMI da una AWS partizione all'altra AWS

Archiviando e ripristinando un'AMI utilizzando i bucket S3, puoi copiare un AMI da una AWS partizione all'altra o da una AWS regione all'altra. Nell'esempio seguente, si copia un AMI dalla partizione commerciale principale alla AWS GovCloud (US) partizione, in particolare dalla `us-east-2` regione alla `us-gov-east-1` regione.

Per copiare un'AMI da una partizione a un'altra, completa la seguente procedura:

- Archiviare l'AMI in un bucket S3 nella regione corrente utilizzando `CreateStoreImageTask`. In questo esempio, il bucket S3 si trova in `us-east-2`. Per un comando di esempio, consulta Archiviazione di un'AMI in un bucket S3.
- Monitorare lo stato di avanzamento dell'attività di archiviazione utilizzando `DescribeStoreImageTasks`. L'oggetto diventa visibile nel bucket S3 una volta completata l'attività. Per un comando di esempio, consulta Descrizione dello stato di avanzamento di un'attività di archiviazione AMI.
- Copiare l'oggetto AMI archiviato in un bucket S3 nella partizione di destinazione utilizzando una procedura a scelta. In questo esempio, l'S3 Bucket si trova in `us-gov-east-1`.

> **Note**
>
> Poiché sono necessarie AWS credenziali diverse per ogni partizione, non è possibile copiare un oggetto S3 direttamente da una partizione all'altra. Il processo per copiare un oggetto S3 tra le partizioni non rientra nell'ambito di questa documentazione. Forniamo i seguenti processi di copia come esempi, ma è necessario utilizzare il processo di copia che soddisfa i requisiti di sicurezza.
>
> - Per copiare un'AMI tra le partizioni, il processo di copia potrebbe essere semplice come il seguente: scarica l'oggetto dal bucket di origine su un host intermedio (ad esempio, un'istanza EC2 o un laptop), quindi carica l'oggetto dall'host intermedio al bucket di destinazione. Per ogni fase del processo, usa le AWS credenziali per la partizione.
> - Per un utilizzo più duraturo, è consigliabile sviluppare un'applicazione che gestisca le copie, potenzialmente utilizzando download e caricamenti multipart S3.

- Ripristinare l'AMI dal bucket S3 nella partizione di destinazione utilizzando `CreateRestoreImageTask`. In questo esempio, l'S3 Bucket si trova in `us-gov-east-1`. Per un comando di esempio, consulta Ripristino di un'AMI da un bucket S3.
- Monitorare l'avanzamento dell'attività di ripristino descrivendo l'AMI per verificare quando il relativo stato diventa disponibile. È inoltre possibile monitorare le percentuali di avanzamento degli snapshot che costituiscono l'AMI ripristinata descrivendo gli snapshot.

Creazione di copie di archiviazione delle AMI

È possibile creare copie di archiviazione delle AMI archiviandole in un bucket S3. Per un comando di esempio, consulta Archiviazione di un'AMI in un bucket S3.

L'AMI è incorporata in un singolo oggetto in S3 e tutti i metadati dell'AMI (escluse le informazioni di condivisione) vengono conservati come parte dell'AMI archiviata. I dati dell'AMI vengono compressi come parte del processo di archiviazione. Le AMI che contengono dati che possono essere facilmente compressi generano oggetti più piccoli in S3. Per ridurre i costi, è possibile utilizzare livelli di archiviazione S3 meno costosi. Per maggiori informazioni, consultare Classi di archiviazione di Amazon S3 e la pagina dei prezzi di Amazon S3.

Come funzionano le API di archiviazione e ripristino dell'AMI

Per memorizzare e ripristinare un'AMI utilizzando S3, utilizza le seguenti API:

- `CreateStoreImageTask`: memorizza l'AMI in un bucket S3
- `DescribeStoreImageTasks` –: fornisce lo stato di avanzamento dell'attività di archiviazione dell'AMI
- `CreateRestoreImageTask`: ripristina l'AMI da un bucket S3

Come funzionano le API

- CreateStoreImageTask
- DescribeStoreImageTasks
- CreateRestoreImageTask

CreateStoreImageTask

L'CreateStoreImageTaskAPI archivia un AMI come oggetto singolo in un bucket S3.

L'API crea un'attività che legge tutti i dati dall'AMI e dai relativi snapshot e quindi utilizza un caricamento in più parti S3 per archiviare i dati in un oggetto S3. L'API prende tutti i componenti dell'AMI, inclusa la maggior parte dei metadati dell'AMI non specifici della regione, e tutti gli snapshot EBS contenuti nell'AMI e li inserisce in un singolo oggetto in S3. I dati vengono compressi come parte del processo di caricamento in modo d ridurre la quantità di spazio utilizzato in S3, quindi l'oggetto in S3 potrebbe essere inferiore alla somma delle dimensioni degli snapshot nell'AMI.

Se sono presenti tag di AMI e snapshot visibili all'account che chiama questa API, questi saranno conservati.

L'oggetto in S3 ha lo stesso ID dell'AMI, ma con estensione `.bin`. I seguenti dati vengono memorizzati anche come tag di metadati S3 sull'oggetto S3: nome AMI, descrizione AMI, data di registrazione AMI, account proprietario AMI e un timestamp per l'operazione di archiviazione.

Il tempo necessario per completare l'attività dipende dalle dimensioni dell'AMI. Dipende anche dal numero delle altre attività in corso perché le attività vengono messe in coda. Puoi monitorare lo stato di avanzamento dell'attività chiamando l'DescribeStoreImageTasksAPI.

La somma delle dimensioni di tutte le AMI in corso è limitata a 600 GB di dati snapshot EBS per account. Un'ulteriore creazione di attività verrà rifiutata fino a quando le attività in corso non saranno inferiori al limite. Ad esempio, se un'AMI con 100 GB di dati snapshot e un'altra AMI con 200 GB di dati snapshot sono in fase di archiviazione, verrà accettata un'altra richiesta, poiché il totale in corso è 300 GB, che è inferiore al limite. Tuttavia, se una singola AMI con 800 GB di dati snapshot è in fase di archiviazione, ulteriori attività saranno rifiutate fino al completamento dell'attività.

DescribeStoreImageTasks

L'DescribeStoreImageTasksAPI descrive lo stato di avanzamento delle attività dell'archivio AMI. È possibile descrivere le attività per le AMI specificate. Se non si specificano le AMI, si ottiene un elenco impaginato di tutte le attività dell'immagine archivio che sono state elaborate negli ultimi 31 giorni.

Per ogni attività dell'AMI, la risposta indica se l'attività è `InProgress`, `Completed` o `Failed`. Per le attività `InProgress`, la risposta mostra uno stato di avanzamento in forma percentuale.

Le attività sono elencate in ordine cronologico inverso.

Al momento è possibile visualizzare solo le attività del mese precedente.

CreateRestoreImageTask

L'CreateRestoreImageTaskAPI avvia un'attività che ripristina un'AMI da un oggetto S3 precedentemente creato utilizzando una CreateStoreImageTaskrichiesta.

L'attività di ripristino può essere eseguita nella stessa regione o in una regione diversa in cui è stata eseguita l'attività di archiviazione.

Il bucket S3 da cui verrà ripristinato l'oggetto AMI deve trovarsi nella stessa regione in cui è richiesta l'attività di ripristino. L'AMI sarà ripristinata in questa regione.

L'AMI viene ripristinata con i relativi metadati, ad esempio il nome, la descrizione e i mapping dei dispositivi a blocchi corrispondenti ai valori dell'AMI archiviata. Il nome deve essere univoco per le AMI nella regione per questo account. Se non si fornisce un nome, la nuova AMI avrà lo stesso nome dell'AMI originale. L'AMI ottiene un nuovo ID AMI che viene generato al momento del processo di ripristino.

Il tempo necessario per completare l'attività di ripristino dell'AMI dipende dalle dimensioni dell'AMI. Dipende anche dal numero delle altre attività in corso perché le attività vengono messe in coda. È possibile visualizzare l'avanzamento dell'attività descrivendo l'AMI (describe-images) o i relativi snapshot EBS (describe-snapshot). Se l'attività non riesce, l'AMI e gli snapshot passano allo stato non riuscito.

La somma delle dimensioni di tutte le AMI in corso è limitata a 300 GB (in base alle dimensioni dopo il ripristino) dei dati snapshot EBS per account. Un'ulteriore creazione di attività verrà rifiutata fino a quando le attività in corso non saranno inferiori al limite.

Limitazioni

- Per archiviare un AMI, è Account AWS necessario possedere l'AMI e le relative istantanee oppure l'AMI e le relative istantanee devono essere condivisi direttamente con il proprio account. Non è possibile archiviare un'AMI se è condivisa solo pubblicamente.
- Solo le AMI EBS-backed possono essere archiviate utilizzando queste API.
- Le AMI paravirtual (PV) non sono supportate.
- La dimensione di un'AMI (prima della compressione) che può essere archiviata è limitata a 5.000 GB.
- Quota sulle richieste di immagini di archiviazione: 600 GB di lavoro di archiviazione (dati snapshot) in corso.
- Quota per le richieste di immagini di ripristino: 300 GB di lavoro di ripristino (dati snapshot) in corso.
- Per la durata dell'attività di archiviazione, gli snapshot non devono essere eliminati e l'entità IAM che esegue l'archiviazione deve avere accesso agli snapshot, altrimenti il processo di archiviazione avrà esito negativo.
- Non è possibile creare più copie di un'AMI nello stesso bucket S3.
- Un'AMI archiviata in un bucket S3 non può essere ripristinata con il suo ID AMI originale. È possibile mitigare questo effetto utilizzando l'alias AMI.
- Attualmente le API di archiviazione e ripristino sono supportate solo utilizzando gli AWS Command Line Interface AWS SDK e l'API Amazon EC2. Non è possibile archiviare e ripristinare un'AMI utilizzando la console Amazon EC2.

Costi

Quando si memorizzano e si ripristinano le AMI utilizzando S3, vengono addebitati i servizi utilizzati dalle API di archiviazione e ripristino e per il trasferimento dei dati. Le API utilizzano S3 e l'API

EBS Direct (utilizzata internamente da queste API per accedere ai dati delle snapshot). Per ulteriori dettagli, consulta Prezzi di Amazon S3 e Prezzi di Amazon EBS.

Protezione delle AMI

Per utilizzare le API di archiviazione e ripristino, il bucket S3 e l'AMI devono trovarsi nella stessa regione. È importante assicurarsi che il bucket S3 sia configurato con un livello di sicurezza sufficiente per proteggere il contenuto dell'AMI e che la sicurezza venga mantenuta per tutto il tempo che gli oggetti AMI rimangono nel bucket. Se ciò non è possibile, è preferibile non utilizzare queste API. Assicurarsi che non sia consentito l'accesso pubblico al bucket S3. Si consiglia di abilitare la crittografia lato server per il bucket S3 in cui si archiviano le AMI anche se non è necessario.

Per informazioni su come impostare le impostazioni di sicurezza appropriate per i bucket S3, consultare i seguenti argomenti sulla sicurezza:

- Blocco dell'accesso pubblico all'archiviazione Amazon S3
- Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3
- Quale policy sui bucket S3 posso utilizzare per rispettare la regola s3-? AWS Config bucket-ssl-requests-only
- Abilitazione della registrazione degli accessi al server Amazon S3

Quando gli snapshot AMI vengono copiati nell'oggetto S3, i dati vengono quindi copiati tramite connessioni TLS. È possibile archiviare le AMI con snapshot crittografati, ma gli snapshot vengono poi decrittografati come parte del processo di archiviazione.

Autorizzazioni per l'archiviazione e il ripristino di AMI utilizzando S3

Se le entità principali IAM archiviano o ripristinano le AMI utilizzando Amazon S3, devi concedere loro le autorizzazioni richieste.

La seguente policy di esempio include tutte le operazioni necessarie per consentire a un'entità IAM di eseguire le attività di archiviazione e ripristino.

Puoi anche creare policy IAM che consentono alle entità principali l'accesso solo a risorse specifiche. Per altre policy di esempio, consulta la sezione Gestione degli accessi alle AWS risorse nella IAM User Guide.

> **Note**
>
> Se gli snapshot che compongono l'AMI sono crittografati o se il tuo account è abilitato per la crittografia per impostazione predefinita, l'entità principale IAM deve disporre dell'autorizzazione per usare la chiave KMS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Utilizzo delle API di archiviazione e ripristino dell'AMI

Argomenti

- Archiviazione di un'AMI in un bucket S3

- Descrizione dello stato di avanzamento di un'attività di archiviazione AMI
- Ripristino di un'AMI da un bucket S3

Archiviazione di un'AMI in un bucket S3

Per archiviare un'AMI (AWS CLI)

Utilizza il comando create-store-image-task. Specificare l'ID AMI e il nome del bucket S3 in cui archiviare l'AMI.

```
aws ec2 create-store-image-task \
    --image-id ami-1234567890abcdef0 \
    --bucket DOC-EXAMPLE-BUCKET
```

Output previsto

```
{
  "ObjectKey": "ami-1234567890abcdef0.bin"
}
```

Descrizione dello stato di avanzamento di un'attività di archiviazione AMI

Per descrivere lo stato di avanzamento di un'attività di archiviazione AMI (AWS CLI)

Utilizza il comando describe-store-image-tasks.

```
aws ec2 describe-store-image-tasks
```

Output previsto

```
{
    "StoreImageTaskResults": [
        {
            "AmiId": "ami-1234567890abcdef0",
            "Bucket": "DOC-EXAMPLE-BUCKET",
            "ProgressPercentage": 17,
            "S3objectKey": "ami-1234567890abcdef0.bin",
            "StoreTaskState": "InProgress",
            "StoreTaskFailureReason": null,
            "TaskStartTime": "2022-01-01T01:01:01.001Z"
```

```
        }
    ]
}
```

Ripristino di un'AMI da un bucket S3

Per ripristinare un'AMI (AWS CLI)

Utilizza il comando create-restore-image-task. Utilizzando i valori per `S3ObjectKey` e `Bucket` dall'output `describe-store-image-tasks`, specificare la chiave oggetto dell'AMI e il nome del bucket S3 in cui è stata copiata l'AMI. Specificare anche un nome per l'AMI ripristinata. Il nome deve essere univoco per le AMI nella regione per questo account.

> **Note**
>
> L'AMI ripristinata ottiene un nuovo ID AMI.

```
aws ec2 create-restore-image-task \
    --object-key ami-1234567890abcdef0.bin \
    --bucket DOC-EXAMPLE-BUCKET \
    --name "New AMI Name"
```

Output previsto

```
{
   "ImageId": "ami-0eab20fe36f83e1a8"
}
```

Utilizzo dei percorsi dei file in S3

Puoi utilizzare i percorsi dei file durante l'archiviazione e il ripristino delle AMI, nel modo seguente:

- Quando si archivia un'AMI in S3, il percorso del file può essere aggiunto al nome del bucket. Internamente, il sistema separa il percorso dal nome del bucket e quindi aggiunge il percorso alla chiave oggetto generata per archiviare l'AMI. Il percorso completo di un oggetto è mostrato nella risposta di una chiamata API.
- Quando si ripristina l'AMI, poiché è disponibile un parametro della chiave oggetto, il percorso può essere aggiunto all'inizio del valore della chiave oggetto.

È possibile utilizzare i percorsi dei file quando si utilizzano gli SDK AWS CLI and.

Esempio: utilizza un percorso del file durante l'archiviazione e il ripristino di un'AMI (AWS CLI)

L'esempio seguente archivia innanzitutto un'AMI in S3, con il percorso del file aggiunto al nome del bucket. L'esempio ripristina quindi l'AMI da S3, con il percorso del file anteposto al parametro della chiave oggetto.

1. Archivia l'AMI. In `--bucket`, specifica il percorso del file dopo il nome del bucket, come riportato di seguito:

```
aws ec2 create-store-image-task \
    --image-id ami-1234567890abcdef0 \
    --bucket DOC-EXAMPLE-BUCKET/path1/path2
```

   Output previsto

```
{
  "ObjectKey": "path1/path2/ami-1234567890abcdef0.bin"
}
```

2. Ripristina l'AMI. In `--object-key`, specifica il valore dell'output del passaggio precedente, che include il percorso del file.

```
aws ec2 create-restore-image-task \
    --object-key path1/path2/ami-1234567890abcdef0.bin \
    --bucket DOC-EXAMPLE-BUCKET \
    --name "New AMI Name"
```

Dichiarazione di un'AMI come obsoleta

Puoi dichiarare un'AMI come obsoleta per indicare che non è aggiornata e non deve essere utilizzata. Puoi inoltre specificare una data di definizione come obsoleta futura per un'AMI, indicando da quando l'AMI non sarà più aggiornata. Ad esempio, è possibile dichiarare un'AMI come obsoleta se non è più gestita attivamente oppure se è stata sostituita da una versione più recente. Per impostazione predefinita, le AMI obsolete non vengono visualizzate negli elenchi AMI, impedendo ai nuovi utenti di utilizzare le AMI. out-of-date Tuttavia, gli utenti e i servizi di avvio esistenti, come i modelli di avvio e i gruppi Auto Scaling, possono continuare a utilizzare un'AMI obsoleta specificandone l'ID. Per

eliminare l'AMI in modo che gli utenti e i servizi non possano più utilizzarla, è necessario annullare la sua registrazione.

Dopo che un'AMI è stata dichiarata obsoleta:

- Per gli utenti AMI, l'AMI obsoleto non viene visualizzato DescribeImagesnelle chiamate API a meno che non ne specifichi l'ID o specifichi che devono apparire AMI obsolete. I proprietari di AMI continuano a vedere AMI obsolete nelle chiamate API. DescribeImages
- Per gli utenti delle AMI, l'AMI obsoleta non è disponibile per la selezione tramite la console EC2. Ad esempio, un'AMI obsoleta non viene visualizzata nel catalogo AMI nella procedura guidata di avvio istanze. I proprietari delle AMI continueranno a vedere le AMI obsolete nella console EC2.
- Per gli utenti delle AMI, se si conosce l'ID di un'AMI obsoleta, è possibile continuare ad avviare istanze con l'AMI obsoleta utilizzando l'API, la CLI o gli SDK.
- I servizi di avvio, come i modelli di avvio e i gruppi Auto Scaling, possono continuare a fare riferimento alle AMI obsolete.
- Le istanze EC2 che sono state avviate tramite un'AMI che viene successivamente dichiarata come obsoleta non sono interessate e possono essere arrestate, avviate e riavviate.

È possibile dichiarare obsolete sia le AMI pubbliche che quelle private.

Puoi inoltre creare policy AMI supportate da Amazon Data Lifecycle Manager EBS per rendere obsolete automaticamente le AMI EBS-backed. Per ulteriori informazioni, consulta Automatizzare i cicli di vita delle AMI.

> **Note**
>
> Di default, la data di obsolescenza di tutte le AMI pubbliche è impostata a due anni dalla data di creazione dell'AMI. È possibile impostare la data di obsolescenza prima dei due anni. Per annullare la data di deprecazione o per spostarla ulteriormente a una data successiva, è necessario rendere privata l'AMI solo condividendola con account AWS specifici.

Argomenti

- Descrizione di AMI obsolete
- Annullamento della dichiarazione di un'AMI come obsoleta

Costi

Quando si dichiara un'AMI obsoleta, l'AMI non viene eliminata. Il proprietario dell'AMI continuerà a pagare gli snapshot dell'AMI. Per interrompere il pagamento per gli snapshot, il proprietario dell'AMI deve eliminare l'AMI annullandone la registrazione.

Limitazioni

- Solo i proprietari dell'AMI possono dichiararla come obsoleta.

Dichiarazione di un'AMI come obsoleta

È possibile dichiarare un'AMI come obsoleta in una data e un'ora specifiche. Per eseguire questa procedura, è necessario essere il proprietario dell'AMI.

Console

Come dichiarare obsoleta un'AMI in una data specifica

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel navigatore a sinistra, scegli AMIs (AMI).
3. Nella barra del filtro, scegli Owned by me (Di mia proprietà).
4. Seleziona l'AMI, quindi scegli Actions (Operazioni), Manage AMI Deprecation (Gestisci deprecazione AMI). Puoi selezionare più AMI per impostare la stessa data di deprecazione di più AMI contemporaneamente.
5. Seleziona la casella di controllo Enable (Abilita) e poi inserisci la data e l'ora di deprecazione.

   Il limite massimo per la data di obsolescenza è di 10 anni dalla data attuale, tranne per le AMI pubbliche, per cui il limite superiore è 2 anni dalla data di creazione. Non puoi specificare una data passata.
6. Selezionare Salva.

AWS CLI

Come dichiarare obsoleta un'AMI in una data specifica

Utilizza il comando enable-image-deprecation. Specifica l'ID AMI e la data e l'ora in cui si desidera che l'AMI diventi obsoleta. Se specifichi un valore in secondi, Amazon EC2 arrotonda i secondi al minuto più vicino.

Il limite massimo per `deprecate-at` è 10 anni dalla data attuale, tranne per le AMI pubbliche, per cui il limite superiore è 2 anni dalla data di creazione. Non puoi specificare una data passata.

```
aws ec2 enable-image-deprecation \
    --image-id ami-1234567890abcdef0 \
    --deprecate-at "2021-10-15T13:17:12.000Z"
```

Output previsto

```
{
  "Return": "true"
}
```

Controlla quando un AMI è stato usato l'ultima volta

`LastLaunchedTime` è un timestamp che indica la data e l'ora dell'ultimo utilizzo dell'AMI per avviare un'istanza. Le AMI non utilizzate di recente per avviare un'istanza potrebbero essere candidate ideali per l'annullamento della registrazione o la dichiarazione come obsolete.

> **Note**
>
> - Quando si utilizza un'AMI per avviare un'istanza, il relativo utilizzo viene segnalato dopo 24 ore.
> - I dati `lastLaunchedTime` sono disponibili a partire da aprile 2017.

Console

Per visualizzare l'ultima data e ora di avvio di un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel navigatore a sinistra, scegli AMIs (AMI).
3. Nella barra del filtro, scegli Owned by me (Di mia proprietà).
4. Seleziona l'AMI e controlla il campo Last launched time (Ultima data e ora di avvio) (se hai selezionato la casella di controllo accanto all'AMI, si trova nella scheda Details [Dettagli]). Il campo mostra la data e l'ora dell'ultimo utilizzo dell'AMI per avviare un'istanza.

AWS CLI

Per visualizzare l'ultima data e ora di avvio di un'AMI

Esegui il describe-image-attributecomando e specifica`--attribute lastLaunchedTime`. Questa operazione può essere eseguita solo dal proprietario dell'AMI.

```
aws ec2 describe-image-attribute \
    --image-id ami-1234567890example \
    --attribute lastLaunchedTime
```

Output di esempio

```
{
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    },
    "ImageId": "ami-1234567890example",
}
```

Descrizione di AMI obsolete

Puoi visualizzare la data e l'ora di deprecazione di un'AMI e filtrare tutte le AMI per data di deprecazione. Puoi anche utilizzare il AWS CLI per descrivere tutte le AMI che sono state dichiarate obsolete, la cui data di deprecazione appartiene al passato.

Console

Per visualizzare la data di dichiarazione di un'AMI come obsoleta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel navigatore a sinistra, scegli AMIs (AMI) e quindi seleziona l'AMI.

3. Controlla il campo Deprecation time (Tempo di deprecazione) (se hai selezionato la casella di controllo accanto all'AMI, posizionata nella scheda Details [Dettagli]). Il campo mostra la data e l'ora di deprecazione dell'AMI. Se il campo è vuoto, l'AMI non è deprecata.

Per filtrare le AMI in base alla data di dichiarazione di un'AMI come obsoleta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel navigatore a sinistra, scegli AMIs (AMI).
3. Dalla barra del filtro, scegli Owned by me (Di mia proprietà) o Private images (Immagini private) (le immagini private includono AMI condivise con te e di tua proprietà).
4. Nella barra Search (Cerca) inserisci **`Deprecation time`** (mentre inserisci le lettere, viene visualizzato il filtro Deprecation time [Tempo di deprecazione]), quindi scegli un operatore, una data e un'ora.

AWS CLI

Quando si descrivono tutte le AMI utilizzando il comando describe-images, i risultati sono diversi a seconda che tu sia un utente dell'AMI o il proprietario dell'AMI.

- Se sei un utente dell'AMI:

  Per impostazione predefinita, quando si descrivono tutte le AMI utilizzando il comando describe-images, le AMI obsolete che non sono di proprietà dell'utente, ma che sono condivise con l'utente, non vengono visualizzate nei risultati. Ciò perché l'impostazione predefinita è `--no-include-deprecated`. Per includere AMI obsolete nei risultati, è necessario specificare il parametro `--include-deprecated`.
- Se sei il proprietario dell'AMI:

  Quando si descrivono tutte le AMI utilizzando il comando describe-images, tutte le AMI di cui si è proprietari, incluse le AMI obsolete, vengono visualizzate nei risultati. Non è necessario specificare il parametro `--include-deprecated`. Inoltre, non è possibile escludere le AMI obsolete di cui si è proprietari dai risultati utilizzando `--no-include-deprecated`.

Se un'AMI è obsoleta, nei risultati viene visualizzato il campo `DeprecationTime`.

> **Note**
>
> Un'AMI obsoleta è un'AMI la cui data di dichiarazione come obsoleta è nel passato. Se la data di dichiarazione come obsoleta è stata impostata su una data futura, l'AMI non è ancora obsoleta.

Come includere tutte le AMI dichiarate obsolete quando si descrivono tutte le AMI

Utilizza il comando describe-images e specifica il parametro `--include-deprecated` in modo da includere nei risultati tutte le AMI obsolete di cui non sei proprietario.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners 123456example
    --include-deprecated
```

Come descrivere la data di dichiarazione di un'AMI come obsoleta

Utilizza il comando describe-images e specifica l'ID dell'AMI.

Se si specifica `--no-include-deprecated` insieme all'ID AMI, l'AMI obsoleta sarà restituita nei risultati.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Output previsto

Il campo `DeprecationTime` riporta la data in cui l'AMI è impostata per essere considerata obsoleta. Se l'AMI non è impostata per essere obsoleta, il campo `DeprecationTime` non viene visualizzato nell'output.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
```

```
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "available",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2021-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Annullamento della dichiarazione di un'AMI come obsoleta

Puoi annullare la deprecazione di un'AMI, rimuovendo la data e l'ora dal campo Deprecation time (Tempo di deprecazione) (console) o il campo `DeprecationTime` dall'output describe-images (AWS CLI). Per eseguire questa procedura, è necessario essere il proprietario dell'AMI.

Console

Come annullare la dichiarazione di un'AMI come obsoleta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel navigatore a sinistra, scegli AMIs (AMI).
3. Nella barra del filtro, scegli Owned by me (Di mia proprietà).
4. Seleziona l'AMI, quindi scegli Actions (Operazioni), Manage AMI Deprecation (Gestisci deprecazione AMI). Puoi selezionare più AMI per annullare la deprecazione di più AMI contemporaneamente.
5. Deseleziona la casella di controllo Enable (Abilita), quindi scegli Save (Salva).

AWS CLI

Come annullare la dichiarazione di un'AMI come obsoleta

Usa il disable-image-deprecationcomando e specifica l'ID dell'AMI.

```
aws ec2 disable-image-deprecation \
    --image-id ami-1234567890abcdef0
```

Output previsto

```
{
  "Return": "true"
}
```

Disabilitazione di un'AMI

È possibile disabilitare un'AMI per impedirne l'utilizzo per gli avvii delle istanze. Non è possibile avviare nuove istanze da un'AMI disabilitata. È possibile riabilitare un'AMI disabilitata al fine di utilizzarla nuovamente per gli avvii delle istanze.

> **Warning**
>
> La disabilitazione di un'AMI rimuove tutte le relative autorizzazioni di avvio.

Quando un'AMI è disabilitata:

- Lo stato dell'AMI cambia in `disabled`.
- Non è possibile condividere un'AMI disabilitata. Se un'AMI in precedenza era pubblica o condivisa, viene resa privata. Se un'AMI è stata condivisa con un' Account AWS organizzazione o un'unità organizzativa, queste perdono l'accesso all'AMI disattivata.
- Per impostazione predefinita, un'AMI disabilitata non viene visualizzata nelle chiamate API DescribeImages.
- Un'AMI disabilitata non viene visualizzata nel filtro della console Di mia proprietà. Per trovare le AMI disabilitate, usa il filtro della console Immagini disabilitate.
- Non è possibile selezionare un'AMI disabilitata per gli avvii delle istanze nella console EC2. Ad esempio, un'AMI disabilitata non viene visualizzata nel catalogo AMI nella procedura guidata di avvio delle istanze o durante la creazione di un modello di istanza.
- I servizi di avvio, come i modelli di avvio e i gruppi con dimensionamento automatico, possono continuare a fare riferimento alle AMI obsolete. I successivi avvii delle istanze da un'AMI disattivata avranno esito negativo, quindi consigliamo di aggiornare i modelli di avvio e i gruppi con dimensionamento automatico in modo che facciano riferimento solo alle AMI disponibili.
- Le istanze EC2 che sono state avviate tramite un'AMI che viene successivamente disabilitata non sono interessate e possono essere arrestate, avviate e riavviate.
- Non è possibile eliminare snapshot associati alle AMI disabilitate. Il tentativo di eliminare uno snapshot associato restituisce l'errore `snapshot is currently in use`.

Quando un'AMI viene abilitata nuovamente:

- Lo stato dell'AMI cambia in `available` e può essere utilizzata per avviare le istanze.
- L'AMI può essere condivisa.
- Gli Account AWS, le organizzazioni e le unità organizzative che hanno perso l'accesso all'AMI quando era disabilitata non riottengono automaticamente l'accesso, ma è possibile condividere nuovamente l'AMI con loro.

È possibile disabilitare sia le AMI pubbliche sia quelle private.

Argomenti

- Costi

Costi

Quando si disabilita un'AMI, l'AMI non viene eliminata. Se l'AMI è supportata da EBS, continui a pagare per gli snapshot dei volumi EBS dell'AMI. Se desideri mantenere l'AMI, potresti essere in grado di ridurre i costi di archiviazione archiviando gli snapshot. Per ulteriori informazioni, consulta Archiviare gli snapshot di Amazon EBS nella Guida per l'utente di Amazon EBS. Se non si desidera conservare l'AMI e i relativi snapshot, è necessario annullare la registrazione dell'AMI ed eliminare gli snapshot. Per ulteriori informazioni, consulta Elimina le risorse associate alla tua AMI supportata da Amazon EBS.

Prerequisiti

Per disabilitare o riabilitare un'AMI, devi essere il proprietario dell'AMI.

Autorizzazioni IAM richieste

Per disabilitare e riabilitare un'AMI, devi disporre delle seguenti autorizzazioni IAM:

- `ec2:DisableImage`
- `ec2:EnableImage`

Disabilitazione di un'AMI

Puoi disabilitare un'AMI utilizzando la console EC2 o il AWS Command Line Interface (AWS CLI). Per eseguire questa procedura, è necessario essere il proprietario dell'AMI.

Console

Disabilitazione di un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI).
3. Nella barra del filtro, scegli Owned by me (Di mia proprietà).
4. Seleziona l'AMI, quindi scegli Operazioni, Disabilita AMI. È possibile selezionare più AMI per disabilitarle contemporaneamente.
5. Nella finestra Disabilita AMI, scegli Disabilita AMI.

AWS CLI

Disabilitazione di un'AMI

Utilizza il comando disable-image e specifica l'ID dell'AMI.

```
aws ec2 disable-image --image-id ami-1234567890abcdef0
```

Output previsto

```
{
  "Return": "true"
}
```

Descrizione delle AMI disabilitate

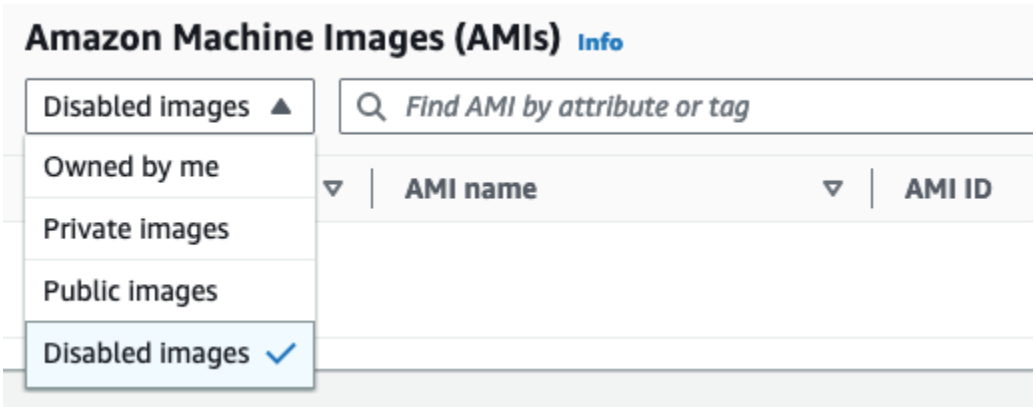
È possibile disabilitare un'AMI utilizzando la console EC2 oppure la AWS CLI.

Devi essere il proprietario delle AMI per visualizzare le AMI disabilitate. Poiché le AMI disabilitate vengono rese private, non puoi visualizzarle se non ne sei il proprietario.

Console

Visualizzazione delle AMI disabilitate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegli Immagini disattivate.



AWS CLI

Per impostazione predefinita, quando si utilizza il comando describe-images per descrivere tutte le AMI, le AMI disabilitate non vengono visualizzate nei risultati. Ciò perché l'impostazione predefinita è `--no-include-disabled`. Per includere le AMI disabilitate nei risultati, è necessario specificare il parametro `--include-disabled`.

Inclusione di tutte le AMI disabilitate quando si descrivono tutte le AMI

Utilizza il comando describe-images e specifica il parametro `--include-disabled` per recuperare le AMI disabilitate oltre a tutte le altre AMI. Facoltativamente, specifica `--owners self` per recuperare solo le AMI di cui sei proprietario.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners self
    --include-disabled
```

Se si specifica l'ID di un'AMI disabilitata ma non si specifica `--include-disabled`, l'AMI disabilitata viene restituita nei risultati.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Recupero delle sole AMI disabilitate

Specifica `--filters Name=state,Values=disabled`. È necessario specificare `--include-disabled`, altrimenti si ottiene un errore.

```
aws ec2 describe-images \
    --include-disabled \
    --filters Name=state,Values=disabled
```

Output di esempio

Il campo `State` mostra lo stato di un'AMI. `disabled` indica che l'AMI è disabilitata.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "disabled",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2023-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": false,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
```

```
        }
    ]
}
```

Riabilitazione di un'AMI disabilitata

È possibile abilitare nuovamente un'AMI disabilitata. Per eseguire questa procedura, è necessario essere il proprietario dell'AMI.

Console

Riabilitazione di un'AMI disabilitata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegli Immagini disattivate.
4. Seleziona l'AMI, quindi scegli Operazioni, Abilita AMI. È possibile selezionare più AMI per riabilitarle contemporaneamente.
5. Nella finestra Abilita AMI, scegli Abilita.

AWS CLI

Riabilitazione di un'AMI disabilitata

Utilizza il comando enable-image e specifica l'ID dell'AMI.

```
aws ec2 enable-image --image-id ami-1234567890abcdef0
```

Output previsto

```
{
  "Return": "true"
}
```

Archiviazione degli snapshot delle AMI

È possibile archiviare snapshot associati alle AMI supportate da EBS disabilitate. In questo modo è possibile ridurre i costi di archiviazione associati alle AMI utilizzate di rado, che devono essere conservate per lunghi periodi. Per ulteriori informazioni, consulta Archiviare gli snapshot di Amazon EBS nella Guida per l'utente di Amazon EBS.

Archiviazione degli snapshot associati a un'AMI

1. Disabilita l'AMI.
2. Archivia gli snapshot.

Non è possibile utilizzare un'AMI se è disabilitata e gli snapshot associati sono archiviati.

Ripristino di un'AMI disabilitata con snapshot archiviati da utilizzare

1. Ripristina le istantanee archiviate associate all'AMI.
2. Abilita l'AMI.

Annullare la registrazione (eliminare) un AMI

Quando annulli la registrazione di un'AMI, Amazon EC2 la elimina definitivamente. Una volta annullata la registrazione, non puoi utilizzare l'AMI per avviare nuove istanze. Potresti prendere in considerazione l'idea di annullare la registrazione di un'AMI quando hai finito di utilizzarla.

Per proteggerti dall'annullamento accidentale o doloso della registrazione di un AMI, puoi attivare la protezione dall'annullamento della registrazione. Se annulli accidentalmente la registrazione di un'AMI supportata da EBS, puoi utilizzare il Cestino per ripristinarla solo se la ripristini entro il periodo di tempo consentito prima che venga eliminata definitivamente.

L'annullamento della registrazione di un'AMI non ha alcun effetto sulle istanze avviate dall'AMI. È possibile continuare a utilizzare queste istanze. L'annullamento della registrazione di un'AMI non ha inoltre alcun effetto sulle istantanee create durante il processo di creazione dell'AMI. Continuerai a sostenere i costi di utilizzo per queste istanze e i costi di archiviazione per le istantanee. Pertanto, per evitare di incorrere in costi inutili, ti consigliamo di chiudere tutte le istanze ed eliminare le istantanee che non ti servono. Per ulteriori informazioni, consulta Evita i costi derivanti da risorse non utilizzate.

Indice

Considerazioni

- Non è possibile annullare la registrazione di un'AMI che non è di proprietà dell'account.
- Non puoi utilizzare Amazon EC2 per annullare la registrazione di un'AMI gestita dal servizio. AWS Backup Utilizza invece AWS Backup per eliminare i punti di ripristino corrispondenti nel vault di backup. Per ulteriori informazioni, consulta la sezione Eliminazione dei backup nella Guida per gli sviluppatori di AWS Backup .

Annullare la registrazione di un AMI

Utilizza uno dei seguenti metodi per annullare la registrazione di un AMI supportato da EBS o di un AMI basato su instance store-backed.

> **Tip**
>
> Per evitare di incorrere in costi inutili, è necessario eliminare tutte le risorse non necessarie. Ad esempio, per le AMI supportate da EBS, se non sono necessarie le istantanee associate all'AMI annullata, è necessario eliminarle. Per ulteriori informazioni, consulta Evita i costi derivanti da risorse non utilizzate.

Console

Per annullare la registrazione di un AMI

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegli Owned by me per elencare le AMI disponibili oppure scegli Immagini disattivate per elencare le AMI disabilitate.
4. Seleziona l'AMI per annullare la registrazione.

5. Scegli Actions (Operazioni), quindi Deregister AMI (Annulla registrazione AMI).
6. Quando ti viene richiesta la conferma, scegli Annulla registrazione AMI.

   Potrebbero essere necessari alcuni minuti prima che la console rimuova l'AMI dall'elenco. Scegliere Refresh (Aggiorna) per aggiornare lo stato.

AWS CLI

Per annullare la registrazione di un AMI

Usa il comando deregister-image e specifica l'ID dell'AMI per annullare la registrazione.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

Powershell

Per annullare la registrazione di un AMI

Utilizzare il Unregister-EC2Imagecmdlet e specificare l'ID dell'AMI per annullare la registrazione.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

Controlla quando un AMI è stato usato l'ultima volta

`LastLaunchedTime` è un timestamp che indica la data e l'ora dell'ultimo utilizzo dell'AMI per avviare un'istanza. Le AMI non utilizzate di recente per avviare un'istanza potrebbero essere candidate ideali per l'annullamento della registrazione o la dichiarazione come obsolete.

> **Note**
>
> - Quando si utilizza l'AMI per avviare un'istanza, il relativo utilizzo viene segnalato dopo 24 ore.
> - I dati `lastLaunchedTime` sono disponibili a partire da aprile 2017.

Console

Per visualizzare l'ultima data e ora di avvio di un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI).
3. Nella barra del filtro, scegli Owned by me (Di mia proprietà).
4. Seleziona l'AMI e controlla il campo Last launched time (Ultima data e ora di avvio) (se hai selezionato la casella di controllo accanto all'AMI, si trova nella scheda Details [Dettagli]). Il campo mostra la data e l'ora dell'ultimo utilizzo dell'AMI per avviare un'istanza.

AWS CLI

È possibile utilizzare il comando describe-images o il describe-image-attributecomando per visualizzare l'ora dell'ultimo avvio di un'AMI.

Per visualizzare l'ora dell'ultimo avvio di un'AMI utilizzando describe-images

Utilizza il comando describe-images e specifica l'ID dell'AMI.

```
aws ec2 describe-images --image-id ami-0123456789example
```

Output di esempio

> **Note**
>
> Il `LastLaunchedTime` campo appare solo nell'output delle AMI che possiedi.

```
{
    "Images": [
       {
           ...
           "LastLaunchedTime": {
               "Value": "2024-04-02T02:03:18Z"
           },
           ...
       }
   ]
```

```
}
```

Per visualizzare l'ultima data e ora di avvio di un'AMI

Usa il describe-image-attributecomando e specifica`--attribute lastLaunchedTime`. Devi essere il proprietario dell'AMI per eseguire questo comando.

```
aws ec2 describe-image-attribute \
    --image-id ami-0123456789example \
    --attribute lastLaunchedTime
```

Output di esempio

```
{
    "ImageId": "ami-1234567890example",
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    }
}
```

Proteggi un AMI dall'annullamento della registrazione

Puoi attivare la protezione dall'annullamento della registrazione su un'AMI per impedirne l'eliminazione accidentale o dolosa. Quando attivi la protezione dall'annullamento della registrazione, nessun utente può annullare la registrazione dell'AMI, indipendentemente dalle sue autorizzazioni IAM. Se desideri annullare la registrazione dell'AMI, devi prima disattivare la protezione dalla cancellazione dell'AMI.

Quando attivi la protezione dall'annullamento della registrazione su un AMI, hai la possibilità di includere un periodo di recupero di 24 ore. Questo periodo di recupero è il periodo durante il quale la protezione dall'annullamento della registrazione rimane attiva dopo la sua disattivazione. Durante questo periodo di recupero, non è possibile annullare la registrazione dell'AMI. Al termine del periodo di cooldown, è possibile annullare la registrazione dell'AMI.

La protezione dall'annullamento della registrazione è disattivata per impostazione predefinita su tutte le AMI nuove e esistenti.

Attiva la protezione dall'annullamento della registrazione

Utilizza uno dei seguenti metodi per attivare la protezione dall'annullamento della registrazione su un'AMI. Per fare ciò, devi essere il proprietario dell'AMI.

Console

Per attivare la protezione dall'annullamento della registrazione su un AMI

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegli Owned by me per elencare le AMI disponibili oppure scegli Immagini disattivate per elencare le AMI disabilitate.
4. Seleziona l'AMI su cui desideri attivare la protezione dall'annullamento della registrazione, quindi scegli Azioni, Gestisci la protezione dall'annullamento della registrazione AMI.
5. Nella finestra di dialogo Gestisci la protezione dall'annullamento della registrazione AMI, puoi attivare la protezione dall'annullamento della registrazione con o senza un periodo di recupero. Selezionare una delle seguenti opzioni:
   - Abilita con un periodo di recupero di 24 ore: con un periodo di recupero, l'AMI non può essere annullata per 24 ore quando la protezione dall'annullamento della registrazione è disattivata.
   - Abilita senza tempo di recupero: senza un periodo di recupero, l'AMI può essere immediatamente annullata quando la protezione dall'annullamento della registrazione è disattivata.
6. Selezionare Salva.

AWS CLI

Per attivare la protezione dall'annullamento della registrazione su un AMI

Usa il enable-image-deregistration-protectioncomando e specifica l'ID AMI. Per includere il periodo di recupero opzionale di 24 ore, includi `--with-cooldown` impostato `true` su. Per escludere il periodo di cooldown, omettete il parametro. `--with-cooldown`

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0123456789example \
    --with-cooldown true
```

Disattiva la protezione dall'annullamento della registrazione

Utilizza uno dei seguenti metodi per disattivare la protezione dall'annullamento della registrazione su un'AMI. Per fare ciò, devi essere il proprietario dell'AMI.

> **Note**
>
> Se hai scelto di includere un periodo di recupero di 24 ore quando hai attivato la protezione dall'annullamento della registrazione per l'AMI, quando disattivi la protezione dall'annullamento della registrazione, non potrai annullare immediatamente la registrazione dell'AMI. Il periodo di recupero è il periodo di 24 ore durante il quale la protezione dalla cancellazione della registrazione rimane attiva anche dopo averla disattivata. Durante questo periodo di recupero, non è possibile annullare la registrazione dell'AMI. Al termine del periodo di cooldown, è possibile annullare la registrazione dell'AMI.

Console

Per disattivare la protezione dall'annullamento della registrazione su un AMI

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegli Owned by me per elencare le AMI disponibili oppure scegli Immagini disattivate per elencare le AMI disabilitate.
4. Seleziona l'AMI per disattivare la protezione dall'annullamento della registrazione, quindi scegli Azioni, Gestisci la protezione dall'annullamento della registrazione AMI.
5. Nella finestra di dialogo Gestisci la protezione dalla cancellazione dell'AMI, scegli Disabilita.
6. Selezionare Salva.

AWS CLI

Per disattivare la protezione dall'annullamento della registrazione su un AMI

Usa il disable-image-deregistration-protectioncomando e specifica l'ID AMI.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0123456789example
```

Evita i costi derivanti da risorse non utilizzate

Quando si annulla la registrazione di un AMI, non si eliminano le risorse associate all'AMI. Queste risorse includono le istantanee per le AMI supportate da EBS e i file in Amazon S3, ad esempio le AMI supportate da storage. Quando annulli la registrazione di un'AMI, inoltre, non interrompi o interrompi alcuna istanza lanciata dall'AMI.

Continuerai a sostenere i costi per l'archiviazione delle istantanee e dei file e dovrai sostenere i costi per tutte le istanze in esecuzione. Per ulteriori informazioni, consulta Come vengono addebitati i costi.

Per evitare di incorrere in questi tipi di costi non necessari, ti consigliamo di eliminare tutte le risorse che non ti servono.

Per determinare se la tua AMI è supportata da EBS o da istanze archiviate, consulta. Determinare il tipo di dispositivo root dell'AMI

Elimina le risorse associate alla tua AMI supportata da Amazon EBS

Utilizza uno dei seguenti metodi per eliminare le risorse associate alla tua AMI supportata da EBS.

Console

Per eliminare le risorse associate alla tua AMI supportata da EBS

1. Annulla la registrazione dell'AMI.

   Prendi nota dell'ID AMI: questo può aiutarti a trovare le istantanee da eliminare nel passaggio successivo.
2. Elimina le istantanee che non ti servono.

   L'ID dell'AMI associata viene visualizzato nella colonna Descrizione della schermata Istantanee.
3. Termina le istanze che non ti servono.

AWS CLI

Per eliminare le risorse associate alla tua AMI supportata da EBS

1. Annulla la registrazione dell'AMI utilizzando il comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Elimina le istantanee che non ti servono utilizzando il comando delete-snapshot.

```
aws ec2 delete-snapshot --snapshot-id snap-0123456789example
```

3. Termina le istanze che non ti servono utilizzando il comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

PowerShell

Per eliminare le risorse associate alla tua AMI supportata da EBS

1. Annullare la registrazione dell'AMI utilizzando il Unregister-EC2Imagecmdlet.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

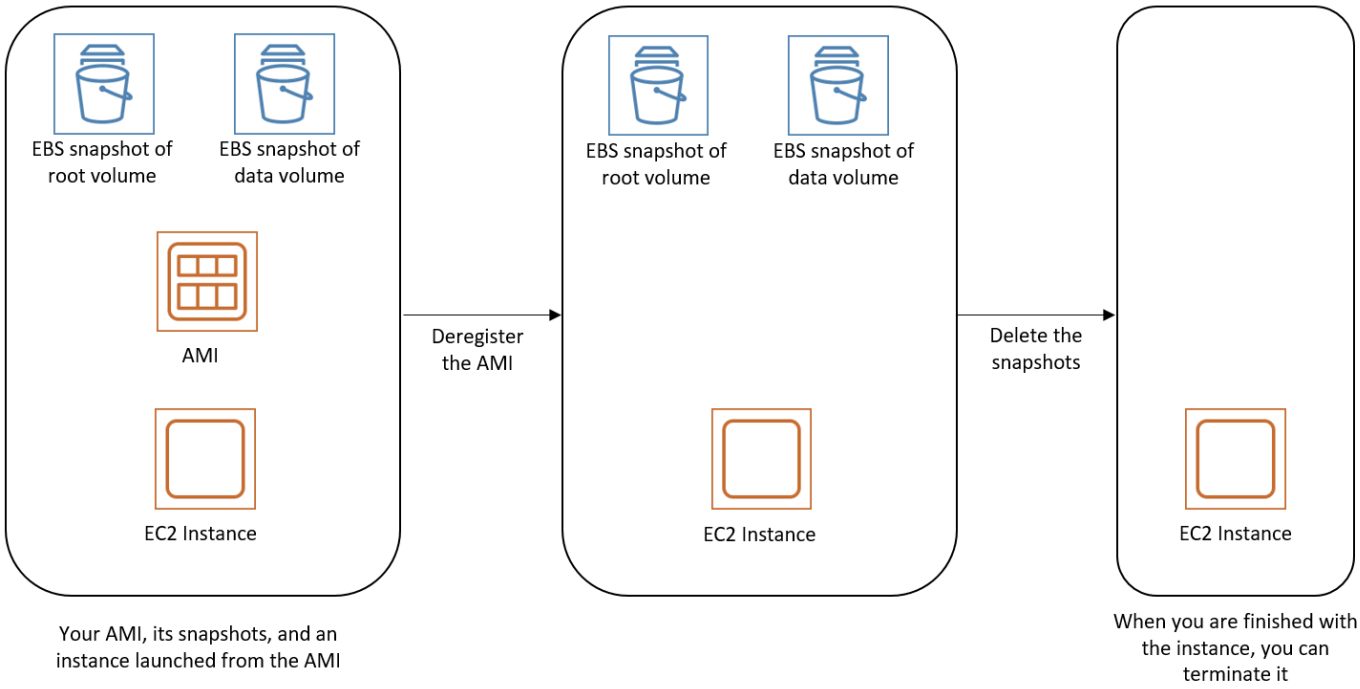
2. Eliminare le istantanee non necessarie utilizzando il cmdlet. Remove-EC2Snapshot

```
Remove-EC2Snapshot -SnapshotId snap-0123456789example
```

3. Termina le istanze che non ti servono utilizzando il cmdlet. Remove-EC2Instance

```
Remove-EC2Instance -InstanceId i-0123456789example
```

Il diagramma seguente illustra il flusso per eliminare le risorse associate a un'AMI supportata da EBS.



Eliminare le risorse associate all'AMI supportata da instance store-backed

Utilizza il seguente metodo per eliminare le risorse associate all'AMI con supporto store-backed dell'istanza.

Per eliminare le risorse associate all'AMI basata su instance store-backed

1. Annulla la registrazione dell'AMI utilizzando il comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Elimina il pacchetto in Amazon S3 utilizzando il comando ec2-delete-bundle (AMI tools).

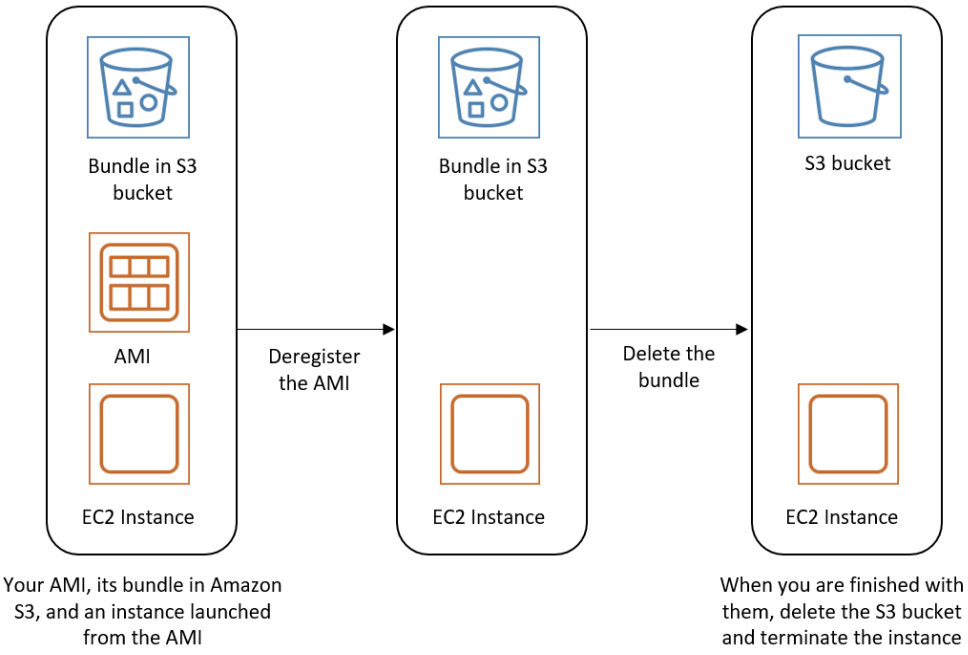
```
ec2-delete-bundle -b DOC-EXAMPLE-BUCKET/myami -a your_access_key_id -
s your_secret_access_key -p image
```

3. Termina le istanze che non ti servono utilizzando il comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

4. Se hai finito con il bucket Amazon S3 in cui hai caricato il pacchetto, puoi eliminare il bucket. Per eliminare un bucket Amazon S3, aprire la console Amazon S3, selezionare il bucket, scegliere Actions (Operazioni), quindi scegliere Delete (Elimina).

Il diagramma seguente illustra il flusso per eliminare le risorse associate all'AMI basato sullo store-backed dell'istanza.



Automatizzare il ciclo di vita AMI supportato da EBS

Puoi utilizzare Amazon Data Lifecycle Manager per creare, conservare, copiare, rendere obsolete ed eliminare automaticamente le AMI Amazon EBS-backed e i relativi snapshot di supporto. Per ulteriori informazioni, consulta Amazon Data Lifecycle Manager.

Utilizzo della crittografia con le AMI EBS-backed

Le AMI supportate dagli snapshot Amazon EBS possono utilizzare la crittografia Amazon EBS. Gli snapshot sia dei dati che dei volumi root possono essere crittografati e collegati a un'AMI. Puoi avviare le istanze e copiare le immagini con supporto completo della crittografia EBS. I parametri di crittografia per queste operazioni sono supportati in tutte le regioni in cui AWS KMS è disponibile.

Le istanze EC2 con volumi EBS crittografati vengono avviate dalle AMIs come le altre istanze. Inoltre, quando avvii un'istanza da una AMI basata su snapshot EBS non crittografati, puoi crittografare alcuni o tutti i volumi durante l'avvio.

Analogamente ai volumi EBS, le istantanee nelle AMI possono essere crittografate per impostazione predefinita AWS KMS key o su una chiave gestita dal cliente specificata dall'utente. In ogni caso, devi comunque disporre dell'autorizzazione per utilizzare la Chiave KMS selezionata.

Le AMI con istantanee crittografate possono essere condivise tra più account. AWS Per ulteriori informazioni, consulta AMI condivise.

Crittografia con gli argomenti AMI basati su EBS

- Scenari di avvio di istanze
- Scenari di copia delle immagini

Scenari di avvio di istanze

Le istanze Amazon EC2 vengono avviate dalle AMI utilizzando l'`RunInstances`azione con i parametri forniti tramite la mappatura dei dispositivi a blocchi, tramite o direttamente utilizzando l'API AWS Management Console o la CLI di Amazon EC2. Per ulteriori informazioni, consulta Mappatura dei dispositivi a blocchi. Per esempi di controllo della mappatura a blocchi dei dispositivi da AWS CLI, consulta Launch, List e Terminate EC2 Instances.

Per impostazione predefinita, senza parametri di crittografia espliciti, un'operazione `RunInstances` mantiene lo stato della crittografia esistente degli snapshot di origine di un'AMI e ripristina i volumi EBS da tali snapshot. Se la crittografia è abilitata per impostazione predefinita, tutti i volumi creati dall'AMI (da istantanee crittografate o non crittografate) vengono crittografati. Se la crittografia per impostazione predefinita non è abilitata, l'istanza mantiene lo stato di crittografia dell'AMI.

Puoi anche avviare un'istanza e contemporaneamente applicare un nuovo stato della crittografia ai restanti volumi fornendo i parametri di crittografia. Di conseguenza, si registrano i seguenti comportamenti:

Avvio senza parametri di crittografia

- Uno snapshot non crittografato viene ripristinato su un volume non crittografato, a meno che non sia abilitata la crittografia predefinita, nel cui caso tutti i volumi appena creati verranno crittografati.
- Uno snapshot crittografato di cui sei il proprietario viene ripristinato su un volume crittografato sulla stessa Chiave KMS.
- Un'istantanea crittografata che non possiedi (ad esempio, l'AMI è condivisa con te) viene ripristinata su un volume crittografato dalla chiave KMS predefinita del tuo AWS account.

I comportamenti predefiniti possono essere sovrascritti fornendo i parametri di crittografia. I parametri disponibili sono `Encrypted` e `KmsKeyId`. La sola impostazione del parametro `Encrypted` comporta le seguenti operazioni:

Comportamenti di avvio dell'istanza con **`Encrypted`** impostati, ma nessun **`KmsKeyId`** specificato

- Uno snapshot non crittografato viene ripristinato su un volume EBS crittografato dalla chiave KMS di default del tuo account AWS .
- Uno snapshot crittografato di cui sei il proprietario viene ripristinato su un volume EBS crittografato dalla stessa Chiave KMS. (Pertanto, il parametro `Encrypted` non ha alcun effetto.)
- Un'istantanea crittografata che non possiedi (ad esempio, l'AMI è condivisa con te) viene ripristinata su un volume crittografato dalla chiave KMS predefinita del tuo AWS account. (Pertanto, il parametro `Encrypted` non ha alcun effetto.)

L'impostazione dei parametri `Encrypted` e `KmsKeyId` consente di specificare una Chiave KMS non predefinita per un'operazione di crittografia. Risultano i seguenti comportamenti:

Viene impostata un'istanza con **`Encrypted`** e **`KmsKeyId`**

- Uno snapshot non crittografato viene ripristinato su un volume EBS crittografato dalla Chiave KMS specificata.
- Uno snapshot crittografato viene ripristinato su un volume EBS crittografato non sulla Chiave KMS originale, ma sulla Chiave KMS specificata.

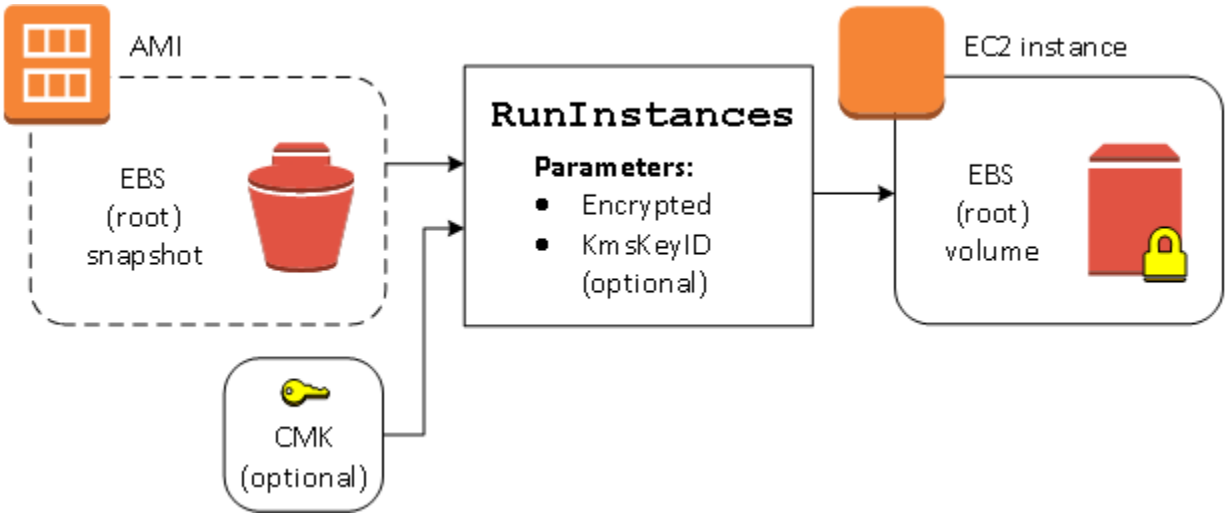
L'invio di `KmsKeyId` senza l'impostazione del parametro `Encrypted` causa un errore.

Le seguenti sezioni offrono esempi di avvio di istanze dalle AMI utilizzando parametri di crittografia non predefiniti. In ognuno dei seguenti scenari, i parametri forniti all'operazione `RunInstances` portano a un cambiamento dello stato della crittografia durante il ripristino di un volume da uno snapshot.

Per informazioni sull'utilizzo della console per avviare un'istanza da un'AMI, consulta Lancio dell'istanza.

Crittografia di un volume durante l'avvio

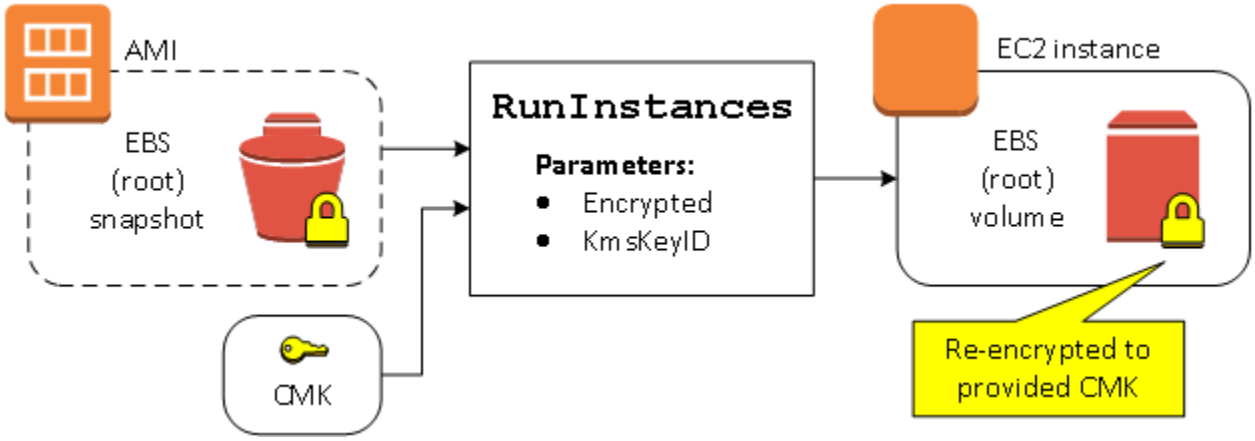
In questo esempio, viene utilizzata un'AMI basata su uno snapshot non crittografato per avviare un'istanza EC2 con un volume EBS crittografato.



Il parametro `Encrypted` da solo comporta la crittografia del volume per questa istanza. La fornitura di un parametro `KmsKeyId` è facoltativa. Se non viene specificato alcun ID di chiave KMS, per crittografare il volume viene utilizzata la chiave KMS predefinita dell' AWS account. Per crittografare il volume su una Chiave KMS diversa di tua proprietà, specifica il parametro `KmsKeyId`.

Nuova crittografia di un volume durante l'avvio

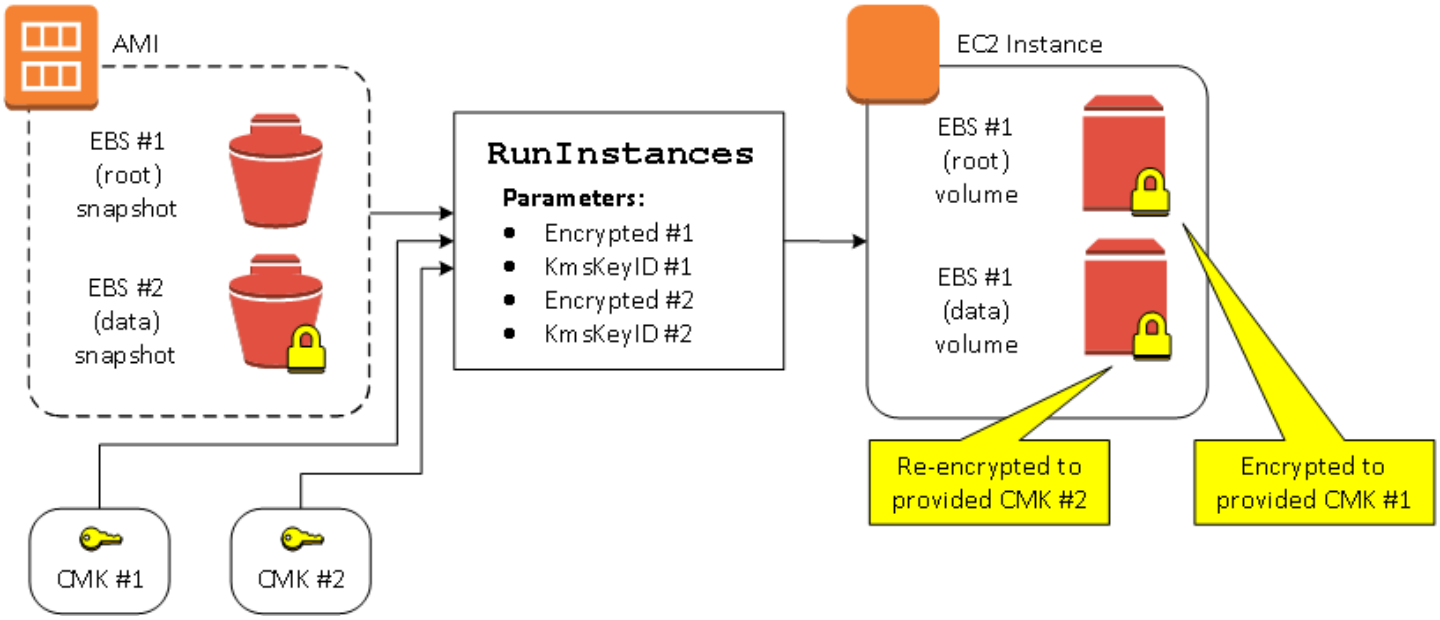
In questo esempio, viene utilizzata un'AMI basata su uno snapshot crittografato per avviare un'istanza EC2 con un volume EBS crittografato da una nuova Chiave KMS.



Se sei il proprietario dell'AMI e non fornisci parametri di crittografia, l'istanza risultante ha un volume crittografato dalla stessa Chiave KMS dello snapshot. Se invece condividi l'AMI anziché esserne il proprietario e non fornisci parametri di crittografia, il volume viene crittografato dalla Chiave KMS predefinita. Con i parametri di crittografia forniti come illustrato, il volume viene crittografato dalla Chiave KMS specificata.

Cambio dello stato della crittografia di più volumi durante l'avvio

In questo esempio più complesso, viene utilizzata un'AMI basata su più snapshot (ognuno con il proprio stato della crittografia) per avviare un'istanza EC2 con un volume appena crittografato e un volume crittografato nuovamente.



In questo scenario, l'operazione `RunInstances` viene fornita con parametri di crittografia per ognuno degli snapshot di origine. Quando sono specificati tutti i parametri di crittografia possibili, l'istanza risultante è la stessa indipendentemente dal fatto che tu sia il proprietario dell'AMI.

Scenari di copia delle immagini

Le AMI di Amazon EC2 sono copiate utilizzando l'operazione `CopyImage` tramite la AWS Management Console o utilizzando direttamente l'API o la CLI di Amazon EC2.

Per impostazione predefinita, senza parametri di crittografia espliciti, un'azione `CopyImage` mantiene lo stato della crittografia esistente degli snapshot di origine di un'AMI durante la copia. Puoi anche copiare un'AMI e contemporaneamente applicare un nuovo stato della crittografia agli snapshot EBS associati fornendo i parametri di crittografia. Di conseguenza, si registrano i seguenti comportamenti:

Copia senza parametri di crittografia

- Uno snapshot non crittografato viene copiato su un altro snapshot non crittografato, a meno che non sia abilitata la crittografia predefinita, nel cui caso tutti gli snapshot appena creati verranno crittografati.

- Uno snapshot crittografato di cui sei il proprietario viene copiato su uno snapshot crittografato con la stessa Chiave KMS.
- Un'istantanea crittografata di cui non sei proprietario (ovvero l'AMI è condivisa con te) viene copiata in un'istantanea crittografata dalla chiave KMS predefinita del tuo AWS account.

Tutti questi comportamenti predefiniti possono essere sovrascritti fornendo i parametri di crittografia. I parametri disponibili sono `Encrypted` e `KmsKeyId`. La sola impostazione del parametro `Encrypted` comporta le seguenti operazioni:

Comportamenti di copia dell'immagine con **`Encrypted`** impostati, ma nessun **`KmsKeyId`** specificato

- Uno snapshot non crittografato viene copiato su uno snapshot crittografato dalla chiave KMS di default dell'account AWS .
- Uno snapshot crittografato viene copiato su uno snapshot crittografato dalla stessa Chiave KMS. (Pertanto, il parametro `Encrypted` non ha alcun effetto.)
- Un'istantanea crittografata che non possiedi (ad esempio, l'AMI è condivisa con te) viene copiata su un volume crittografato dalla chiave KMS predefinita del tuo AWS account. (Pertanto, il parametro `Encrypted` non ha alcun effetto.)

L'impostazione di entrambi i parametri `Encrypted` e `KmsKeyId` consente di specificare una Chiave KMS gestita dal cliente per un'operazione di crittografia. Risultano i seguenti comportamenti:

Comportamenti di copia dell'immagine con **`Encrypted`** e **`KmsKeyId`** impostati

- Uno snapshot non crittografato viene copiato su uno snapshot crittografato dalla Chiave KMS specificata.
- Uno snapshot crittografato viene copiato su uno snapshot crittografato non sulla Chiave KMS originale, ma sulla Chiave KMS specificata.

L'invio di `KmsKeyId` senza l'impostazione del parametro `Encrypted` causa un errore.

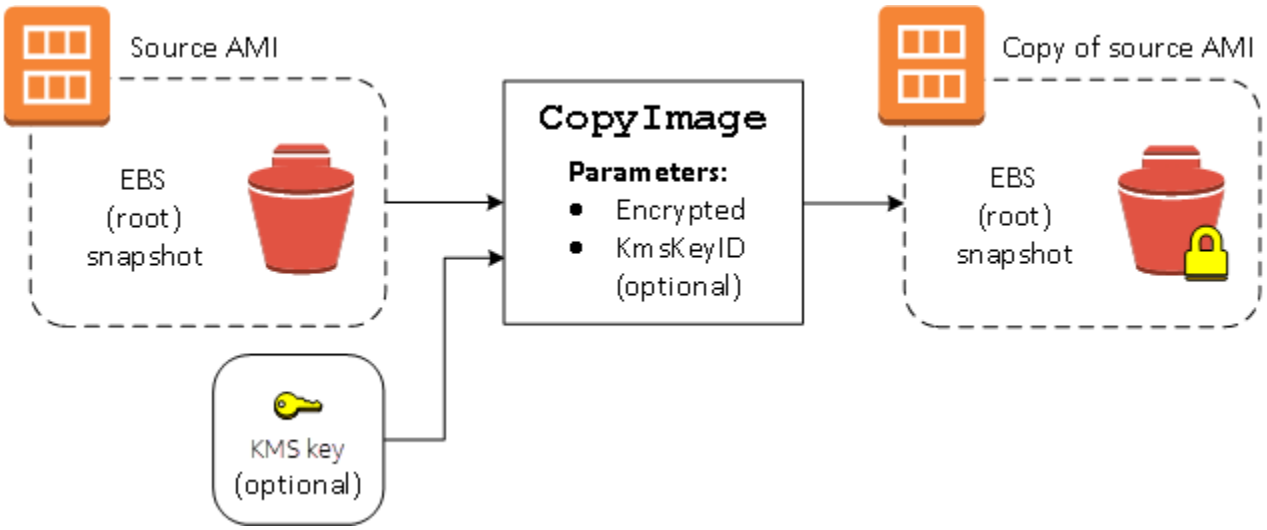
La seguente sezione offre un esempio della copia di un'AMI utilizzando parametri di crittografia non predefiniti, il che porta a una modifica dello stato di crittografia.

Per istruzioni dettagliate sull'utilizzo della console, consulta Copiare un'AMI.

Crittografia di un'immagine non crittografata durante la copia

In questo scenario, un'AMI supportata da uno snapshot di root non crittografato viene copiato in un'AMI con uno snapshot di root crittografato. L'operazione `CopyImage` viene richiamata con due parametri di crittografia, inclusa una chiave gestita dal cliente. Di conseguenza, lo stato di crittografia dello snapshot root cambia, in modo che l'AMI di destinazione sia supportata da uno snapshot root contenente gli stessi dati dello snapshot di origine, ma crittografato utilizzando la chiave specificata. Ti verranno addebitati costi di archiviazione per gli snapshot in entrambe le AMI, nonché addebiti per tutte le istanze avviate da entrambe le AMI.

> **Note**
>
> L'abilitazione della crittografia per impostazione predefinita ha lo stesso effetto dell'impostazione del `Encrypted` parametro su `true` per tutte le istantanee nell'AMI.



L'impostazione del parametro `Encrypted` consente di crittografare il singolo snapshot per questa istanza. Se non specifichi il parametro `KmsKeyId`, per crittografare la copia snapshot viene utilizzata la chiave gestita dal cliente di default.

> **Note**
>
> Puoi inoltre copiare un'immagine con più snapshot e configurare lo stato di crittografia di ognuno.

Monitora gli eventi AMI utilizzando Amazon EventBridge

Quando lo stato di un'Amazon Machine Image (AMI) cambia, Amazon EC2 genera un evento che viene inviato ad Amazon EventBridge (precedentemente noto come Amazon Events). CloudWatch Puoi usare Amazon EventBridge per rilevare e reagire a questi eventi. Puoi farlo creando regole EventBridge che attivano un'azione in risposta a un evento. Ad esempio, puoi creare una EventBridge regola che rileva quando il processo di creazione dell'AMI è completato e quindi richiama un argomento Amazon SNS per inviarti una notifica e-mail.

Amazon EC2 genera un evento quando un'AMI entra in uno dei seguenti stati:

- `available`
- `failed`
- `deregistered`
- `disabled`

La tabella seguente elenca le operazioni AMI e gli stati che un'AMI può assumere. Nella tabella, Sì indica gli stati che l'AMI può assumere quando viene eseguita l'operazione corrispondente.

Operazioni AMI	available	failed	deregistered	disabled
CopyImage	Sì	Sì		
CreateImage	Sì	Sì		
CreateRestoreImageTask	Sì	Sì		
DeregisterImage			Sì	
DisableImage				Sì
EnableImage	Sì			
RegisterImage	Sì	Sì		

Gli eventi vengono generati in base al miglior tentativo.

Argomenti

Eventi AMI

Gli eventi EC2 AMI State Change sono quattro:

- available
- failed
- deregistered
- disabled

Gli eventi vengono inviati al bus degli EventBridge eventi predefinito in formato JSON.

I campi seguenti dell'evento possono essere utilizzati per creare regole che attivano un'operazione:

`"source": "aws.ec2"`

Identifica che l'evento proviene da Amazon EC2.

`"detail-type": "EC2 AMI State Change"`

Identifica il nome dell'evento.

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

Il file fornisce le informazioni seguenti:

- L'ID AMI: se vuoi tenere traccia di un'AMI specifica.
- Lo stato dell'AMI (`available`, `failed`, `deregistered` oppure `disabled`).

`available`

Di seguito è illustrato un esempio di un evento generato da Amazon EC2 quando l'AMI assume lo stato `available` dopo un'operazione `CreateImage`, `CopyImage`, `RegisterImage`, `CreateRestoreImageTask` o `EnableImage` riuscita.

`"State": "available"` indica che l'operazione è riuscita.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

`failed`

Di seguito è illustrato un esempio di un evento generato da Amazon EC2 quando l'AMI assume lo stato `failed` dopo un'operazione `CreateImage`, `CopyImage`, `RegisterImage` o `CreateRestoreImageTask` non riuscita.

I campi seguenti forniscono informazioni pertinenti:

- `"State": "failed"`: indica che l'operazione non è riuscita.
- `"ErrorMessage": ""`: fornisce il motivo dell'operazione non riuscita.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "failed",
```

```
        "ErrorMessage": "Description of failure"
    }
}
```

deregistered

Di seguito è illustrato un esempio di un evento generato da Amazon EC2 quando l'AMI assume lo stato `deregistered` dopo un'operazione `DeregisterImage` riuscita. Se l'operazione ha esito negativo, non viene generato alcun evento. Qualsiasi errore viene comunicato immediatamente perché `DeregisterImage` è un'operazione sincrona.

`"State": "deregistered"` indica che l'operazione `DeregisterImage` è riuscita.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "deregistered",
        "ErrorMessage": ""
    }
}
```

disabled

Di seguito è illustrato un esempio di un evento generato da Amazon EC2 quando l'AMI assume lo stato `disabled` dopo un'operazione `DisableImage` riuscita. Se l'operazione ha esito negativo, non viene generato alcun evento. Qualsiasi errore viene comunicato immediatamente perché `DisableImage` è un'operazione sincrona.

`"State": "disabled"` indica che l'operazione `DisableImage` è riuscita.

```
{
```

```
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "disabled",
        "ErrorMessage": ""
    }
}
```

Crea EventBridge regole Amazon

Puoi creare una EventBridge regola Amazon che specifichi un'azione da intraprendere quando EventBridge riceve un evento che corrisponde al modello di evento nella regola. Quando un evento corrisponde, EventBridge invia l'evento al target specificato e attiva l'azione definita nella regola.

I modelli di eventi hanno la stessa struttura degli eventi a cui corrispondono. Un modello di eventi può corrispondere o meno a un evento.

Quando crei una regola per un evento di cambio di stato dell'AMI, puoi includere i seguenti campi nel modello di eventi:

`"source": "aws.ec2“`

Identifica che l'evento proviene da Amazon EC2.

`"detail-type": "EC2 AMI State Change"`

Identifica il nome dell'evento.

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

Il file fornisce le informazioni seguenti:

- L'ID AMI: se vuoi tenere traccia di un'AMI specifica.
- Lo stato dell'AMI (`available`, `failed`, `deregistered` oppure `disabled`).

Esempio: creare una EventBridge regola per inviare una notifica

L'esempio seguente crea una EventBridge regola per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando un AMI si trova nello `available` stato dopo che l'`CreateImage`operazione è stata completata correttamente.

Prima di creare la EventBridge regola, devi creare l'argomento Amazon SNS per l'e-mail, il messaggio di testo o la notifica push per dispositivi mobili.

Per creare una EventBridge regola per inviare una notifica quando un AMI viene creato e si trova nello **`available`** stato

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.
3. Per Define rule detail (Definisci dettagli della regola), effettua le seguenti operazioni:
   a. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.

      Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso bus di eventi.
   b. Per Event bus (Bus di eventi), scegli default. Quando un servizio AWS nell'account genera un evento, passa sempre al bus di eventi di default dell'account.
   c. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
   d. Seleziona Successivo.
4. Per Build event pattern (Crea modello di eventi), procedi come segue:
   a. Per Event source, scegli AWS eventi o eventi EventBridge partner.
   b. Per Event pattern (Modello di eventi), ai fini di questo esempio specificherai il seguente modello di eventi in modo che corrisponda a qualsiasi evento `EC2 AMI State Change` generato quando un'AMI entra nello stato `available`:

```
{
 "source": ["aws.ec2"],
 "detail-type": ["EC2 AMI State Change"],
 "detail": {"State": ["available"]}
}
```

Per aggiungere il modello di eventi, puoi utilizzare un modello scegliendo Event pattern form (Formato del modello di eventi) o specificare il tuo modello scegliendo Custom pattern (JSON editor) (Modello personalizzato (editor JSON)), come segue:

i. Per utilizzare un modello per creare il modello di eventi, procedi come segue:

A. Scegli Event pattern form (Formato del modello di eventi).

B. Per Event source (Origine evento), scegli AWS services (Servizi).

C. Per AWS Service (Servizio), scegli EC2.

D. Per Event type (Tipo di evento), scegli EC2 AMI State Change (Cambio stato AMI EC2).

E. Per personalizzare il modello, scegli Edit pattern (Modifica modello) e apporta le modifiche in modo che corrisponda al modello di eventi di esempio.

ii. Per specificare un modello di eventi personalizzato, procedi come segue:

A. Scegli Custom pattern (JSON editor) (Modello personalizzato (editor JSON)).

B. Nella casella Event pattern (Modello di eventi), aggiungi il modello di eventi per questo esempio.

c. Seleziona Successivo.

5. Per Select target(s) (Seleziona destinazione/i), esegui queste operazioni:

a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).

b. Per Select a target (Seleziona una destinazione, scegli SNS topic (Argomento SNS) per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando si verifica l'evento.

c. Per Argomento, scegliere un argomento esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) nella Amazon Simple Notification Service Developer Guide.

d. (Facoltativo) In Additional settings (Impostazioni aggiuntive), facoltativamente puoi configurare impostazioni aggiuntive. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi (passaggio 16) nella Amazon EventBridge User Guide.

e. Seleziona Successivo.

6. (Opzionale) Per Tags (Tag), se desideri puoi assegnare uno o più tag alla regola, quindi scegli Next (Successivo).
7. Per Review and create (Verifica e crea), procedi come segue:
   a. Verifica i dettagli della regola e modificali se necessario.
   b. Scegli Crea regola.

Per ulteriori informazioni, consulta i seguenti argomenti nella Amazon EventBridge User Guide:

- EventBridge Eventi Amazon
- Modelli di EventBridge eventi Amazon
- EventBridge Regole di Amazon

Per un tutorial su come creare una funzione Lambda e una EventBridge regola che esegua la funzione Lambda, consulta Tutorial: Log the state of an Amazon EC2 using in the Developer Guide. EventBridgeAWS Lambda

Comprendere le informazioni di fatturazione AMI

Quando lanci le istanze, puoi scegliere tra molte Amazon Machine Image (AMI) che supportano una varietà di piattaforme del sistema operativo e funzionalità. Per capire in che modo l'AMI che scegli all'avvio dell'istanza influisce sui profitti della AWS fattura, puoi cercare il sistema operativo, la piattaforma e le informazioni di fatturazione associate. Esegui questa operazione prima di avviare qualsiasi istanza on demand o Istanze spot o di acquistare una Istanza riservata.

Ecco due esempi di come ricercare la tua AMI in anticipo può aiutarti a scegliere l'AMI più adatta alle tue esigenze:

- Per Istanze spot, è possibile utilizzare i Dettagli della piattaforma per confermare che l'AMI è supportata per Istanze spot.
- Al momento dell'acquisto di una Istanza riservata, è possibile assicurarsi di selezionare la piattaforma del sistema operativo (Piattaforma) mappata ai Dettagli della piattaforma AMI.

Per ulteriori informazioni sui prezzi delle istanze, consulta Prezzi di Amazon EC2.

Indice

Campi informativi di fatturazione AMI

I seguenti campi forniscono informazioni di fatturazione associate a un'AMI:

Dettagli della piattaforma

I dettagli della piattaforma associati al codice di fatturazione dell'AMI. Ad esempio, `Red Hat Enterprise Linux`.

Operazione di utilizzo

L'operazione dell'istanza Amazon EC2 e il codice di fatturazione associato all'AMI. Ad esempio, `RunInstances:0010`. Le operazioni di utilizzo corrispondono alla colonna LineItem/Operation nel rapporto sui AWS costi e sull'utilizzo (CUR) e nell'API Price List.AWS

Puoi visualizzare questi campi nella pagina Istanze o AMI nella console Amazon EC2 o nella risposta restituita dal comando describe-images. Get-EC2Image

Dati di esempio: operazione di utilizzo per piattaforma

La tabella seguente elenca alcuni dettagli della piattaforma e valori delle operazioni di utilizzo che possono essere visualizzati nelle pagine Istanze o AMI nella console Amazon EC2 o nella risposta restituita dal comando describe-images. Get-EC2Image

Dettagli della piattaforma	Operazione di utilizzo 2
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0[3]
Red Hat Enterprise Linux	RunInstances:0010

Dettagli della piattaforma	Operazione di utilizzo 2
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise[1]	RunInstances:0102
Windows with SQL Server Standard[1]	RunInstances:0006

Dettagli della piattaforma	Operazione di utilizzo 2
Windows with SQL Server Web[1]	RunInstances:0202

[1] Se due licenze software sono associate a un'AMI, il campo Dettagli piattaforma le mostra entrambe.

[2] Se utilizzi istanze Spot, il valore riportato nel report lineitem/Operationsui AWS costi e sull'utilizzo potrebbe essere diverso dal valore dell'operazione di utilizzo elencato qui. Ad esempio, se `lineitem/Operation` viene visualizzato`RunInstances:0010:SV006`, significa che Amazon EC2 sta eseguendo Red Hat Enterprise Linux Spot Instance-hour negli Stati Uniti orientali (Virginia settentrionale) nella Zona 6.

[3] Viene visualizzato come RunInstances (Linux/UNIX) nei report di utilizzo.

Ricerca dei dettagli di fatturazione e utilizzo dell'AMI

Nella console Amazon EC2 è possibile visualizzare le informazioni di fatturazione AMI dalla pagina AMI o dalla pagina Istanze. Puoi anche trovare le informazioni di fatturazione utilizzando il servizio di metadati AWS CLI o l'istanza.

I seguenti campi possono aiutarti a verificare gli addebiti AMI in fattura:

- Dettagli della piattaforma
- Operazione di utilizzo
- ID ISTANZA AMI

Trovare le informazioni di fatturazione AMI (console)

Attieniti alla seguente procedura per visualizzare le informazioni di fatturazione AMI nella console Amazon EC2:

Cercare le informazioni di fatturazione AMI dalla pagina AMI

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di spostamento scegli AMI, e quindi seleziona un'AMI.
3. Nella scheda Details (Dettagli) controllare i valori per i Platform details (Dettagli della piattaforma) e Usage operation (Operazione di utilizzo).

Cercare le informazioni di fatturazione AMI dalla pagina Istanze

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione scegli Instances (Istanze) e quindi selezionarne una.
3. Nella scheda Dettagli (o nella scheda Descrizione, se si utilizza la versione precedente della console), controllare i valori di Dettagli della piattaforma e Operazioni di utilizzo.

Trovare le informazioni di fatturazione AMI (AWS CLI)

Per trovare le informazioni di fatturazione AMI utilizzando il AWS CLI, è necessario conoscere l'ID AMI. Se non si conosce l'ID AMI, è possibile ottenerlo dall'istanza utilizzando il comando describe-instances.

Per trovare l'ID AMI

Se si conosce l'ID istanza, è possibile ottenere l'ID AMI dell'istanza utilizzando il comando describe-instances.

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

Nell'output, l'ID AMI è specificato nel campo `ImageId`.

```
..."Instances": [
{
    "AmiLaunchIndex": 0,
    "ImageId": "ami-0123456789EXAMPLE",
    "InstanceId": "i-123456789abcde123",
    ...
}]
```

Per trovare le informazioni di fatturazione AMI

Se si conosce l'ID AMI, si può utilizzare il comando describe-images per visualizzare i dettagli della piattaforma AMI e delle operazioni di utilizzo.

```
$ aws ec2 describe-images --image-ids ami-0123456789EXAMPLE
```

L'output di esempio seguente mostra i campi `PlatformDetails` e `UsageOperation`. In questo esempio, la piattaforma AMI-0123456789EXAMPLEe è `Red Hat Enterprise Linux` e l'operazione di utilizzo e il codice di fatturazione è `RunInstances:0010`.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "Hypervisor": "xen",
            "EnaSupport": true,
            "SriovNetSupport": "simple",
            "ImageId": "ami-0123456789EXAMPLE",
            "State": "available",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "UsageOperation": "RunInstances:0010",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Verificare gli addebiti AMI in fattura

Per assicurarti di non sostenere costi imprevisti, puoi verificare che le informazioni di fatturazione per un'istanza nel tuo rapporto sui AWS costi e sull'utilizzo (CUR) corrispondano alle informazioni di fatturazione associate all'AMI che hai utilizzato per avviare l'istanza.

Per confermare le informazioni di fatturazione, trovare l'ID istanza nel CUR e controllare il valore corrispondente nella colonna `lineitem/Operation`. Il valore deve corrispondere al valore Operazione di utilizzo associato all'AMI.

Ad esempio, l'AMI `ami-0123456789EXAMPLE` dispone delle seguenti informazioni di fatturazione:

- Dettagli della piattaforma = `Red Hat Enterprise Linux`
- Operazione di utilizzo = `RunInstances:0010`

Se è stata avviata un'istanza utilizzando questa AMI, è possibile trovare l'ID istanza nel CUR e controllare il valore corrispondente nella colonna `lineitem/Operation`. In questo esempio, il valore dovrebbe essere `RunInstances:0010`.

Quote di AMI

Le quote seguenti si applicano alla creazione e alla condivisione di AMI. Le quote si applicano per Regione AWS.

Nome quota	Descrizione	Quota predefinita per regione
AMI	Il numero massimo di AMI pubbliche e private consentite per regione. Sono incluse le AMI disponibili, in sospeso e disabilitate e le AMI nel Cestino.	50.000
AMI pubbliche	Numero massimo di AMI pubbliche, incluse le AMI pubbliche nel Cestino, consentito per regione.	5

Nome quota	Descrizione	Quota predefinita per regione
Condivisione AMI	Numero massimo di entità (organizzazioni, unità organizzative e account) con cui può essere condivisa un'AMI in una regione. Tieni presente che se condividi un'AMI con un'organizzazione o un'unità organizzativa, il numero di account nell'orga nizzazione o nell'unità organizzativa non viene conteggiato ai fini della quota.	1.000

Se superi le quote e se vuoi creare o condividere altre AMI, hai queste opzioni:

- Se superi la quota totale di AMI o di AMI pubbliche, valuta la possibilità di rimuovere la registrazione delle immagini non utilizzate.
- Se superi la quota di AMI pubbliche, valuta la possibilità di rendere private una o più AMI pubbliche.
- Se superi la quota di condivisione di AMI, valuta la possibilità di condividere le AMI con un'organizzazione o un'unità organizzativa anziché con account separati.
- Richiedi un aumento delle quote per le AMI.

Richiedi un aumento delle quote per le AMI

Se hai bisogno di estendere la quota di default per le AMI, puoi richiedere un aumento della quota.

Richiedere un aumento delle AMI

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/
2. Nel pannello di navigazione, scegli Servizi AWS .
3. Scegli Amazon Elastic Compute Cloud (Amazon EC2) dall'elenco o digita il nome del servizio nel campo di ricerca.
4. Scegli la quota delle AMI per richiedere un aumento. Puoi scegliere tra:

- AMI
- AMI pubbliche
- Condivisione AMI

5. Scegliere Request quota increase (Richiedi aumento di quota).
6. Sotto Change quota value (Modifica il valore della quota), inserisci il nuovo valore della quota, quindi seleziona Request (Richiedi).

Per visualizzare eventuali richieste in sospeso o risolte di recente, scegliere Dashboard dal riquadro di navigazione. Per le richieste in sospeso, scegliere lo stato della richiesta per aprire la ricevuta della richiesta. Lo stato iniziale di una richiesta è Pending (In attesa). Quando la denominazione dello stato cambia in Quota requested (Quota richiesta), vedrai il numero della pratica al di sotto di Support Center case number (Numero del caso assegnato dal centro di supporto). Scegli il numero del caso per aprire il ticket della tua richiesta.

Dopo aver risolto la richiesta, il valore della quota applicata per la quota viene impostato sul nuovo valore.

Per maggiori informazioni, consulta Guida per l'utente di Service Quotas.

Istanze Amazon EC2

Prima di avviare un ambiente di produzione, è necessario rispondere alle domande seguenti.

D. Quale tipo di istanza soddisfa al meglio le mie esigenze?

Amazon EC2 fornisce diversi tipi di istanza per consentire di scegliere la CPU, la memoria, lo archiviazione e la capacità di rete che servono a eseguire le applicazioni. Per ulteriori informazioni, consulta Tipi di istanza Amazon EC2.

D. Quale opzione di acquisto soddisfa al meglio le mie esigenze?

Amazon EC2 supporta Istanze on demand (opzione predefinita), Istanze spot e Istanze riservate. Per ulteriori informazioni, consulta Opzioni di acquisto delle istanze.

D. Che tipo di volume root soddisfa al meglio le mie esigenze?

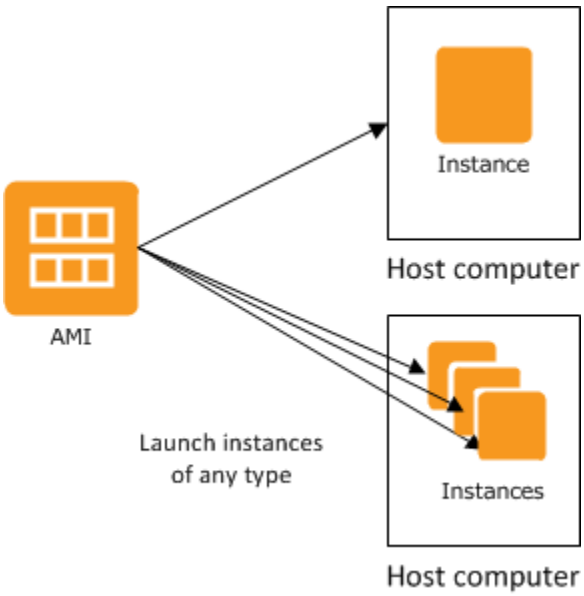
Ogni istanza è supportata da Amazon EBS oppure dall'instance store. Selezionare un'AMI in base al tipo di volume radice necessario. Per ulteriori informazioni, consulta Archiviazione del dispositivo root.

D. Posso gestire in remoto un parco istanze EC2 e delle macchine nel mio ambiente ibrido?

AWS Systems Manager ti consente di gestire in remoto e in modo sicuro la configurazione delle tue istanze Amazon EC2 e delle istanze e delle macchine virtuali (VM) locali in ambienti ibridi, comprese le VM di altri provider cloud. Per ulteriori informazioni, consulta la Guida per l'utente AWS Systems Manager.

Istanze e AMI

Un'Amazon Machine Image (AMI) è un modello che contiene una configurazione software (ad esempio un sistema operativo, un server di applicazioni e le applicazioni). Da un'AMI, puoi avviare un'istanza, ovvero una copia dell'AMI in esecuzione come server virtuale nel cloud. Puoi avviare più istanze di un'AMI, come mostrato nell'illustrazione seguente.



Le istanze continuano a essere eseguite finché non le arresti, le iberni o le termini o finché non si verifica un errore. Se un'istanza non va a buon fine, puoi avviarne una nuova dall'AMI.

Istanze

Un'istanza è un server virtuale nel cloud. La sua configurazione all'avvio è una copia dell'AMI specificata quando l'istanza è stata avviata.

Puoi avviare diversi tipi di istanze da una sola AMI. Un tipo di istanza determina fondamentalmente l'hardware del computer host utilizzato per l'istanza. Ciascun tipo di istanza offre diverse capacità di calcolo e memoria. Seleziona un tipo di istanza in base alla quantità di memoria e potenza di calcolo necessarie per l'applicazione o il software che intendi eseguire sull'istanza. Per le specifiche dettagliate del tipo di istanza, consulta la sezione Specifiche nella Amazon EC2 Instance Types Guide. Per informazioni sui prezzi, consulta la pagina dei prezzi on demand di Amazon EC2.

In seguito all'avvio, l'istanza appare come un host tradizionale con cui puoi interagire come faresti con un computer qualsiasi. Hai il controllo completo delle istanze; puoi utilizzare sudo per eseguire i comandi che richiedono privilegi root.

Il tuo AWS account ha un limite al numero di istanze che puoi avere in esecuzione. Per ulteriori informazioni su questo limite e su come richiedere che venga aumentato, consulta la sezione relativa al numero di istanze che è possibile eseguire in Amazon EC2 nella sezione delle domande frequenti generali di Amazon EC2.

Archiviazione della propria istanza

Il dispositivo root dell'istanza contiene l'immagine utilizzata per il suo avvio. Il dispositivo root è un volume Amazon Elastic Block Store (Amazon EBS) o un volume instance store. Per ulteriori informazioni, consulta Volumi root per le tue istanze Amazon EC2.

L'istanza può includere volumi di archiviazione locali, noti come volumi instance store, che puoi configurare al momento dell'avvio con la mappatura dei dispositivi a blocchi. Per ulteriori informazioni, consulta Mappatura dei dispositivi a blocchi. Dopo aver aggiunto ed effettuato la mappatura di questi volumi sull'istanza, questi ultimi sono disponibili per il montaggio e l'utilizzo. In caso di errore dell'istanza, o se l'istanza viene arrestata o terminata, i dati presenti su tali volumi andranno persi; pertanto, è consigliabile utilizzare questi volumi per i dati temporanei. Per proteggere i dati importanti, occorre utilizzare una strategia di replica su più istanze oppure archiviare i dati persistenti in Amazon S3 o sui volumi Amazon EBS. Per ulteriori informazioni, consulta Opzioni di archiviazione per le istanze Amazon EC2.

Best practice di sicurezza

- Usa AWS Identity and Access Management (IAM) per controllare l'accesso alle tue AWS risorse, comprese le istanze. Per ulteriori informazioni, consulta Identity and Access Management per Amazon EC2.
- Limita l'accesso consentendo soltanto agli host o alle reti attendibili di accedere alle porte sull'istanza. Ad esempio, puoi limitare l'accesso SSH limitando il traffico in entrata sulla porta 22. Per ulteriori informazioni, consulta Gruppi di sicurezza Amazon EC2 per le tue istanze EC2.
- Riconsulta abitualmente le regole nei gruppi di sicurezza e assicurati di applicare il principio del privilegio minimo: concedi soltanto le autorizzazioni necessarie. Puoi inoltre creare gruppi di sicurezza diversi per gestire le istanze con requisiti di sicurezza diversi. Prendi in considerazione la creazione di un gruppo di sicurezza bastion che consente gli accessi esterni e mantieni le istanze rimanenti in un gruppo che non consente gli accessi esterni.
- Disabilita gli accessi basati su password per le istanze avviate dall'AMI. Le password possono essere scoperte o decifrate e rappresentano un rischio per la sicurezza. Per ulteriori informazioni, consulta Disabilitazione degli accessi remoti basati su password per l'utente root. Per ulteriori informazioni sulla condivisione sicura delle AMI, consulta AMI condivise.

Arrestare e terminare le istanze

Puoi arrestare o terminare un'istanza in esecuzione in qualsiasi momento.

Arrestare un'istanza

Quando viene arrestata, l'istanza esegue un normale arresto e passa allo stato `stopped`. Tutti i volumi Amazon EBS rimangono collegati e puoi avviare nuovamente l'istanza in un secondo momento.

Non ti verrà addebitato alcun costo per l'utilizzo aggiuntivo dell'istanza quando questa è nello stato di arresto. Ti viene addebitato un costo per ogni transizione da uno stato interrotto a uno in esecuzione. Se il tipo di istanza è cambiato mentre l'istanza era interrotta, dopo l'avvio dell'istanza viene addebitata la tariffa per il nuovo tipo di istanza. Ti viene inoltre addebitato lo storage Amazon EBS associato alla tua istanza, incluso il volume del dispositivo root.

Quando un'istanza si trova nello stato di arresto, puoi collegare o distaccare i volumi Amazon EBS. Puoi inoltre creare un'AMI dall'istanza e modificare il kernel, il disco RAM e il tipo di istanza.

Terminare un'istanza

Quando viene terminata, l'istanza esegue un normale arresto. Il volume del dispositivo root viene eliminato per impostazione predefinita, ma i volumi Amazon EBS collegati vengono conservati per impostazione predefinita in base all'impostazione dell'attributo `deleteOnTermination` di ciascun volume. La stessa istanza viene eliminata e non puoi avviarla nuovamente in un secondo momento.

Per impedire le interruzioni accidentali, puoi disabilitare l'interruzione dell'istanza. In questo caso, assicurati che l'attributo `disableApiTermination` sia impostato su `true` per l'istanza. Per controllare il comportamento dell'arresto di un'istanza, come `shutdown -h` in Linux o `shutdown` in Windows, imposta l'attributo di istanza `instanceInitiatedShutdownBehavior` su `stop` o `terminate` come desiderato. Le istanze con i volumi Amazon EBS per il dispositivo root vengono impostate per impostazione predefinita su `stop` e le istanze con dispositivi root di instance store vengono sempre terminate come conseguenza dell'arresto dell'istanza.

Per ulteriori informazioni, consulta Ciclo di vita dell'istanza.

> **Note**
>
> Alcune AWS risorse, come i volumi Amazon EBS e gli indirizzi IP elastici, comportano costi indipendentemente dallo stato dell'istanza. Per ulteriori informazioni, consulta l'argomento Evitare costi inattesi nella Guida per l'utente AWS Billing . Per ulteriori informazioni sui costi di Amazon EBS, consulta Prezzi di Amazon EBS.

AMI

Amazon Web Services (AWS) pubblica Amazon Machine Images (AMI) che contengono configurazioni software comuni per uso pubblico. Inoltre, i membri della comunità di AWS sviluppatori hanno pubblicato le proprie AMI personalizzate. Puoi anche creare le tue AMI personalizzate; in questo modo puoi avviare rapidamente e facilmente nuove istanze con tutto ciò di cui hai bisogno. Ad esempio, se l'applicazione è un sito Web o un servizio Web, l'AMI può includere un server Web, il contenuto statico associato e il codice delle pagine dinamiche. Come risultato, dopo aver avviato un'istanza da questa AMI, il server Web si avvia e la tua applicazione è pronta ad accettare richieste.

Tutte le AMI vengono categorizzate come con supporto Amazon EBS, che indica che il dispositivo root per un'istanza avviata dall'AMI è un volume Amazon EBS, o come con supporto instance store, che indica che il dispositivo root per un'istanza inviata dall'AMI è un volume instance store creato da un modello archiviato in Amazon S3.

Nella descrizione dell'AMI è indicato il tipo di dispositivo root (`ebs` o `instance store`). Si tratta di un'informazione importante perché esistono differenze significative in merito alle operazioni che è possibile effettuare con ciascun tipo di AMI. Per ulteriori informazioni su queste differenze, consulta Archiviazione del dispositivo root.

Puoi annullare la registrazione di un'AMI quando hai terminato di utilizzarla. Dopo aver annullato la registrazione di un'AMI, non puoi più utilizzarla per avviare nuove istanze. Le istanze esistenti avviate dall'AMI non saranno interessate da questa operazione. Pertanto, quando hai finito di utilizzare le istanze avviate con queste AMI, ti consigliamo di terminarle.

Tipi di istanza Amazon EC2

Quando si avvia un'istanza, il tipo di istanza specificato determina l'hardware del computer host utilizzato per tale istanza. Ogni tipo di istanza è caratterizzato da diverse capacità di calcolo, memoria e archiviazione ed è raggruppato in famiglie di istanze basate su tali capacità. Seleziona un tipo di istanza in base ai requisiti dell'applicazione o del software che intendi eseguire sull'istanza.

Amazon EC2 dedica alcune risorse del computer host, come CPU, memoria e archiviazione dell'istanza, a un'istanza specifica. Amazon EC2 condivide altre risorse del computer host, ad esempio la rete e il sottosistema del disco, tra le istanze. Se ogni istanza in un computer host cerca di utilizzare la maggior quantità possibile di queste risorse condivise, a ciascuna istanza viene assegnata la stessa quantità di una risorsa. Tuttavia, quando viene utilizzata una quantità inferiore di una risorsa, un'istanza potrà utilizzare una quantità maggiore di tale risorsa in base alla sua disponibilità.

Ogni tipo di istanza fornisce prestazioni minime inferiori o superiori in base a una risorsa condivisa. Ad esempio, i tipi di istanza con prestazioni I/O elevate si avvalgono di un'allocazione maggiore di risorse condivise. L'allocazione di una maggiore quantità di risorse condivise riduce inoltre la varianza delle prestazioni I/O. Per la maggior parte delle applicazioni, prestazioni I/O modeste sono più che sufficienti. Tuttavia, per le applicazioni che richiedono prestazioni I/O più alte o maggiormente costanti, valuta l'ipotesi di utilizzare un tipo di istanza con prestazioni I/O maggiori.

Indice

Tipi di istanza disponibili

Amazon EC2 offre un'ampia selezione di tipi di istanza ottimizzati per adattarsi a diversi casi d'uso. I tipi di istanza comprendono diverse combinazioni di CPU, memoria, archiviazione e capacità di rete, inoltre offrono la flessibilità necessaria per scegliere la combinazione di risorse appropriata per le applicazioni. Ogni tipo di istanza include una o più dimensioni di istanza, che consentono di scalare le risorse in base ai requisiti del carico di lavoro di destinazione. Per ulteriori informazioni sulle caratteristiche e sui casi d'uso, consulta i dettagli sui tipi di istanze di Amazon EC2.

Convenzioni di denominazione dei tipi di istanza

I nomi si basano sulla famiglia di istanze, sulla generazione, sulla famiglia di processori, sulle capacità e sulle dimensioni. Per ulteriori informazioni, consulta le convenzioni di denominazione nella Amazon EC2 Instance Types Guide.

Individuazione di un tipo di istanza

Per determinare quali tipi di istanza soddisfano i tuoi requisiti, ad esempio regioni supportate, risorse di calcolo o risorse di storage, consulta Individuazione di un tipo di istanza Amazon EC2 le specifiche del tipo di istanza Amazon EC2 nella Amazon EC2 Instance Types Guide.

Istanze della generazione attuale

- Uso generale: M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6a | M6g | M6gD | M6i | M6iD | M6idn | M6in | M7a | M7g | M7i | M7i-Flex | Mac1 | Mac2 | MAC2-M1Ultra | Mac2-M2 | Mac2-M2 Pro | T2 | T3 | T3a | T4G
- Elaborazione ottimizzata: C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6gn | C6i | C6id | C6in | C7a | C7g | C7gd | C7gn | C7i | C7i-flex
- Memoria ottimizzata: R5 | R5a | R5ad | R5b | R5d | R5dn | R6a | R6g | R6gd | R6i | R6idn | R6in | R6id | R7a | R7g | R7gd | R7i | R7iZ | R8g | U-3TB1 | U-6TB1 | U-9TB1 | U-12TB1 | U-18TB1 | U-24TB1 | U7i-12TB | U7in-16TB | U7in-24TB | U7in-32TB | X1 | X2gD | X2idn | X2iEzn | X1e | z1d
- Archiviazione ottimizzata: D2 | D3 | D3en | H1 | I3 | I3en | i4G | i4i | Im4gn | IS4Gen
- Calcolo accelerato: DL1 | DL2q | F1 | G4ad | G4dn | G5 | G5g | G6 | Gr6 | Inf1 | Inf2 | P2 | P3 | P3dn | P4d | P4de | P5 | Trn1 | TRN1n | VT1
- Elaborazione ad alte prestazioni: HPC6a | HPC6id | HPC7a | HPC7g

Istanze di generazioni precedenti

- Uso generale: A1 | M1 | M2 | M3 | M4 | T1
- Ottimizzato per il calcolo: C1 | C3 | C4
- Memoria ottimizzata: R3 | R4
- Archiviazione ottimizzata: I2
- Elaborazione accelerata: G3

Specifiche dell'hardware

Per le specifiche dettagliate del tipo di istanza, consulta la sezione Specifiche nella Amazon EC2 Instance Types Guide. Per informazioni sui prezzi, consulta la pagina dei prezzi on demand di Amazon EC2.

Per determinare il tipo di istanza più idoneo alle specifiche esigenze, ti consigliamo di avviare un'istanza e utilizzare la tua applicazione per il benchmark. Dal momento che l'addebito dei costi viene calcolato al secondo, è più conveniente eseguire il test di più tipi di istanza prima di prendere una decisione. Se le esigenze cambiano nel tempo dopo una decisione specifica, si potrà sempre ridimensionare l'istanza in un secondo momento. Per ulteriori informazioni, consulta Cambiare il tipo di istanza.

Caratteristiche del processore Intel

Le istanze Amazon EC2 che vengono eseguite su processori Intel possono includere le seguenti funzionalità. Non tutte le seguenti funzionalità del processore sono supportate da tutti i tipi di istanza. Per informazioni dettagliate sulle funzionalità disponibili per ogni tipo di istanza, consulta Tipi di istanze Amazon EC2.

- Intel AES New Instructions (AES-NI) — Il set di istruzioni di crittografia Intel AES-NI è migliorato rispetto all'algoritmo originale Advanced Encryption Standard (AES), garantendo così protezione dei dati più rapida e maggiore sicurezza. Tutte le istanze EC2 di attuale generazione supportano questa caratteristica del processore.
- Advanced Vector Extension di Intel (Intel AVX, Intel AVX2 e Intel AVX-512) — Intel AVX e Intel AVX2 sono estensioni dei set di istruzioni a 256 bit, e Intel AVX-512 a 512 bit, per applicazioni con elevate esigenze di calcoli in virgola mobile. Le istruzioni Intel AVX migliorano le prestazioni per applicazioni come elaborazione di immagini e audio/video, simulazioni scientifiche, analisi finanziarie e modelli e analisi 3D. Queste funzionalità sono disponibili solo su istanze avviate con AMI HVM.
- Tecnologia Intel Turbo Boost — I processori Intel Turbo Boost eseguono automaticamente i core più velocemente della frequenza operativa di base.
- Intel Deep Learning Boost (Intel DL Boost) — Accelera i casi d'uso di deep learning AI. I processori Intel Xeon Scalable di seconda generazione estendono Intel AVX-512 con una nuova istruzione di rete neurale vettoriale (VNNI/INT8) che aumenta significativamente le prestazioni di inferenza di deep learning rispetto ai corrispettivi processori di precedente generazione (con FP32), per riconoscimento/segmentazione di immagini, rilevamento di oggetti, riconoscimento vocale, traduzione linguistica, sistemi di raccomandazione, apprendimento per rinforzo e altro ancora. VNNI potrebbe non essere compatibile con tutte le distribuzioni di Linux.

  Le istanze seguenti supportano VNNI: `M5n`, `R5n`, `M5dn`, `M5zn`, `R5b`, `R5dn`, `D3`, `D3en` e `C6i`. Le istanze `C5` e `C5d` supportano VNNI solo per le istanze `12xlarge`, `24xlarge` e `metal`.

Tuttavia, potrebbe sorgere un certo livello di confusione a causa delle convenzioni di denominazione standard per le CPU a 64 bit. Il produttore di chip Advanced Micro Devices (AMD) ha introdotto la prima architettura a 64 bit di successo basata sul set di istruzioni Intel x86. Di conseguenza, a questo tipo di architettura viene in genere fatto riferimento con AMD64, indipendentemente dal produttore. Windows e numerose distribuzioni Linux si conformano a questo standard. Ciò spiega il motivo per

cui nelle informazioni sul sistema esterno in un'istanza EC2 in Ubuntu o Windows l'architettura della CPU viene definita come AMD64, anche se le istanze vengono eseguite su hardware Intel.

AWS Processori Graviton

AWS Graviton è una famiglia di processori progettata per offrire il miglior rapporto prezzo/prestazioni per i carichi di lavoro in esecuzione su istanze Amazon EC2.

Per ulteriori informazioni, consulta Guida introduttiva a Graviton.

AWS Trainium

Le istanze basate su AWS Trainium sono progettate appositamente per una formazione di deep learning ad alte prestazioni ed economica. È possibile utilizzare queste istanze per addestrare l'elaborazione del linguaggio naturale, la visione artificiale e i modelli di raccomandazione utilizzati in un'ampia gamma di applicazioni, come il riconoscimento vocale, la raccomandazione, il rilevamento delle frodi e la classificazione di immagini e video. Utilizza i flussi di lavoro esistenti nei framework ML più diffusi, come e. PyTorch TensorFlow

AWS Inferentia

Le istanze basate su AWS Inferentia sono progettate per accelerare l'apprendimento automatico. Forniscono inferenze di machine learning ad alte prestazioni e bassa latenza. Queste istanze sono ottimizzate per la distribuzione di modelli di Deep Learning (DL) per applicazioni, quali l'elaborazione del linguaggio naturale, il rilevamento e la classificazione degli oggetti, la personalizzazione e il filtro dei contenuti e il riconoscimento vocale.

È possibile iniziare in diversi modi:

- Use SageMaker, un servizio completamente gestito che è il modo più semplice per iniziare a utilizzare i modelli di machine learning. Per ulteriori informazioni, consulta Get Started with SageMaker nella Amazon SageMaker Developer Guide.
- Avvia un'istanza Inf1 o Inf2 utilizzando l'AMI Deep Learning. Per ulteriori informazioni, consulta AWS Inferentia con DLAMI nella Guida per gli sviluppatori di AWS Deep Learning AMI .
- Avvia un'istanza Inf1 o Inf2 utilizzando la tua AMI e installa l'SDK AWS Neuron, che consente di compilare, eseguire e profilare modelli di deep learning per AWS Inferentia.
- Avvia un'istanza di container utilizzando un'istanza Inf1 o Inf2 e un'AMI ottimizzata per Amazon ECS. Per ulteriori informazioni, consulta AMI Amazon Linux 2 (Inferentia) in Amazon Elastic Container Service Developer Guide.

- Creare un cluster Amazon EKS con nodi che eseguono istanze Inf1. Per maggiori informazioni, consulta Supporto Inferentia nella Guida per l'utente di Amazon EKS.

Tipi di virtualizzazione dell'AMI

Il tipo di virtualizzazione dell'istanza viene determinato dall'AMI utilizzata per avviarla. I tipi di istanza della generazione corrente supportano solo la tipologia HVM (Hardware Virtual Machine). Alcuni tipi di istanze della generazione precedente supportano le istanze paravirtuali (PV) e alcune AWS regioni supportano le istanze PV. Per ulteriori informazioni, consulta Tipi di virtualizzazione dell'AMI.

Per ottenere prestazioni migliori, ti consigliamo di usare un'AMI HVM. Inoltre, è consigliabile utilizzare le AMI HVM se desideri sfruttare le funzionalità avanzate di rete. La virtualizzazione HVM utilizza la tecnologia di assistenza hardware fornita dalla piattaforma. AWS Con la virtualizzazione HVM, la VM guest viene eseguita come se si trovasse su una piattaforma di hardware nativo, con la differenza che utilizza comunque driver di archiviazione e una rete PV per migliorare le prestazioni.

Individuazione di un tipo di istanza Amazon EC2

Prima di poter avviare un'istanza, devi selezionare un tipo di istanza da utilizzare. Il tipo di istanza scelto può dipendere dalle risorse richieste dal carico di lavoro, ad esempio risorse di elaborazione, memoria o archiviazione. Può essere utile identificare diversi tipi di istanze che potrebbero adattarsi al carico di lavoro e valutarne le prestazioni in un ambiente di test. Non ci sono alternative per misurare le prestazioni dell'applicazione sotto carico.

Se hai già istanze EC2 in esecuzione, puoi utilizzarle AWS Compute Optimizer per ottenere consigli sui tipi di istanze da utilizzare per migliorare le prestazioni, risparmiare denaro o entrambi. Per ulteriori informazioni, consulta the section called “Per carichi di lavoro esistenti”.

Attività

- Individuazione di un tipo di istanza mediante la console
- Trovate un tipo di istanza utilizzando il AWS CLI

Individuazione di un tipo di istanza mediante la console

Puoi individuare un tipo di istanza che soddisfa le esigenze utilizzando la console Amazon EC2.

Per individuare un tipo di istanza mediante la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione selezionare la regione in cui avviare le istanze. È possibile selezionare qualsiasi regione disponibile, indipendentemente dalla posizione.
3. Nel riquadro di navigazione, scegliere Instance Types (Tipi di istanza).
4. (Facoltativo) Scegliere l'icona delle preferenze (ingranaggi) per selezionare quali attributi del tipo di istanza visualizzare, ad esempio i prezzi Linux on demand, quindi scegliere Conferma. In alternativa, seleziona il nome di un tipo di istanza per aprire la pagina dei dettagli e visualizzare tutti gli attributi disponibili tramite la console. La console non visualizza tutti gli attributi disponibili tramite l'API o la riga di comando.
5. Utilizzare gli attributi del tipo di istanza per filtrare l'elenco dei tipi di istanza visualizzati ai soli tipi di istanza che soddisfano le proprie esigenze. Ad esempio, è possibile applicare un filtro ai seguenti attributi:

   - Zone di disponibilità: il nome della zona di disponibilità, della zona locale o della zona Wavelength. Per ulteriori informazioni, consulta the section called “Regioni e zone”.
   - vCPU o Core: il numero di vCPU o core.
   - Memoria (GiB): la dimensione della memoria in GiB.
   - Prestazioni di rete: le prestazioni di rete, in Gigabit.
   - Storage dell'istanza locale: indica se il tipo di istanza dispone di archiviazione dell'istanza locale (`true` | `false`).
6. (Facoltativo) Per visualizzare un side-by-side confronto, seleziona la casella di controllo relativa a più tipi di istanze. Il confronto viene visualizzato nella parte inferiore dello schermo.
7. (Facoltativo) Per salvare l'elenco di tipi di istanza in un file di valori separati da virgola (.csv) per ulteriore analisi, scegliere Actions (Operazioni), Download list CSV (Scarica elenco CSV). Il file include tutti i tipi di istanza che corrispondono ai filtri impostati.
8. (Facoltativo) Per avviare istanze utilizzando un tipo di istanza che soddisfa le proprie esigenze, selezionare la casella di controllo per il tipo di istanza e scegliere Actions (Operazioni), Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Trovate un tipo di istanza utilizzando il AWS CLI

Puoi usare AWS CLI i comandi per Amazon EC2 per trovare un tipo di istanza che soddisfi le tue esigenze.

Per trovare un tipo di istanza, utilizza il AWS CLI

1. Se non l'hai già fatto, installa il AWS CLI Per ulteriori informazioni, consulta la Guida per l'AWS Command Line Interface utente.
2. Utilizzate il describe-instance-typescomando per filtrare i tipi di istanza in base agli attributi dell'istanza. Ad esempio, è possibile utilizzare il comando seguente per visualizzare solo i tipi di istanza della generazione corrente con 64 GiB (65.536 MiB) di memoria.

   ```
   aws ec2 describe-instance-types --filters "Name=current-generation,Values=true"
    "Name=memory-info.size-in-mib,Values=65536" --query "InstanceTypes[*].
   [InstanceType]" --output text | sort
   ```

3. Utilizzate il describe-instance-type-offeringscomando per filtrare i tipi di istanza offerti per posizione (Regione o Zona). Ad esempio, è possibile utilizzare il comando seguente per visualizzare i tipi di istanza offerti nella zona specificata.

   ```
   aws ec2 describe-instance-type-offerings --location-type "availability-
   zone" --filters Name=location,Values=us-east-2a --region us-east-2 --query
    "InstanceTypeOfferings[*].[InstanceType]" --output text | sort
   ```

4. Dopo aver individuato i tipi di istanza che soddisfano le proprie esigenze, salvare l'elenco in modo da poter utilizzare questi tipi di istanza quando si avviano le istanze. Per ulteriori informazioni, consulta la pagina Avvio di un'istanza nella Guida per l'utente di AWS Command Line Interface .

Ottenere raccomandazioni per i tipi di istanza

I seguenti strumenti possono aiutarti a selezionare i tipi di istanze ottimali per i tuoi carichi di lavoro nuovi o esistenti:

- Nuovi carichi di lavoro: lo strumento di ricerca del tipo di istanza EC2 considera il caso d'uso, il tipo di carico di lavoro, le preferenze del produttore della CPU e il modo in cui dai priorità a prezzo e prestazioni, oltre a parametri aggiuntivi che puoi specificare. Utilizza quindi questi dati per fornire suggerimenti e linee guida per i tipi di istanze Amazon EC2 più adatti ai tuoi nuovi carichi di lavoro.

- Carichi di lavoro esistenti: AWS Compute Optimizer analizza le specifiche e i parametri di utilizzo delle istanze esistenti. Successivamente utilizza i dati compilati per raccomandare i tipi di istanza Amazon EC2 ottimizzati per i costi o le prestazioni, o entrambi, per i carichi di lavoro esistenti.

Ottieni le raccomandazioni per i tipi di istanza:

- Ottenimento delle raccomandazioni per i tipi di istanza per un nuovo carico di lavoro
- Ottenimento delle raccomandazioni per i tipi di istanza per un carico di lavoro esistente

Ottenimento delle raccomandazioni per i tipi di istanza per un nuovo carico di lavoro

Lo strumento di ricerca del tipo di istanza EC2 considera il tuo caso d'uso, il tipo di carico di lavoro, le preferenze del produttore di CPU e il modo in cui dai priorità a prezzo e prestazioni, oltre a parametri aggiuntivi che puoi specificare. Utilizza quindi questi dati per fornire suggerimenti e linee guida per i tipi di istanze Amazon EC2 più adatti ai tuoi nuovi carichi di lavoro.

Con così tanti tipi di istanze disponibili, trovare i tipi di istanza giusti per il tuo carico di lavoro può essere lungo e complesso. Utilizzando lo strumento di ricerca dei tipi di istanze EC2, puoi rimanere aggiornato sui tipi di istanze più recenti e ottenere il miglior rapporto prezzo/prestazioni per i tuoi carichi di lavoro.

Questo argomento descrive come ottenere suggerimenti e linee guida per i tipi di istanze EC2 tramite la console Amazon EC2. Puoi anche passare direttamente ad Amazon Q per chiedere, ad esempio, consigli sul tipo di istanza. Per ulteriori informazioni, consulta la Amazon Q Developer User Guide.

Se stai cercando, ad esempio, consigli di tipo di istanza per un carico di lavoro esistente, usa AWS Compute Optimizer. Per ulteriori informazioni, consulta Ottenimento delle raccomandazioni per i tipi di istanza per un carico di lavoro esistente.

Usa lo strumento di ricerca del tipo di istanza EC2

Nella console Amazon EC2, puoi ottenere suggerimenti sul tipo di istanza dal Finder del tipo di istanza EC2 nella procedura guidata di avvio dell'istanza, durante la creazione di un modello di avvio o nella pagina dei tipi di istanza.

Utilizza le seguenti istruzioni per ottenere suggerimenti e indicazioni per i tipi di istanze EC2 utilizzando lo strumento di ricerca del tipo di istanza EC2 nella console Amazon EC2. Per visualizzare un'animazione dei passaggi, consulta. Visualizza un'animazione: ottieni suggerimenti sul tipo di istanza utilizzando lo strumento di ricerca del tipo di istanza EC2

Per ottenere suggerimenti sui tipi di istanza, utilizza lo strumento di ricerca del tipo di istanza EC2

1. Inizia il processo utilizzando uno dei seguenti metodi:

   - Segui la procedura per avviare un'istanza. Accanto a Tipo di istanza, scegli il link Fatti consigliare.
   - Segui la procedura per creare un modello di lancio. Accanto a Tipo di istanza, scegli il link Fatti consigliare.
   - Nel riquadro di navigazione, scegli Tipi di istanza, quindi scegli il pulsante Instance type finder.

2. Nella schermata Ottieni consigli sulla selezione del tipo di istanza, procedi come segue:

   a. Specificate i requisiti del tipo di istanza selezionando le opzioni relative ai produttori di tipo di carico di lavoro, caso d'uso, priorità e CPU.

   b. (Facoltativo) Per specificare requisiti più dettagliati per il tuo carico di lavoro, procedi come segue:

      i. Espandi Parametri avanzati.

      ii. Per aggiungere un parametro, selezionate un parametro, scegliete Aggiungi e specificate un valore per il parametro. Ripetete l'operazione per ogni parametro aggiuntivo che desiderate aggiungere. Per non indicare alcun valore minimo o massimo, lascia il campo vuoto.

      iii. Per rimuovere un parametro dopo averlo aggiunto, scegliete la X accanto al parametro.

   c. Scegli Ricevi consigli sul tipo di istanza.

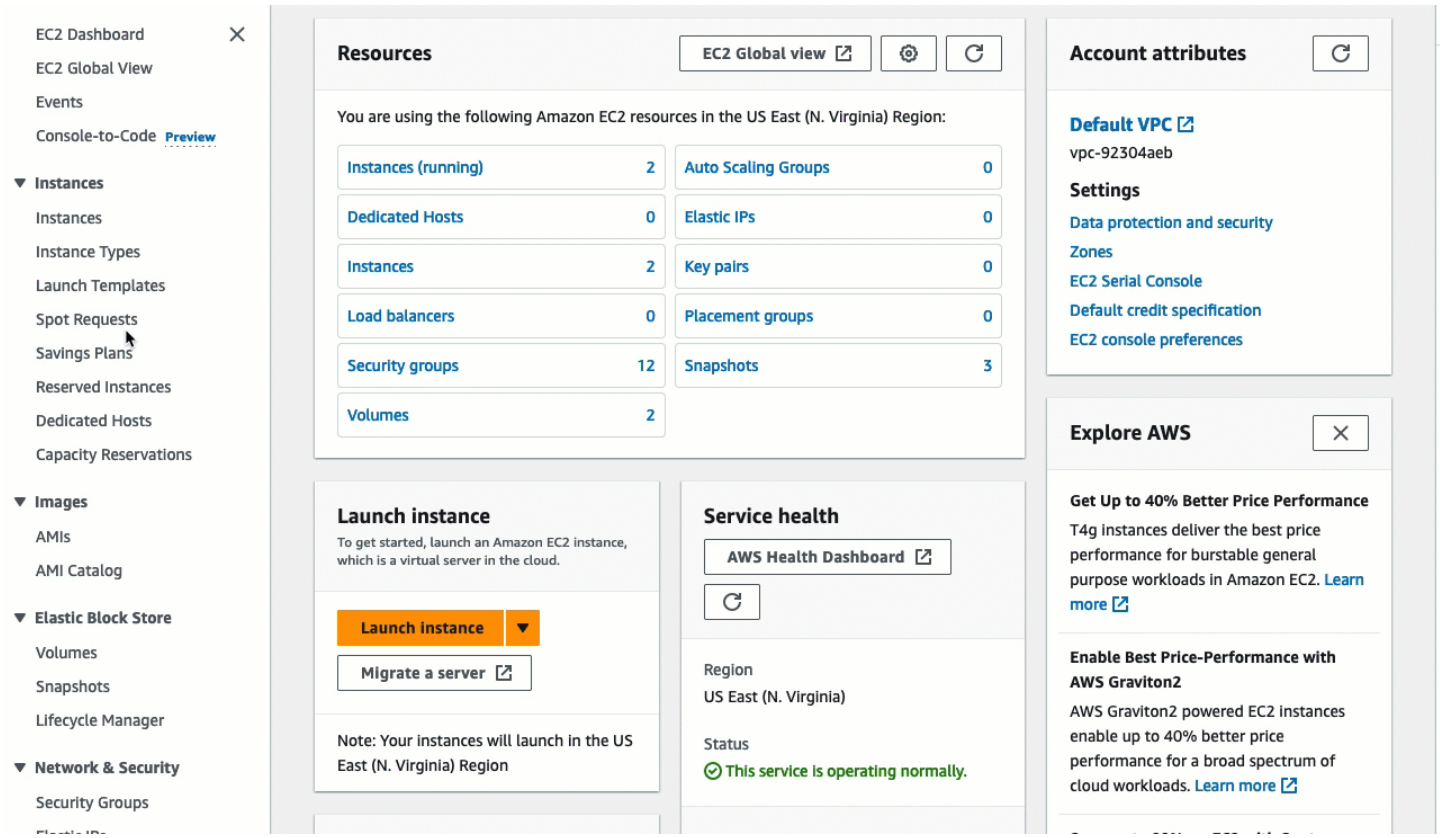
      Amazon EC2 ti fornisce suggerimenti per esempio famiglie che soddisfano i requisiti specificati.

3. Per visualizzare i dettagli di ogni tipo di istanza all'interno delle famiglie di istanze suggerite, scegli Visualizza i dettagli della famiglia di istanze consigliata.

4. Seleziona un tipo di istanza che soddisfi i tuoi requisiti, quindi scegli Azioni, Avvia istanza o Azioni, Crea modello di avvio.

   In alternativa, se hai avviato il processo nella procedura guidata di avvio dell'istanza o nella pagina del modello di avvio e preferisci tornare al flusso originale, prendi nota del tipo di istanza che desideri utilizzare. Quindi, nella procedura guidata di avvio dell'istanza o nel modello di avvio, per Tipo di istanza, scegli il tipo di istanza e completa la procedura per avviare un'istanza o creare un modello di avvio.

Visualizza un'animazione: ottieni suggerimenti sul tipo di istanza utilizzando lo strumento di ricerca del tipo di istanza EC2



Ottenimento delle raccomandazioni per i tipi di istanza per un carico di lavoro esistente

AWS Compute Optimizer fornisce consigli sulle istanze di Amazon EC2 per aiutarti a migliorare le prestazioni, risparmiare denaro o entrambi. Puoi utilizzare queste raccomandazioni per decidere se passare a un nuovo tipo di istanza.

Per fornire le raccomandazioni, Compute Optimizer analizza le specifiche delle istanze esistenti e i parametri di utilizzo. I dati compilati vengono quindi utilizzati per raccomandare i tipi di istanza Amazon EC2 più adatti per gestire il carico di lavoro esistente. Le raccomandazioni vengono restituite insieme ai prezzi delle istanze per ora.

In questo argomento viene descritto come visualizzare le raccomandazioni tramite la console Amazon EC2. Per ulteriori informazioni, consulta la Guida per l'utente AWS Compute Optimizer.

> **Note**
>
> Per ottenere le raccomandazioni da Compute Optimizer, devi prima optare per Compute Optimizer. Per ulteriori informazioni, consulta Nozioni di base su AWS Compute Optimizer nella Guida per l'utente di AWS Compute Optimizer .

Se stai cercando consigli sul tipo di istanza per un nuovo carico di lavoro, usa il selettore del tipo di istanza EC2 di Amazon Q. Per ulteriori informazioni, consulta Ottenimento delle raccomandazioni per i tipi di istanza per un nuovo carico di lavoro.

Indice

Limitazioni

Compute Optimizer attualmente genera raccomandazioni per i tipi di istanza C, D, H, I, M, R, T, X e z. Altri tipi di istanza non sono considerati da Compute Optimizer. Se utilizzi altri tipi di istanza, questi non verranno elencati nella visualizzazione delle raccomandazioni di Compute Optimizer. Per ulteriori informazioni sui tipi di istanza supportati e non supportati, consulta la sezione Requisiti di istanza Amazon EC2 nella Guida per l'utente di AWS Compute Optimizer .

Risultati

Compute Optimizer classifica le sue conclusioni per le istanze EC2 come segue:

- Under-provisioned (Provisioning insufficiente) – Un'istanza EC2 viene considerata con provisioning insufficiente quando almeno una specifica dell'istanza, ad esempio CPU, memoria o rete, non soddisfa i requisiti di prestazioni del carico di lavoro. Le istanze EC2 con provisioning insufficiente potrebbero compromettere le prestazioni dell'applicazione.
- Over-provisioned (Provisioning eccessivo) – Un'istanza EC2 viene considerata con provisioning eccessivo quando almeno una specifica dell'istanza, ad esempio CPU, memoria o rete, può essere

ridotta senza compromettere i requisiti di prestazioni del carico di lavoro, e quando nessuna specifica presenta provisioning insufficiente. Le istanze EC2 con provisioning eccessivo potrebbero comportare costi di infrastruttura non necessari.

- Optimized (Ottimizzata)– Un'istanza EC2 viene considerata ottimizzata quando tutte le specifiche dell'istanza, ad esempio CPU, memoria e rete, soddisfano i requisiti di prestazioni del carico di lavoro e l'istanza non presenta provisioning eccessivo. Un'istanza EC2 ottimizzata esegue i carichi di lavoro con prestazioni e costi di infrastruttura ottimali. Per le istanze ottimizzate, Compute Optimizer può talvolta raccomandare un tipo di istanza di nuova generazione.
- None (Nessuna) – Non ci sono raccomandazioni per questa istanza. Ciò potrebbe verificarsi se Compute Optimizer è stato attivato da meno di 12 ore o quando l'istanza è in esecuzione da meno di 30 ore o quando il tipo di istanza non è supportato da Ottimizzatore di calcolo. Per ulteriori informazioni, consulta Limitazioni nella sezione precedente.

Visualizzare le raccomandazioni

Dopo aver effettuato l'accesso su Compute Optimizer, puoi visualizzare i risultati generati da Compute Optimizer per le istanze EC2 nella console EC2. Puoi quindi accedere alla console Compute Optimizer per visualizzare i suggerimenti. Se hai aderito di recente, i risultati potrebbero non essere visualizzati nella console EC2 per un massimo di 12 ore.

Per visualizzare una raccomandazione per un'istanza EC2 tramite la console EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Istanze, quindi scegli l'ID dell'istanza .
3. Nella pagina di riepilogo dell'istanza, dal banner AWS Compute Optimizer nella parte inferiore della pagina, seleziona Visualizza dettagli.

   L'istanza viene aperta in Compute Optimizer, dove viene etichettata come istanza Current (Corrente). Vengono fornite fino a tre raccomandazioni per il tipo di istanza, etichettate come Option 1 (Opzione 1), Option 2 (Opzione 2) e Option 3 (Opzione 3). La metà inferiore della finestra mostra i dati CloudWatch metrici recenti per l'istanza corrente: utilizzo della CPU, utilizzo della memoria, ingresso rete e uscita rete.
4. (Facoltativo) Nella console Compute Optimizer, scegli impostazioni

   () per modificare le colonne visibili nella tabella o per visualizzare le informazioni pubbliche sui prezzi per un'opzione di acquisto diversa per i tipi di istanze correnti e consigliati.

> **Note**
>
> Se hai acquistato un'Istanza riservata, è possibile che l'Istanza on demand venga fatturata come Istanza riservata. Prima di modificare il tipo di istanza corrente, valuta innanzitutto l'impatto sull'utilizzo e sulla copertura dell'Istanza riservata.

Valuta se vuoi utilizzare una delle raccomandazioni. Decidi se ottimizzare per migliorare le prestazioni, per ridurre i costi o per entrambe le motivazioni. Per ulteriori informazioni, consulta Visualizzazione dei suggerimenti sulle risorse nella sezione Guida per l'utente di AWS Compute Optimizer .

Per visualizzare le raccomandazioni per tutte le istanze EC2 in tutte le regioni tramite la console di Compute Optimizer

1. Apri la console di Compute Optimizer all'indirizzo https://console.aws.amazon.com/compute-optimizer/.
2. Scegli Visualizza suggerimenti per tutte le istanze EC2.
3. Nella pagina dei suggerimenti si possono eseguire le seguenti operazioni:

   a. Per filtrare i consigli in base a una o più AWS regioni, inserisci il nome della regione nella casella di testo Filtra per una o più regioni oppure scegli una o più regioni nell'elenco a discesa visualizzato.

   b. Per visualizzare i suggerimenti per le risorse di un altro account, scegli Account, quindi seleziona un ID account diverso.

      Questa opzione è disponibile solo se è stato effettuato l'accesso a un account di gestione di un'organizzazione e se l'adesione è stata effettuata per tutti gli account membri nell'organizzazione.

   c. Per cancellare i filtri selezionati, scegli Clear filters (Cancella filtri).

   d. Per modificare l'opzione di acquisto visualizzata per i tipi di istanza correnti e consigliati, scegli le impostazioni
      (),
      quindi scegli Istanze su richiesta, Istanze riservate, standard con 1 anno senza anticipo o Istanze riservate, standard con 3 anni senza anticipo.

e. Per visualizzare i dettagli, ad esempio raccomandazioni aggiuntive e un confronto dei parametri di utilizzo, scegliere il risultato elencato accanto all'istanza desiderata, ovvero Under-provisioned (Provisioning insufficiente), Over-provisioned (Provisioning eccessivo) o Optimized (Ottimizzata). Per ulteriori informazioni, consulta Visualizzazione dei dettagli delle risorse nella Guida per l'utente di AWS Compute Optimizer .

Considerazioni sulla valutazione delle raccomandazioni

Prima di modificare un tipo di istanza, considera quanto segue:

- Le raccomandazioni non prevedono l'utilizzo. Le raccomandazioni si basano sull'utilizzo cronologico dell'ultimo periodo di 14 giorni. Assicurati di scegliere un tipo di istanza che soddisfi le tue esigenze future in termini di risorse.
- Concentrati sui parametri dei grafici per determinare se l'utilizzo effettivo è inferiore alla capacità dell'istanza. Puoi anche visualizzare i dati metrici (media, picco, percentile) per valutare ulteriormente i consigli sulle tue istanze EC2. CloudWatch Ad esempio, verifica se i parametri in percentuale della CPU durante il giorno cambiano e se si verifichino picchi che devono essere gestiti. Per ulteriori informazioni, consulta la sezione Visualizzazione delle metriche disponibili nella Amazon CloudWatch User Guide.
- Compute Optimizer può fornire raccomandazioni per le istanze a prestazioni espandibili, ossia le istanze T3, T3a e T2. Se periodicamente ti espandi oltre la linea di base, assicurati di poterlo continuare a fare in base alle vCPU del nuovo tipo di istanza. Per ulteriori informazioni, consulta Concetti e definizioni chiave per istanze espandibili.
- Se hai acquistato un'Istanza riservata, è possibile che l'Istanza on demand venga fatturata come Istanza riservata. Prima di modificare il tipo di istanza corrente, valuta innanzitutto l'impatto sull'utilizzo e sulla copertura dell'Istanza riservata.
- Laddove possibile, valuta il passaggio a istanze di ultima generazione.
- Quando esegui la migrazione a una famiglia di istanze diversa, assicurati che il tipo di istanza corrente e il nuovo tipo di istanza siano compatibili, ad esempio in termini di virtualizzazione, architettura o tipo di rete. Per ulteriori informazioni, consulta Compatibilità per la modifica del tipo di istanza.
- Infine, prendi in considerazione la valutazione del rischio delle prestazioni fornita per ogni raccomandazione. Il rischio delle prestazioni indica l'impegno che potrebbe essere richiesto per stabilire se il tipo di istanza suggerito soddisfi i requisiti di prestazioni del carico di lavoro. Ti consigliamo inoltre di eseguire test rigorosi per il carico e le prestazioni prima e dopo aver apportato eventuali modifiche.

Ci sono altri aspetti da tenere in considerazione quando si ridimensiona un'istanza EC2. Per ulteriori informazioni, consulta Cambiare il tipo di istanza.

Altre risorse

Per ulteriori informazioni:

- Tipi di istanza Amazon EC2
- AWS Compute Optimizer Guida per l'utente

Cambiare il tipo di istanza

Con il mutare delle necessità, è possibile che un'istanza risulti sovrautilizzata (il tipo di istanza è troppo piccolo) o sottoutilizzata (il tipo di istanza è troppo grande). In questo caso, è possibile ridimensionare l'istanza modificandone il tipo di istanza. Ad esempio, se la propria istanza `t2.micro` è troppo piccola per il suo carico di lavoro, è possibile aumentarne le dimensioni modificandola in un tipo di istanza T2 più grande, ad esempio una `t2.large`. In alternativa, è possibile cambiarla in un altro tipo di istanza, ad esempio una `m5.large`. Potrebbe inoltre essere necessario passare sda un tipo di istanza della generazione precedente a uno della generazione corrente per avvalersi di alcune caratteristiche, ad esempio il supporto per IPv6.

Se si desidera un suggerimento per un tipo di istanza che sia in grado di gestire al meglio il carico di lavoro esistente, è possibile utilizzare AWS Compute Optimizer. Per ulteriori informazioni, consulta Ottenimento delle raccomandazioni per i tipi di istanza per un carico di lavoro esistente.

Se modifichi il tipo di istanza, inizierai a pagare la tariffa per il nuovo tipo di istanza. Per conoscere le tariffe on demand di tutti i tipi di istanza, consulta la pagina Prezzi on demand di Amazon EC2.

Per aggiungere spazio di archiviazione aggiuntivo all'istanza senza modificare il tipo di istanza, aggiungi un volume EBS all'istanza. Per ulteriori informazioni, consulta Collegare un volume Amazon EBS a un'istanza nella Amazon EBS User Guide.

Quali istruzioni seguire?

Esistono diverse istruzioni per modificare il tipo di istanza. Le istruzioni da usare dipendono dal volume root dell'istanza e dal fatto che il tipo di istanza sia compatibile con la configurazione corrente dell'istanza. Per informazioni su come viene determinata la compatibilità, consultare Compatibilità per la modifica del tipo di istanza.

Utilizzare la tabella seguente per determinare quali istruzioni seguire.

Volume root	Compatibilità	Seguire le seguenti istruzioni
EBS	Compatible	Modifica il tipo di istanza di un'istanza supportata da EBS
EBS	Non compatibile	Cambiare il tipo di istanza avviando una nuova istanza
Instance store	Non applicabile	Non è possibile modificare il tipo di istanza di una retro-istanza archivio istanze.

Considerazioni per i tipi di istanza compatibili

Quando si modifica il tipo di istanza, considerare quanto segue:

- Per poter modificare il tipo di un'istanza supportata da Amazon EBS, è necessario arrestarla. Assicurati di prevedere i tempi di inattività durante l'arresto dell'istanza. L'arresto dell'istanza e il cambio del suo tipo di istanza potrebbero richiedere alcuni minuti, mentre il riavvio può richiedere un intervallo variabile di tempo, a seconda degli script di startup dell'applicazione. Per ulteriori informazioni, consulta Arresta e avvia le istanze Amazon EC2.
- Quando si interrompe e si avvia un'istanza, spostiamo l'istanza su un nuovo hardware. Se l'istanza ha un indirizzo IPv4 pubblico, l'indirizzo viene rilasciato e viene assegnato un nuovo indirizzo IPv4 pubblico. Se occorre un indirizzo IPv4 pubblico che non cambia, si utilizzi un indirizzo IP elastico.
- Non puoi modificare il tipo di istanza di un'istanza spot.
- [Istanze Windows] Ti consigliamo di aggiornare il pacchetto driver AWS PV prima di cambiare il tipo di istanza. Per ulteriori informazioni, consulta the section called “Aggiornamento dei driver PV”.
- Se l'istanza è inclusa in un gruppo Auto Scaling, il servizio Amazon EC2 Auto Scaling contrassegna l'istanza interrotta come non integra e pertanto può arrestarla e avviare un'istanza di sostituzione. Per evitare questa situazione, si può sospendere il processo di dimensionamento per il gruppo mentre si cambia il tipo di istanza. Per ulteriori informazioni, consultare Sospensione e ripresa di un processo per un gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.
- Quando modifichi il tipo di istanza di un'istanza con volumi dell'archivio istanza NVMe, l'istanza aggiornata potrebbe presentare volumi dell'archivio istanza aggiuntivi, in quanto tutti i volumi

dell'archivio istanza NVMe sono disponibili, anche se non sono specificati nella mappatura dei dispositivi a blocchi dell'AMI o delle istanze. Altrimenti, l'istanza aggiornata ha lo stesso numero di volumi dell'archivio istanza specificato quando hai avviato l'istanza originale.

- Il numero massimo di volumi Amazon EBS che puoi collegare a un'istanza dipende dal tipo e dalle dimensioni dell'istanza. Non puoi passare a un'istanza di tipo e dimensione che non supporti il numero di volumi già collegati all'istanza. Per ulteriori informazioni, consulta Limiti dei volumi delle istanze.

Modifica il tipo di istanza di un'istanza supportata da EBS

Utilizzare le seguenti istruzioni per modificare il tipo di un'istanza supportata da EBS se il tipo di istanza desiderato è compatibile con la configurazione corrente dell'istanza.

Per cambiare il tipo di istanza di un'istanza supportata da Amazon EBS

1. (Facoltativo) Se il nuovo tipo di istanza richiede driver che non sono installati sull'istanza esistente, devi prima connetterti all'istanza e installare i driver. Per ulteriori informazioni, consulta Compatibilità per la modifica del tipo di istanza.
2. [Istanze Windows] Se hai configurato l'istanza di Windows per l'utilizzo di indirizzi IP statici e passi da un tipo di istanza che non supporta reti avanzate a un tipo di istanza che supporta reti avanzate, potresti ricevere un avviso relativo a un potenziale conflitto di indirizzi IP quando riconfigurerai l'indirizzamento IP statico. Per evitare questo problema, abilita il protocollo DHCP sull'interfaccia di rete per l'istanza in uso prima di modificare il tipo di istanza. Dall'istanza aprire la funzionalità Network and Sharing Center (Centro connessioni di rete e condivisione), passare a Internet Protocol Version 4 (TCP/IPv4) Properties (Proprietà protocollo Internet versione 4 [TCP/IPv4]) per l'interfaccia di rete, quindi scegliere Obtain an IP address automatically (Ottieni indirizzo IP automaticamente). Modifica il tipo di istanza e riconfigura l'indirizzo IP statico sull'interfaccia di rete.
3. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
4. Nel riquadro di navigazione, seleziona Instances (Istanze).
5. Seleziona l'istanza e scegli Instance state (Stato istanza), Stop instance (Arresta istanza). Quando viene richiesta la conferma, selezionare Stop (Arresta). Possono essere necessari alcuni minuti per arrestare l'istanza.
6. Con l'istanza ancora selezionata, scegliere Actions (Operazioni), Instance settings (Impostazioni istanza), Change instance type (Cambia tipo di istanza). Questa opzione è disabilitata se lo stato dell'istanza non è `stopped`.

7. Per Change Instance Type (Cambia tipo di istanza), effettuare le seguenti operazioni:

   a. In Tipo di istanza, selezionare il tipo di istanza desiderato.

      Se il tipo di istanza non è nell'elenco, non è compatibile con la configurazione dell'istanza. Utilizzare invece le seguenti istruzioni: Cambiare il tipo di istanza avviando una nuova istanza.

   b. (Facoltativo) Se il tipo di istanza scelto supporta l'ottimizzazione EBS, selezionare EBS-optimized (Ottimizzato per EBS) per abilitare l'ottimizzazione EBS oppure deselezionare EBS-optimized (Ottimizzato per EBS) per disabilitare l'ottimizzazione EBS. Se il tipo di istanza selezionato è ottimizzato per EBS per impostazione predefinita, l'opzione EBS-optimized (Ottimizzato per EBS) è selezionata e non è possibile deselezionarla.

   c. Scegli Apply (Applica) per applicare le nuove impostazioni.

8. Per avviare l'istanza, selezionare l'istanza e scegli Stato istanza, Avvia istanza. Possono essere necessari alcuni minuti affinché l'istanza entri nello stato `running`. Se l'istanza non si avvia, consulta Risoluzione dei problemi relativi alla modifica del tipo di istanza.

9. [Istanze Windows] Se la tua istanza esegue Windows Server 2016 o Windows Server 2019 con EC2Launch v1, connettiti all'istanza di Windows ed esegui il seguente PowerShell script EC2Launch per configurare l'istanza dopo la modifica del tipo di istanza.

> **Important**
>
> La password amministratore verrà reimpostata quando abiliti lo script EC2 Launch dell'istanza di inizializzazione. Puoi modificare il file di configurazione per disattivare la reimpostazione della password amministratore specificandolo nelle impostazioni delle attività di inizializzazione. Per istruzioni su come disabilitare la reimpostazione della password, consulta Configurare le attività di inizializzazione (EC2Launch) o Modifica delle impostazioni (EC2Launch v2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Cambiare il tipo di istanza avviando una nuova istanza

Se la configurazione corrente dell'istanza supportata da EBS non è compatibile con il nuovo tipo di istanza desiderato, non sarà possibile cambiare il tipo di istanza dell'istanza originale. È invece possibile avviare una nuova istanza con una configurazione compatibile con il nuovo tipo di istanza desiderato e migrare l'applicazione alla nuova istanza. Ad esempio, se hai avviato l'istanza originale da un AMI PV, ma desideri passare a un tipo di istanza della generazione attuale che richiede un AMI HVM, dovrai avviare una nuova istanza da un AMI HVM. Per informazioni su come viene determinata la compatibilità, consultare Compatibilità per la modifica del tipo di istanza.

Per eseguire la migrazione dell'applicazione a una nuova istanza, procedere come segue:

- Eseguire il backup dei dati sull'istanza originale.
- Avviare una nuova istanza con una configurazione compatibile con il nuovo tipo di istanza desiderato e collegare tutti i volumi EBS che erano collegati all'istanza originale.
- Installare l'applicazione e tutto il software richiesto sulla nuova istanza.
- Ripristinare tutti i dati.
- Se l'istanza originale ha un indirizzo IP elastico e desideri che gli utenti possano continuare a utilizzare le applicazioni senza interruzioni sulla nuova istanza, è necessario associare l'indirizzo IP elastico alla nuova istanza. Per ulteriori informazioni, consultare Indirizzi IP elastici.

Cambiare il tipo di istanza per la configurazione di una nuova istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Eseguire il backup dei dati che è necessario conservare come riportato di seguito:
   - Per conservare i dati nei volumi di instance store, eseguire il backup di tutti i dati dei volumi in un'archiviazione persistente.
   - Per i dati sui tuoi volumi EBS, crea un'istantanea dei volumi o scollega i volumi dall'istanza in modo da poterli collegare alla nuova istanza in un secondo momento.
3. Nel riquadro di navigazione, seleziona Istanze.
4. Scegliere Launch Instances (Avvia istanze). Quando si configura l'istanza, effettuare le seguenti operazioni:
   a. Selezionare un'AMI che supporti il tipo di istanza desiderato. Tenere presente che i tipi di istanza di generazione corrente richiedono un'AMI HVM.

b. Selezionare il nuovo tipo di istanza. Se il tipo di istanza desiderato non è disponibile, significa che non è compatibile con la configurazione dell'AMI selezionata.

c. Se si ha intenzione di utilizzare un indirizzo IP elastico, selezionare il VPC in cui è attualmente in esecuzione l'istanza originale.

d. Se desideri consentire allo stesso traffico di raggiungere la nuova istanza, seleziona il gruppo di sicurezza associato all'istanza originale.

e. Al termine della configurazione della nuova istanza, completare i passaggi per selezionare una coppia di chiavi e avviare l'istanza. Possono essere necessari alcuni minuti affinché l'istanza entri nello stato `running`.

5. Se necessario, collegare eventuali nuovi volumi EBS in base agli snapshot creati oppure eventuali volumi EBS distaccati dall'istanza originale, alla nuova istanza.
6. Installare l'applicazione e tutto il software richiesto sulla nuova istanza.
7. Ripristina i dati di cui è stato creato il backup dai volumi di instance store dell'istanza originale.
8. Se si utilizza un indirizzo IP elastico, assegnarlo alla nuova istanza nel seguente modo:

   a. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).

   b. Seleziona l'indirizzo IP elastico associato all'istanza originale e scegli Actions (Operazioni), Disassociate Elastic IP address (Dissocia indirizzo IP elastico). Quando viene richiesta la conferma, seleziona Disassociate (Dissocia).

   c. Con l'indirizzo IP elastico ancora selezionato, scegli Actions (Operazioni), quindi seleziona Associate Elastic IP address (Associa indirizzo IP elastico).

   d. Per Resource type (Tipo di risorsa), scegliere Instance (Istanza).

   e. Per Istanza, scegliere l'istanza con cui associare l'indirizzo IP elastico.

   f. (Facoltativo) Per Private IP address (Indirizzo IP privato), specificare un indirizzo IP privato a cui associare l'indirizzo IP elastico.

   g. Seleziona Associate (Associa).

9. (Facoltativo) È possibile terminare l'istanza originale se non è più necessaria. Selezionare l'istanza e verificare che si stia terminando l'istanza originale e non la nuova istanza, ad esempio controllando il nome o l'ora di avvio, quindi scegliere Stato istanza, Termina istanza.

Compatibilità per la modifica del tipo di istanza

È possibile modificare il tipo di un'istanza solo se la configurazione corrente dell'istanza è compatibile con il tipo di istanza desiderato. Se il tipo di istanza desiderato non è compatibile con

la configurazione corrente dell'istanza, si dovrà avviare una nuova istanza con una configurazione compatibile con il tipo di istanza e migrare quindi l'applicazione alla nuova istanza.

[Istanze Linux] Puoi usare il `AWSSupport-MigrateXenToNitroLinux` runbook per migrare istanze Linux compatibili da un tipo di istanza Xen a un tipo di istanza Nitro. Per ulteriori informazioni, consulta `AWSSupport-MigrateXenToNitroLinux runbook` in Documentazione di riferimento del runbook di AWS Systems Manager Automation.

[Istanze Windows] Per ulteriori indicazioni sulla migrazione di istanze Windows compatibili da un tipo di istanza Xen a un tipo di istanza Nitro, consulta Migrazione ai tipi di istanza di ultima generazione.

La compatibilità è determinata nei seguenti modi:

Tipo di virtualizzazione

Le AMI Linux utilizzano uno dei due tipi di virtualizzazione disponibili: paravirtuale (PV) o macchina virtuale hardware (HVM). Non è possibile passare a un'istanza avviata da un'AMI PV a un tipo di istanza solo HVM. Per ulteriori informazioni, consulta Tipi di virtualizzazione dell'AMI. Per verificare il tipo di virtualizzazione dell'istanza, si faccia riferimento al valore di Virtualizzazione nel riquadro dei dettagli della schermata Istanze nella console Amazon EC2.

Architettura

Le AMI sono specifiche per l'architettura del processore, per cui è necessario selezionare un tipo di istanza con la stessa architettura del processore del tipo di istanza corrente. Ad esempio:

- Se il tipo di istanza corrente ha un processore basato sull'architettura Arm, si è limitati ai tipi di istanze che supportano un processore basato sull'architettura Arm, ad esempio C6g e M6g.
- I seguenti tipi di istanza sono gli unici tipi di istanza che supportano le AMIs a 32-bit: `t2.nano`, `t2.micro`, `t2.small`, `t2.medium`, `c3.large`, `t1.micro`, `m1.small`, `m1.medium` e `c1.medium`. Se si stai modificando il tipo di istanza di un'istanza a 32 bit, si è limitati a questi tipi di istanza.

Schede di rete

Se si passa da un driver per una scheda di rete a un altro, le impostazioni della scheda di rete vengono reimpostate quando il sistema operativo crea la nuova scheda. Per riconfigurare le impostazioni, potrebbe essere necessario accedere a un account locale con autorizzazioni di amministratore. Di seguito sono riportati alcuni esempi di spostamento da una scheda di rete a un'altra:

- AWS Da PV (istanze T2) a Intel 82599 VF (istanze M4)

- Da Intel 82599 VF (la maggior parte delle istanze M4) a ENA (istanze M5)
- Da ENA (istanze M5) a ENA ad elevata larghezza di banda (istanze M5n)

Schede di rete

Alcuni tipi di istanza supportano più schede di rete. È necessario selezionare un tipo di istanza che supporti lo stesso numero di schede di rete del tipo di istanza corrente.

Reti avanzate

I tipi di istanza che supportano la connettività di rete migliorata richiedono l'installazione dei driver necessari. Ad esempio, le istanze basate sul sistema AWS Nitro richiedono AMI supportate da EBS con i driver Elastic Network Adapter (ENA) installati. Per passare da un tipo di istanza che non supporta la rete avanzata a un tipo che la supporta, è necessario installare i driver ENA o i driver ixgbevf sull'istanza, a seconda dei casi.

> **Note**
>
> Quando ridimensioni un'istanza con ENA Express abilitato, anche il nuovo tipo di istanza deve supportare ENA Express. Per un elenco dei tipi di istanza che supportano ENA Express, consulta la pagina Tipi di istanza supportati per ENA Express.
> Per passare da un tipo di istanza che supporta ENA Express a un tipo di istanza che non lo supporta, assicurati che ENA Express non sia abilitato prima di ridimensionare l'istanza.

NVMe

I volumi EBS sono esposti come dispositivi a blocchi NVMe su istanze basate sul sistema Nitro. AWS Se si passa da un tipo di istanza che non supporta NVMe a un tipo di istanza che lo supporta, è necessario prima installare i driver NVMe sull'istanza. Inoltre, i nomi dei dispositivi specificati nella mappatura dei dispositivi a blocchi vengono rinominati utilizzando i nomi dei dispositivi NVMe (). `/dev/nvme[0-26]n1`

[Istanze Linux] Pertanto, per montare i file system all'avvio utilizzando`/etc/fstab`, è necessario utilizzare UUID/Label anziché i nomi dei dispositivi.

Limite di volumi

Il numero massimo di volumi Amazon EBS che puoi collegare a un'istanza dipende dal tipo e dalle dimensioni dell'istanza. Per ulteriori informazioni, consulta Limiti dei volumi delle istanze.

È possibile passare solo a un'istanza di tipo e dimensione che supporti lo stesso numero o un numero maggiore di volumi rispetto a quello attualmente collegato all'istanza. Se si passa a un'istanza di tipo e dimensioni che non supporta il numero di volumi attualmente collegati, la richiesta ha esito negativo. Ad esempio, se passi da un'istanza `m7i.4xlarge` con 32 volumi allegati a un`m6i.4xlarge` che supporta massimo 27 volumi, la richiesta ha esito negativo.

Risoluzione dei problemi relativi alla modifica del tipo di istanza

Utilizzare le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante il cambio del tipo di istanza.

L'istanza non viene avviata dopo aver modificato il tipo di istanza

Possibile causa: requisiti per il nuovo tipo di istanza non soddisfatti

Se l'istanza non viene avviata, è possibile che uno dei requisiti per il nuovo tipo di istanza non sia stato soddisfatto. Per ulteriori informazioni, consulta Perché la mia istanza Linux non si avvia dopo che ne ho modificato il tipo?

Possibile causa: l'AMI non supporta il tipo di istanza

Se si utilizza la console EC2 per modificare il tipo di istanza, sono disponibili solo i tipi di istanza supportati dall'AMI selezionata. Tuttavia, se utilizzi il AWS CLI per avviare un'istanza, puoi specificare un AMI e un tipo di istanza incompatibili. Se l'AMI e il tipo di istanza sono incompatibili, l'istanza non può essere avviata. Per ulteriori informazioni, consulta Compatibilità per la modifica del tipo di istanza.

Possibile causa: l'istanza si trova nel gruppo di collocazione cluster

Se la propria istanza si trova in un gruppo di collocazione cluster e, dopo aver modificato il tipo di istanza, l'istanza non viene avviata, provare quanto segue:

1. Arrestare tutte le istanze nel gruppo di collocazione cluster.
2. Cambiare il tipo di istanza dell'istanza interessata.
3. Avviare tutte le istanze nel gruppo di collocazione cluster.

Applicazione o sito Web non raggiungibile da Internet dopo aver modificato il tipo di istanza

Possibile causa: viene rilasciato un indirizzo IPv4 pubblico

Quando si modifica il tipo di istanza, è prima necessario arrestare l'istanza. Quando si arresta un'istanza, viene rilasciato l'indirizzo IPv4 pubblico e ne viene assegnato uno nuovo.

Per mantenere l'indirizzo IPv4 pubblico tra l'arresto e l'avvio dell'istanza, consigliamo di utilizzare un indirizzo IP elastico senza costi aggiuntivi a condizione che l'istanza sia in esecuzione. Per ulteriori informazioni, consulta Indirizzi IP elastici.

Non è possibile modificare il tipo di istanza di una retro-istanza archivio istanze.

Un'istanza supportata da un archivio istanza è un'istanza che dispone di un volume root dell'archivio istanza. Non è possibile modificare il tipo di istanza di un'istanza che dispone di un volume root dell'archivio istanza. È invece necessario creare un'AMI dalla propria istanza, avviare una nuova istanza da questa AMI e selezionare il tipo di istanza desiderato, quindi migrare l'applicazione alla nuova istanza. Il tipo di istanza desiderato deve essere compatibile con l'AMI creata. Per informazioni su come viene determinata la compatibilità, consultare Compatibilità per la modifica del tipo di istanza.

Panoramica del processo

- Eseguire il backup dei dati sull'istanza originale.
- Creare un'AMI dall'istanza originale.
- Avviare una nuova istanza da questa AMI e selezionare il tipo di istanza desiderato.
- Installare la propria applicazione sulla nuova istanza.
- Se l'istanza originale ha un indirizzo IP elastico e desideri che gli utenti possano continuare a utilizzare le applicazioni senza interruzioni sulla nuova istanza, è necessario associare l'indirizzo IP elastico alla nuova istanza. Per ulteriori informazioni, consultare Indirizzi IP elastici.

Per modificare il tipo di istanza di un'istanza che dispone di un volume root dell'archivio istanza

1. Eseguire il backup dei dati che è necessario conservare come riportato di seguito:
   - Per conservare i dati nei volumi di instance store, eseguire il backup di tutti i dati dei volumi in un'archiviazione persistente.

- Per i dati sui volumi EBS, crea un'istantanea dei volumi o scollega il volume dall'istanza in modo da poterlo collegare alla nuova istanza in un secondo momento.

2. Creare un'AMI dall'istanza soddisfando i prerequisiti e attenendosi alle procedure descritte in Creazione di un'AMI Linux supportata da un instance store. Dopo aver creato un'AMI dall'istanza, torna a questa procedura.
3. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
4. Nel riquadro di navigazione scegliere AMIs (AMI). Negli elenchi dei filtri scegliere Owned by me (Di mia proprietà) e selezionare l'immagine creata nella fase 2. Tenere presente che AMI Name (Nome AMI) corrisponde al nome specificato durante la registrazione dell'immagine, mentre Source (Origine) corrisponde al bucket Amazon S3.

   > **Note**
   >
   > Se l'AMI creata nella fase 2 non viene visualizzata, verificare di avere selezionato la regione in cui l'AMI è stata creata.

5. Con l'AMI selezionata, scegliere Avvia istanza dall'immagine. Quando si configura l'istanza, effettuare le seguenti operazioni:

   a. Selezionare il nuovo tipo di istanza. Se il tipo di istanza desiderato non è disponibile, significa che non è compatibile con la configurazione dell'AMI creata. Per ulteriori informazioni, consulta Compatibilità per la modifica del tipo di istanza.

   b. Se si ha intenzione di utilizzare un indirizzo IP elastico, selezionare il VPC in cui è attualmente in esecuzione l'istanza originale.

   c. Se desideri consentire allo stesso traffico di raggiungere la nuova istanza, seleziona il gruppo di sicurezza associato all'istanza originale.

   d. Al termine della configurazione della nuova istanza, completare i passaggi per selezionare una coppia di chiavi e avviare l'istanza. Possono essere necessari alcuni minuti affinché l'istanza entri nello stato `running`.

6. Se necessario, collegare eventuali nuovi volumi EBS in base agli snapshot creati oppure eventuali volumi EBS distaccati dall'istanza originale, alla nuova istanza.
7. Installare l'applicazione e tutto il software richiesto sulla nuova istanza.
8. Se si utilizza un indirizzo IP elastico, assegnarlo alla nuova istanza nel seguente modo:

   a. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).

b. Seleziona l'indirizzo IP elastico associato all'istanza originale e scegli Actions (Operazioni), Disassociate Elastic IP address (Dissocia indirizzo IP elastico). Quando viene richiesta la conferma, seleziona Disassociate (Dissocia).

c. Con l'indirizzo IP elastico ancora selezionato, scegli Actions (Operazioni), quindi seleziona Associate Elastic IP address (Associa indirizzo IP elastico).

d. Per Resource type (Tipo di risorsa), scegliere Instance (Istanza).

e. Per Istanza, scegliere l'istanza con cui associare l'indirizzo IP elastico.

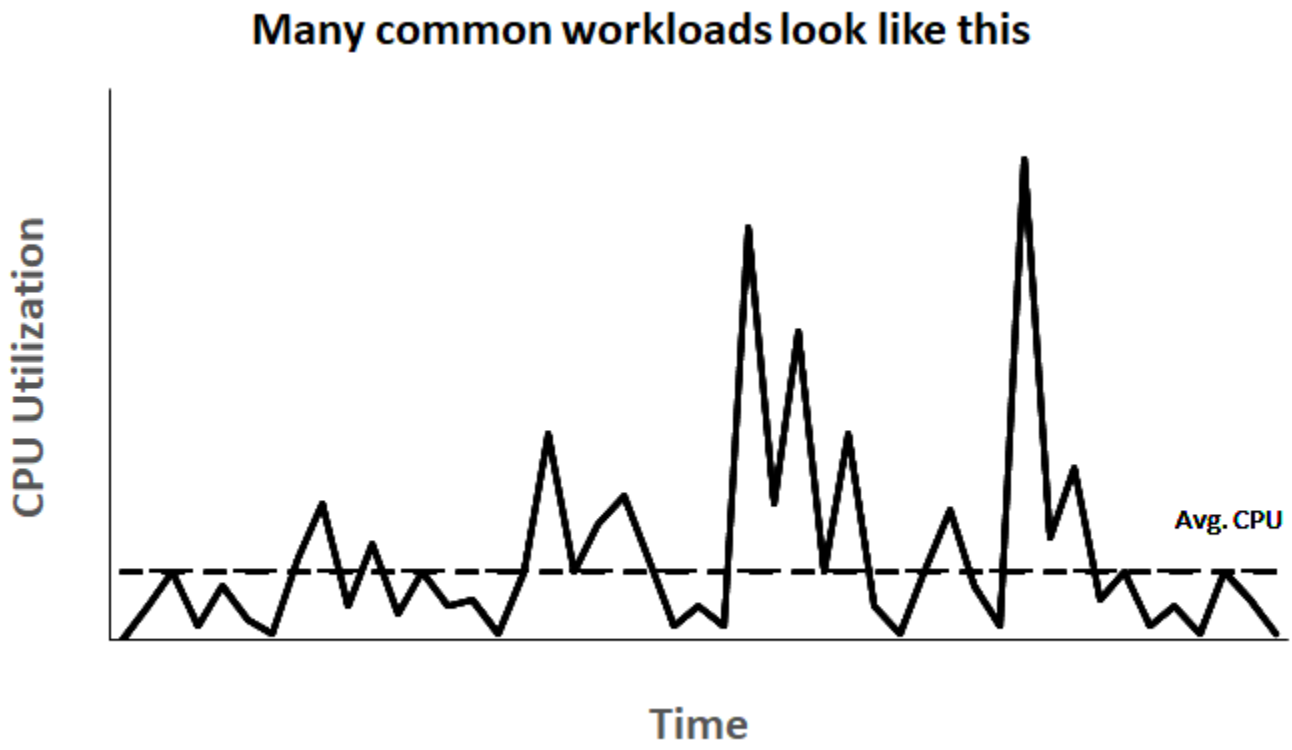
f. (Facoltativo) Per Private IP address (Indirizzo IP privato), specificare un indirizzo IP privato a cui associare l'indirizzo IP elastico.

g. Seleziona Associate (Associa).

9. (Facoltativo) È possibile terminare l'istanza originale se non è più necessaria. Selezionare l'istanza e verificare che si stia terminando l'istanza originale e non la nuova istanza, ad esempio controllando il nome o l'ora di avvio, quindi scegliere Stato istanza, Termina istanza.

Istanze a prestazioni espandibili

Molti carichi di lavoro generici non sono in media occupati e non richiedono un elevato livello di prestazioni della CPU sostenute. Il grafico seguente illustra l'utilizzo della CPU per molti carichi di lavoro comuni che i clienti eseguono oggi nel AWS cloud.



Questi carichi di lavoro relativi all'utilizzo della low-to-moderate CPU comportano uno spreco di cicli della CPU e, di conseguenza, i costi sono superiori a quelli utilizzati. Per superare questo problema, è possibile sfruttare le istanze generiche a basso costo espandibili, che sono le istanze T.

La famiglia di istanze T fornisce prestazioni CPU base con la possibilità di superare la baseline in qualsiasi momento per tutto il tempo necessario. La CPU di base è definita per soddisfare le esigenze della maggior parte dei carichi di lavoro generici, inclusi microservizi su larga scala, server Web, database di piccole e medie dimensioni, registrazione dei dati, repository di codice, desktop virtuali, ambienti di sviluppo e test e applicazioni business-critical. Le istanze T offrono un equilibrio tra risorse di calcolo, memoria e rete e offrono il modo più conveniente per eseguire un ampio spettro di applicazioni generiche che utilizzano la CPU. low-to-moderate Possono risparmiare fino al 15% in termini di costi rispetto alle istanze M e portare a risparmi ancora maggiori sui costi con dimensioni di istanza più piccole ed economiche, offrendo fino a 2 vCPU e 0,5 GiB di memoria. Le dimensioni delle istanze T più piccole, come nano, micro, small e medium, sono adatte per carichi di lavoro che richiedono una piccola quantità di memoria e non prevedono un utilizzo elevato della CPU.

> **Note**
>
> In questo argomento sono descritte le CPU espandibili. Per informazioni sulle prestazioni delle reti espandibili, consulta Larghezza di banda di rete dell'istanza Amazon EC2.

Tipi di istanze espandibili EC2

Le istanze espandibili EC2 sono costituite da tipi di istanze T4g, T3a e T3 e i tipi di istanza T2 della generazione precedente.

I tipi di istanza T4g sono l'ultima generazione di istanze espandibili. Offrono il miglior prezzo per le prestazioni e offrono il costo più basso di tutti i tipi di istanza EC2. I tipi di istanze T4g sono alimentati da processori AWS Graviton2 basati su ARM con un ampio supporto ecosistemico fornito da fornitori di sistemi operativi, fornitori di software indipendenti e servizi e applicazioni più diffusi. AWS

Nella tabella seguente vengono riepilogate le principali differenze tra i tipi di istanza espandibili.

Tipo	Descrizione	Famiglia di processori
Generazione più recente		
T4g	Tipo di istanza EC2 a basso costo con un rapporto prezzo/prestazioni superiore fino al 40% e costi inferiori del 20% rispetto al T3	AWS Processori Graviton2 con core Arm Neoverse N1
T3a	Istanze basate su x86 a basso costo con costi inferiori del 10% rispetto alle istanze T3	Processori EPYC di prima generazione AMD
T3	Miglior rapporto prezzo/prestazioni di picco per carichi di lavoro x86 con un rapporto prezzo/prestazioni inferiore fino al 30% rispetto alle istanze T2 della generazione precedente	Intel Xeon scalabile (processori Skylake, Cascade Lake)

Tipo	Descrizione	Famiglia di processori
Generazione precedente		
T2	Istanze espandibili di generazioni precedenti	Processori Intel Xeon

Per ulteriori informazioni sui prezzi delle istanze e per specifiche aggiuntive, consulta Amazon EC2 Pricing (Prezzi di Amazon EC2) e Amazon EC2 Instance Types (Tipi di istanza Amazon EC2). Per informazioni sulle prestazioni delle reti espandibili, consulta Larghezza di banda di rete dell'istanza Amazon EC2.

Se il tuo account ha meno di 12 mesi, puoi utilizzare un'istanza `t2.micro` gratuitamente (o un'istanza `t3.micro` in regioni in cui `t2.micro` non è disponibile) entro determinati limiti di utilizzo. Per ulteriori informazioni, consulta Piano gratuito di AWS.

Opzioni di acquisto supportate per istanze T

- On-Demand Instances
- Reserved Instances
- Istanze dedicate (solo T3)
- Host dedicati (solo T3, esclusivamente in modalità `standard`)
- Spot Instances

Per ulteriori informazioni, consulta Opzioni di acquisto delle istanze.

Indice

Best practice

Queste best practice consentono di sfruttare al meglio i vantaggi delle istanze a prestazioni espandibili.

- Assicurarsi che le dimensioni dell'istanza scelte rispettino i requisiti minimi di memoria del sistema operativo e delle applicazioni. I sistemi operativi con interfacce utente grafiche che consumano notevoli quantità di risorse di memoria e CPU (ad esempio, Windows) potrebbero richiedere una dimensione dell'istanza `t3.micro` o più grande per molti casi d'uso. Man mano che i requisiti di memoria e CPU del carico di lavoro aumentano nel tempo, con le istanze T è possibile passare a dimensioni maggiori dello stesso tipo di istanza o selezionare un altro tipo di istanza.
- Abilita AWS Compute Optimizer per il tuo account ed esamina i suggerimenti di Compute Optimizer per il tuo carico di lavoro. Compute Optimizer può aiutare a valutare se le istanze devono essere aumentate per migliorare le prestazioni o ridimensionate per risparmiare sui costi. L'ottimizzatore di calcolo può anche consigliare un tipo di istanza diverso in base allo scenario. Per ulteriori informazioni, consulta Visualizzazione dei suggerimenti sulle istanze EC2 nella sezione Guida per l'utente di AWS Compute Optimizer .

Concetti e definizioni chiave per istanze espandibili

I tradizionali tipi di istanze Amazon EC2 forniscono risorse CPU fisse, mentre le istanze espandibili forniscono un livello di baseline di utilizzo della CPU con la possibilità di aumentare l'utilizzo della CPU al di sopra della baseline. In questo modo si garantisce il pagamento solo per la CPU della baseline e per qualsiasi utilizzo aggiuntivo della CPU con conseguente riduzione dei costi di calcolo. Le prestazioni di base e la capacità di espansione sono governate dai crediti CPU. Le istanze a prestazioni espandibili sono gli unici tipi di istanza che utilizzano i crediti per l'utilizzo della CPU.

Ogni istanza espandibile guadagna continuamente credito quando rimane al di sotto della baseline della CPU e spende crediti quando sfora al di sopra della baseline. La quantità di crediti guadagnati o spesi dipende dall'utilizzo della CPU dell'istanza:

- Se l'utilizzo della CPU è inferiore alla baseline, i crediti guadagnati sono superiori ai crediti spesi.
- Se l'utilizzo della CPU è uguale alla baseline, i crediti guadagnati sono uguali ai crediti spesi.
- Se l'utilizzo della CPU è superiore alla baseline, i crediti spesi sono superiori ai crediti guadagnati.

Quando i crediti guadagnati sono superiori ai crediti spesi, la differenza viene chiamata crediti accumulati, crediti che possono essere utilizzati in seguito per andare oltre l'utilizzo della CPU di

base. Allo stesso modo, quando i crediti spesi sono superiori ai crediti guadagnati, il comportamento dell'istanza dipende dalla modalità di configurazione del credito: modalità Standard o modalità Illimitato.

In modalità Standard, quando i crediti spesi sono superiori ai crediti guadagnati, l'istanza utilizza i crediti accumulati per andare oltre l'utilizzo della CPU di base. Se non ci sono crediti accumulati rimanenti, l'istanza si riduce gradualmente all'utilizzo della CPU baseline e non può superare la baseline fino a quando non accumula altri crediti.

In modalità illimitata, se l'istanza supera l'utilizzo della CPU di base, l'istanza utilizza prima i crediti accumulati. Se non ci sono crediti accumulati rimanenti, l'istanza spende i crediti eccedenti. Quando l'utilizzo della CPU è inferiore alla baseline, utilizza i crediti CPU che guadagna per pagare i crediti extra spesi in precedenza. La possibilità di guadagnare crediti CPU per pagare i crediti extra consente ad Amazon EC2 di calcolare una media dell'utilizzo della CPU di un'istanza in un periodo di 24 ore. Se l'utilizzo medio della CPU in un periodo di 24 ore supera la baseline, l'istanza verrà fatturata per l'uso aggiuntivo a una tariffa fissa aggiuntiva per vCPU/ora.

Indice

Concetti e definizioni chiave

I seguenti concetti e definizioni chiave sono applicabili alle istanze espandibili.

Utilizzo CPU

> L'utilizzo della CPU è la percentuale delle unità di elaborazione EC2 assegnate attualmente in uso nell'istanza. Questo parametro misura la percentuale di cicli CPU allocati utilizzati in un'istanza. La CloudWatch metrica sull'utilizzo della CPU mostra l'utilizzo della CPU per istanza e non l'utilizzo della CPU per core. La specifica della CPU di base di un'istanza si basa anche sull'utilizzo della CPU per istanza. Per misurare l'utilizzo della CPU utilizzando AWS Management Console o il AWS CLI, vedere. Ottenere le statistiche su un'istanza specifica

Credito CPU

Un'unità di tempo vCPU.

Esempi:

1 credito CPU = 1 vCPU * 100% di utilizzo * 1 minuto.

1 credito CPU = 1 vCPU * 50% di utilizzo * 2 minuti.

1 credito CPU = 2 vCPU * 25% di utilizzo * 2 minuti.

Utilizzo di base

L'utilizzo di base è il livello in cui la CPU può essere utilizzata per un saldo creditizio netto pari a zero, quando il numero di crediti CPU guadagnati corrisponde al numero di crediti CPU utilizzati. L'utilizzo di base è noto anche come linea di base. L'utilizzo della linea di base è espresso come percentuale di utilizzo della vCPU, calcolata come segue: % utilizzo linea di base = (numero di crediti guadagnati / numero di vCPU) / 60 minuti.

Per l'utilizzo della base di confronto di ogni tipo di istanza a prestazioni espandibili, consulta la tabella del credito.

Crediti guadagnati

I crediti guadagnati continuamente da un'istanza quando è in esecuzione.

Numero di crediti guadagnati per ora = % utilizzo di base * numero di vCPU * 60 minuti

Esempio:

Un t3.nano con 2 vCPU e un utilizzo di base del 5% guadagna 6 crediti all'ora, calcolati come segue:

2 vCPU * 5% di base * 60 minuti = 6 crediti all'ora

Crediti spesi o usati

I crediti utilizzati continuamente da un'istanza quando è in esecuzione.

I crediti CPU spesi al minuto = Numero di vCPU * Utilizzo della CPU * 1 minuto

Crediti accumulati

I crediti CPU non spesi quando un'istanza utilizza un numero di crediti inferiore a quello richiesto per l'utilizzo di base. In altre parole, crediti maturati = (Crediti guadagnati - Crediti usati) sotto la linea di base.

Esempio:

Se un t3.nano è in esecuzione al 2% di utilizzo della CPU, che è al di sotto della sua linea di base del 5% per un'ora, i crediti accumulati vengono calcolati come segue:

Crediti CPU accumulati = (Crediti guadagnati all'ora - Crediti usati all'ora) = 6 - 2 vCPU * 2% utilizzo CPU * 60 minuti = 6 - 2,4 = 3,6 crediti accumulati all'ora

Limite di accumulo di crediti

Dipende dalla dimensione dell'istanza, ma in generale è uguale al numero massimo di crediti guadagnati in 24 ore.

Esempio:

Per t3.nano, il limite di accumulo del credito = 24 * 6 = 144 crediti

Crediti di lancio

Applicabile solo per le istanze T2 configurate per la modalità Standard. I crediti di avvio sono un numero limitato di crediti CPU che vengono allocati a una nuova istanza T2 in modo che, quando viene avviata in modalità Standard, possa superare la linea di base.

Crediti in eccedenza

I crediti che vengono spesi da un'istanza dopo che ha esaurito il suo saldo di credito accumulato. I crediti in eccedenza sono progettati per le istanze espandibili per sostenere prestazioni elevate per un periodo di tempo prolungato e sono utilizzati solo in modalità Illimitato. Il saldo dei crediti in eccedenza viene utilizzato per determinare quanti crediti sono stati utilizzati dall'istanza per l'espansione in modalità Illimitato.

Modalità Standard

Modalità di configurazione del credito, che consente a un'istanza di superare la linea di base spendendo i crediti accumulati nel suo saldo.

Modalità illimitata

Modalità di configurazione del credito, che consente a un'istanza di superare la baseline sostenendo un utilizzo elevato della CPU per tutto il tempo necessario per qualsiasi periodo di tempo. Il prezzo orario copre automaticamente tutti i picchi di utilizzo della CPU se l'utilizzo medio della CPU dell'istanza corrisponde o è inferiore alla baseline per un periodo di 24 ore o la durata dell'istanza, a seconda di quale dei due è inferiore. Se l'istanza viene eseguita a un utilizzo più

elevato della CPU per un periodo di tempo prolungato, verrà applicata una tariffa fissa aggiuntiva all'ora-vCPU.

Nella tabella seguente vengono riepilogate le principali differenze di credito tra i tipi di istanza espandibili.

Tipo	Tipo di crediti CPU supportato	Modalità di configurazione crediti	Durata dei crediti CPU accumulati tra l'avvio e l'arresto dell'istanza
Generazione più recente			
T4g	Crediti guadagnati, Crediti accumulati, Crediti spesi, Crediti in eccedenza (solo modalità Illimitato)	Standard, Illimitato (predefinito)	7 giorni (i crediti persistono per 7 giorni dopo l'interruzione di un'istanza)
T3a	Crediti guadagnati, Crediti accumulati, Crediti spesi, Crediti in eccedenza (solo modalità Illimitato)	Standard, Illimitato (predefinito)	7 giorni (i crediti persistono per 7 giorni dopo l'interruzione di un'istanza)
T3	Crediti guadagnati, Crediti accumulati, Crediti spesi, Crediti in eccedenza (solo modalità Illimitato)	Standard, Illimitato (predefinito)	7 giorni (i crediti persistono per 7 giorni dopo l'interruzione di un'istanza)
Generazione precedente			
T2	Crediti guadagnati, Crediti accumulati, Crediti spesi, Crediti di avvio (solo modalità Standard), Crediti	Standard (predefinito), Illimitato	0 giorni (i crediti vengono persi quando un'istanza viene interrotta)

Tipo	Tipo di crediti CPU supportato	Modalità di configura zione crediti	Durata dei crediti CPU accumulati tra l'avvio e l'arresto dell'istanza
	in eccedenza (solo modalità Illimitato)		

> **Note**
>
> La modalità illimitata non è supportata per le istanze T3 avviate su un host dedicato.

Guadagno di crediti CPU

Ogni istanza a prestazioni espandibili guadagna continuamente (a una risoluzione a livello di millisecondo) un tasso fisso di crediti CPU all'ora, a seconda delle dimensioni dell'istanza. Il processo contabile per l'accumulo o la spesa dei crediti avviene anche a una risoluzione a livello di millisecondo, quindi non devi preoccuparti di spendere troppo i crediti CPU; una breve ottimizzazione della CPU utilizza una piccola frazione del credito CPU.

Se un'istanza a prestazioni espandibili utilizza una quantità inferiore di risorse CPU rispetto a quella necessaria per l'utilizzo di base (ad esempio quando è inattiva), i crediti CPU non spesi vengono accumulati nel saldo del credito CPU. Se un'istanza a prestazioni espandibili deve superare il livello di utilizzo di base, spende i crediti accumulati. Maggiore è il numero di crediti accumulato da un'istanza a prestazioni espandibili, maggiore è il tempo in cui può far aumentare le prestazioni al di là della sua baseline quando è necessario un utilizzo maggiore della CPU.

La seguente tabella elenca i tipi di istanze a prestazioni espandibili, la frequenza a cui i crediti CPU vengono guadagnati all'ora, il numero massimo di crediti CPU guadagnati che un'istanza può accumulare, il numero di vCPU per istanza e il livello di utilizzo di base come percentuale di un full core (utilizzando una singola vCPU).

Tipo di istanza	Crediti CPU guadagnati all'ora	Quantità massima di crediti guadagnati che può essere accumulata*	vCPU***	Utilizzo di base per vCPU
T2				
t2.nano	3	72	1	5%
t2.micro	6	144	1	10%
t2.small	12	288	1	20%
t2.medium	24	576	2	20%**
t2.large	36	864	2	30%**
t2.xlarge	54	1296	4	22,5%**
t2.2xlarge	81,6	1958,4	8	17%**
T3				
t3.nano	6	144	2	5%**
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
T3a				
t3a.nano	6	144	2	5%**

Tipo di istanza	Crediti CPU guadagnati all'ora	Quantità massima di crediti guadagnati che può essere accumulata*	vCPU***	Utilizzo di base per vCPU
t3a.micro	12	288	2	10%**
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**
T4g				
t4g.nano	6	144	2	5%**
t4g.micro	12	288	2	10%**
t4g.small	24	576	2	20%**
t4g.medium	24	576	2	20%**
t4g.large	36	864	2	30%**
t4g.xlarge	96	2304	4	40%**
t4g.2xlarge	192	4608	8	40%**

* Il numero di crediti che possono essere accumulati è equivalente al numero di crediti che possono essere guadagnati in un periodo di 24 ore.

** La percentuale di utilizzo di base nella tabella è per vCPU. In CloudWatch, viene mostrato l'utilizzo della CPU per vCPU. Ad esempio, l'utilizzo della CPU per un'`t3.large`istanza che opera al livello di base viene mostrato come 30% nelle metriche della CPU. CloudWatch Per informazioni su come calcolare l'utilizzo di base, consulta Utilizzo di base.

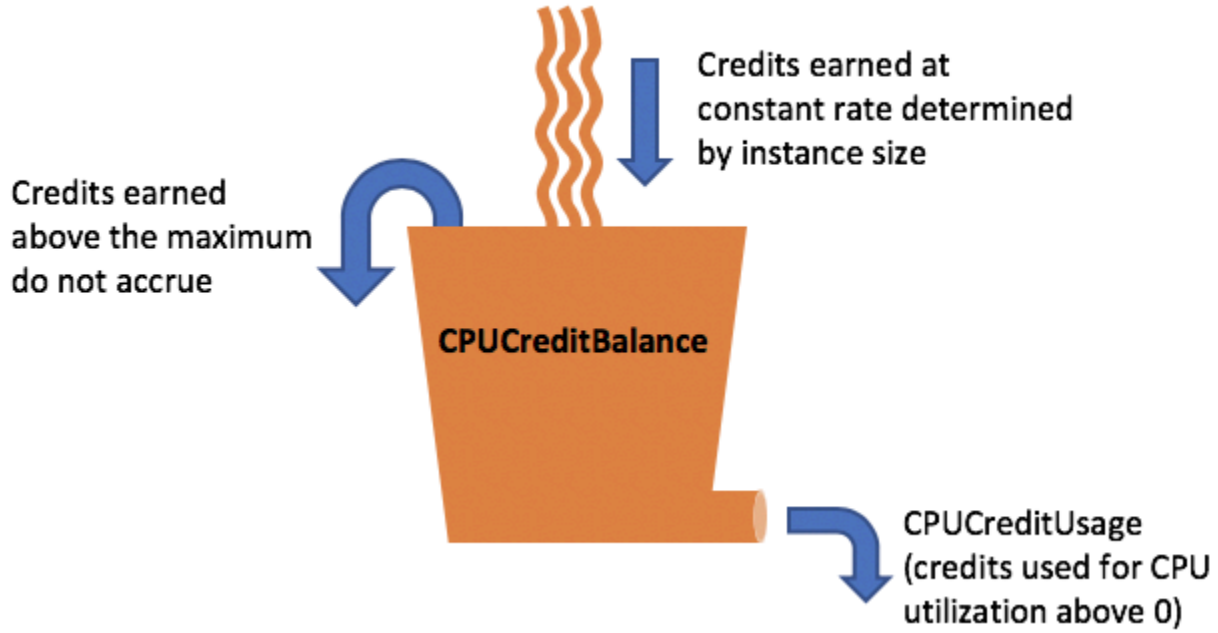
*** Ogni vCPU è un thread di un core Intel Xeon o un core AMD EPYC, ad eccezione delle istanze T2 e T4g.

Tasso di guadagno di crediti CPU

Il numero di crediti CPU guadagnati all'ora è determinato dalle dimensioni dell'istanza. Ad esempio, un'istanza `t3.nano` guadagna sei crediti all'ora, mentre una `t3.small` guadagna 24 crediti all'ora. La tabella precedente elenca il tasso di guadagno di crediti per tutte le istanze.

Limite di accumulo di crediti CPU

Sebbene i crediti guadagnati non scadano mai su un'istanza in esecuzione, esiste un limite al numero di crediti guadagnati che un'istanza può accumulare. Il limite è determinato dal limite del saldo del credito CPU. Una volta raggiunto il limite, tutti i nuovi crediti guadagnati vengono scartati, come indicato nell'immagine seguente. Il bucket pieno indica il limite di saldo del credito CPU e lo spillover indica i crediti appena guadagnati che superano il limite.



Il limite di saldo del credito CPU è diverso per ciascuna dimensione dell'istanza Ad esempio, un'istanza `t3.micro` può accumulare un massimo di 288 crediti CPU guadagnati nel saldo del credito CPU. La tabella precedente elenca il numero massimo di crediti guadagnati che ciascuna istanza di può accumulare.

Anche le istanze T2 Standard guadagnano crediti di lancio. I crediti di lancio non contano per il limite del saldo del credito CPU. Se un'istanza T2 non ha speso i suoi crediti di avvio e rimane inattiva per un periodo di 24 ore mentre accumula crediti guadagnati, il suo saldo del credito CPU appare oltre il limite. Per ulteriori informazioni, consulta Crediti di lancio.

Le istanze T4g, T3a e T3 non guadagnano crediti di avvio. Queste istanze vengono avviate come `unlimited` per impostazione predefinita, pertanto possono espandersi immediatamente all'avvio senza crediti di lancio. Le istanze T3 vengono avviate su host dedicato in modalità `standard` per impostazione predefinita; la modalità `unlimited` non è supportata per le istanze T3 su un host dedicato.

Durata dei crediti CPU accumulati

I crediti CPU su un'istanza in esecuzione non scadono.

Per T2, il saldo del credito CPU non persiste tra le interruzioni e gli avvii dell'istanza. Se interrompi un'istanza T2, l'istanza perde tutti i crediti accumulati.

Per T4g, T3a e T3, il saldo di crediti CPU viene conservato per sette giorni, trascorsi i quali i crediti vengono persi. Se avvii l'istanza entro sette giorni, non viene perso alcun credito.

Per ulteriori informazioni, consulta la tabella delle `CPUCreditBalance` CloudWatch metriche.

Utilizzo di base

L'utilizzo di base è il livello in cui la CPU può essere utilizzata per un saldo creditizio netto pari a zero, quando il numero di crediti CPU guadagnati corrisponde al numero di crediti CPU utilizzati. L'utilizzo di base è noto anche come linea di base.

L'utilizzo di base è espresso come percentuale di utilizzo della vCPU, calcolata come segue:

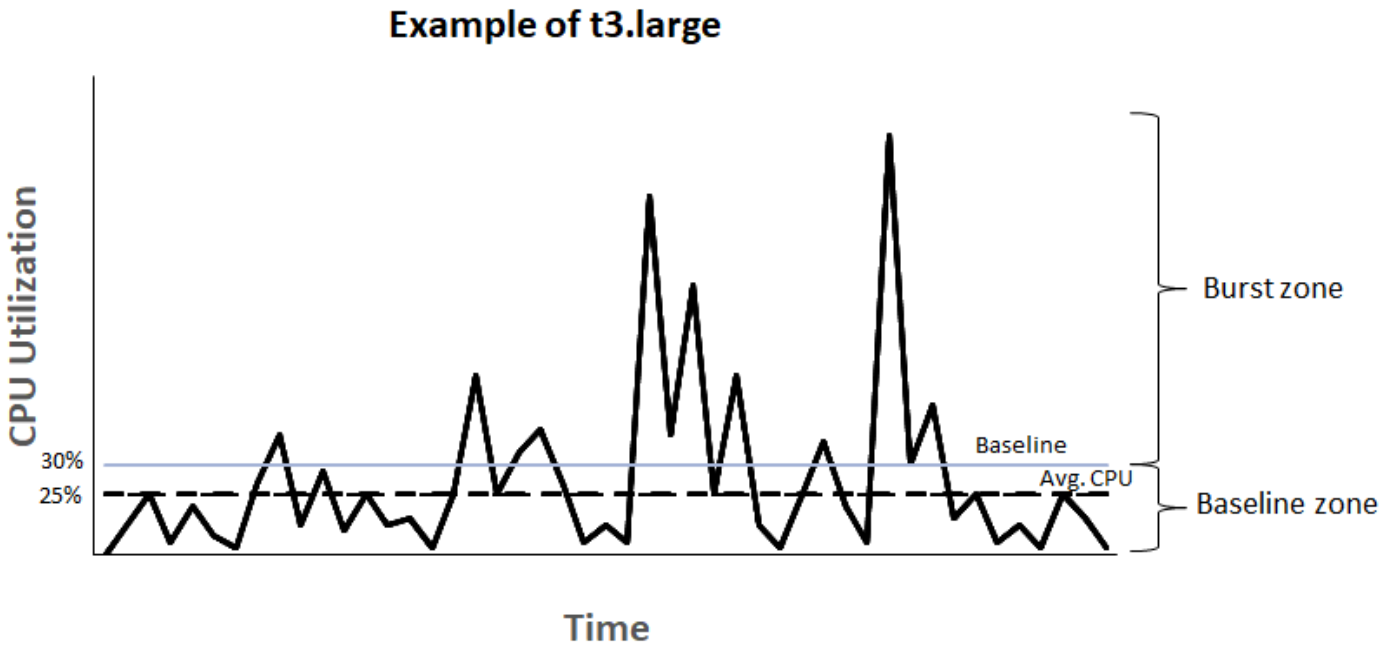
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline
utilization
```

Ad esempio, un'istanza `t3.nano`, con 2 vCPU, guadagna 6 crediti all'ora, con un utilizzo di base del 5%, calcolato come segue:

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

Un'`t3.large`istanza con 2 vCPU guadagna 36 crediti all'ora, con un utilizzo di base del 30% (). `(36/2)/60`

Il grafico seguente fornisce un esempio di utilizzo medio della CPU inferiore `t3.large` alla linea di base.



Modalità illimitata per istanze a prestazioni espandibili

Un'istanza a prestazioni espandibili configurata come `unlimited` può sostenere un utilizzo elevato della CPU per tutto il tempo necessario in qualsiasi momento. Il prezzo orario copre automaticamente tutti i picchi di utilizzo della CPU se l'utilizzo medio della CPU dell'istanza corrisponde o è inferiore alla baseline per un periodo di 24 ore o la durata dell'istanza, a seconda di quale dei due è inferiore.

Per la grande maggioranza dei carichi di lavoro per scopi generici, le istanze configurate come `unlimited` offrono prestazioni elevate senza addebiti aggiuntivi. Se l'istanza viene eseguita a un utilizzo più elevato della CPU per un periodo di tempo prolungato, verrà applicata una tariffa fissa aggiuntiva all'ora vCPU. Per informazioni sui prezzi, consulta prezzi di Amazon EC2 e prezzi di T2/T3/T4 in modalità illimitata.

Se utilizzi un'`t3.micro`istanza `t2.micro` or nell'ambito dell'Piano gratuito di AWSofferta e la utilizzi in `unlimited` modalità standard, potrebbero essere applicati dei costi se l'utilizzo medio su un periodo di 24 ore consecutive supera l'utilizzo di base dell'istanza.

Le istanze T4g, T3a e T3 vengono avviate come impostazione predefinita (a meno che non si modifichi l'impostazione `unlimited` predefinita). Se l'utilizzo medio della CPU per un periodo di 24 ore supera la baseline, vengono addebitati i costi per i crediti in eccedenza. Se avvii le Istanze spot come `unlimited` e prevedi di utilizzarle immediatamente e per un breve periodo, senza tempo di inattività per accumulare crediti CPU, vengono addebitati i costi per i crediti in eccedenza. Consigliamo di avviare le Istanze spot in modalità standard per evitare di pagare costi più elevati. Per ulteriori informazioni, consulta Possibilità di addebito dei costi per i crediti extra e Istanze a prestazioni espandibili.

> **Note**
>
> Le istanze T3 vengono avviate su host dedicato in modalità `standard` per impostazione predefinita; la modalità `unlimited` non è supportata per le istanze T3 su un host dedicato.

Indice

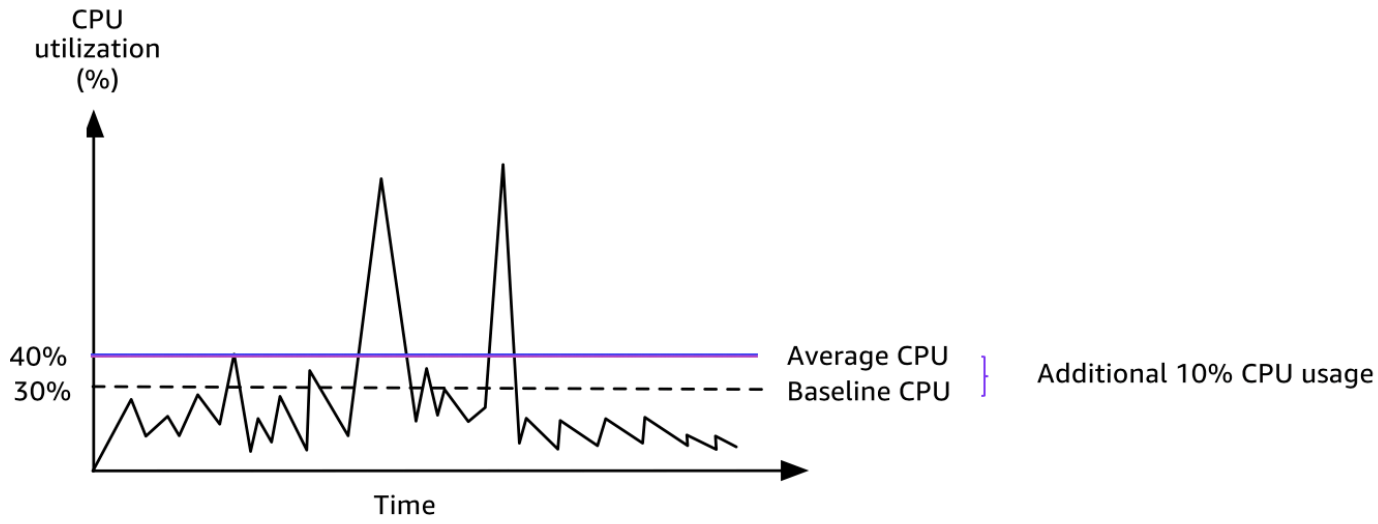
Concetti della modalità illimitata

La modalità `unlimited` è un'opzione di configurazione del credito per le istanze a prestazioni espandibili. Può essere abilitata o disabilitata in qualsiasi momento per un'istanza in esecuzione o arrestata. Puoi impostarla `unlimited` come opzione di credito predefinita a livello di account per AWS regione, per famiglia di istanze Burstable Performance, in modo che tutte le nuove istanze Burstable Performance nell'account vengano avviate utilizzando l'opzione di credito predefinita.

Come funzionano le istanze a prestazioni espandibili illimitata

Se un'istanza a prestazioni espandibili configurata come `unlimited` esaurisce il suo saldo del credito CPU, può spendere crediti extra per superare la linea di base. Quando l'utilizzo della CPU è inferiore alla baseline, utilizza i crediti CPU che guadagna per pagare i crediti extra spesi in precedenza. La possibilità di guadagnare crediti CPU per pagare i crediti extra consente ad Amazon EC2 di calcolare una media dell'utilizzo della CPU di un'istanza in un periodo di 24 ore. Se l'utilizzo medio della CPU in un periodo di 24 ore supera la baseline, l'istanza verrà fatturata per l'uso aggiuntivo a una tariffa fissa aggiuntiva per vCPU/ora.

Il seguente grafico mostra l'utilizzo della CPU di un `t3.large`. L'utilizzo di base della CPU per un `t3.large` è 30%. Se l'istanza viene eseguita al 30% di utilizzo medio della CPU o meno in un periodo di 24 ore, non sono previsti costi aggiuntivi perché i costi sono già coperti dal prezzo orario dell'istanza. Tuttavia, se l'istanza viene eseguita al 40% di utilizzo medio della CPU in un periodo di 24 ore, come mostrato nel grafico, l'istanza viene fatturata per il 10% di utilizzo aggiuntivo della CPU a una tariffa fissa aggiuntiva per vCPU/ora.



Per ulteriori informazioni sull'utilizzo di base per vCPU per ogni tipo di istanza e sul numero di crediti guadagnati da ogni tipo di istanza, consulta la tabella dei crediti.

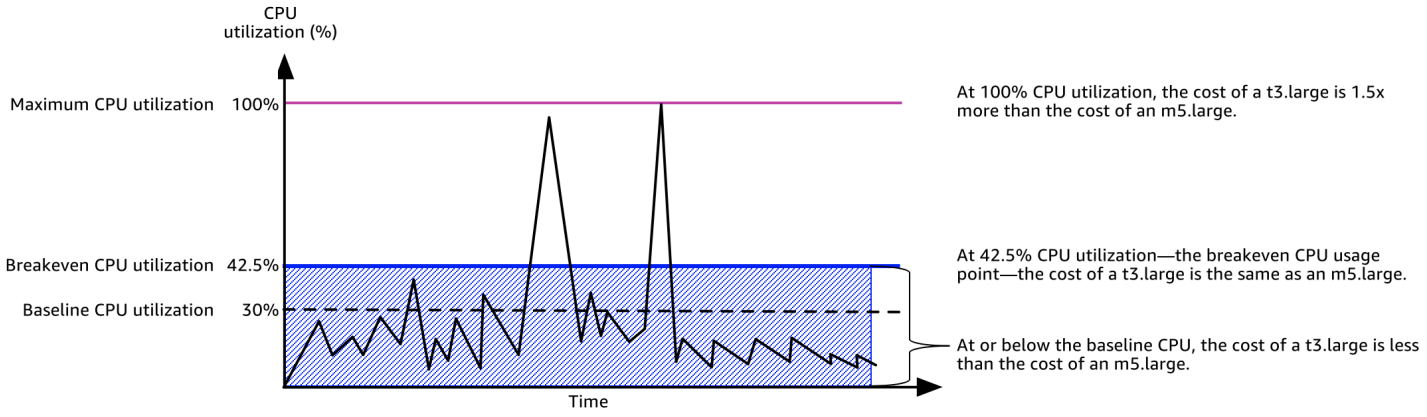
Quando utilizzare la modalità illimitata rispetto alla CPU fissa

Nel determinare se utilizzare un'istanza a prestazioni espandibili in modalità `unlimited`, ad esempio T3 o un'istanza a prestazioni fisse, ad esempio M5, è necessario determinare il punto di utilizzo della CPU di break even. L'utilizzo della CPU di break even per un'istanza a prestazioni espandibili

è il punto in cui il costo di un'istanza a prestazioni espandibili è identico a quello di un'istanza a prestazioni fisse. L'utilizzo della CPU di break even consente di determinare quanto segue:

- Se l'utilizzo medio della CPU in un periodo di 24 ore corrisponde o è inferiore all'utilizzo della CPU di break even, utilizza un'istanza a prestazioni espandibili in modalità `unlimited` per trarre vantaggio dal prezzo inferiore di un'istanza a prestazioni espandibili pur ottenendo le stesse prestazioni di un'istanza a prestazioni fisse.
- Se l'utilizzo medio della CPU in un periodo di 24 ore è superiore all'utilizzo della CPU di break even, l'istanza a prestazioni espandibili costerà di più rispetto all'istanza a prestazioni fisse di dimensioni equivalenti. Se un'istanza T3 emette continuamente picchi al 100% CPU, si pagherà all'incirca 1,5 volte il prezzo di un'istanza M5 di dimensioni equivalenti.

Il grafico seguente mostra il punto di utilizzo della CPU di break even in cui il costo di un `t3.large` è identico a quello di un `m5.large`. Il punto di utilizzo della CPU di break even per un `t3.large` è 42,5%. Se l'utilizzo medio della CPU è al 42,5%, il costo dell'esecuzione di `t3.large` è identico a quello di un `m5.large` ed è più costoso se l'utilizzo medio della CPU è superiore a 42,5%. Se il carico di lavoro richiede meno del 42,5% di utilizzo medio della CPU, puoi trarre vantaggio dal prezzo inferiore del `t3.large` pur ottenendo le stesse prestazioni di un`m5.large`.



La seguente tabella mostra come calcolare la soglia di utilizzo della CPU di break even in modo da determinare quando è meno costoso utilizzare un'istanza a prestazioni espandibili in modalità `unlimited` o un'istanza a prestazioni fisse. Le colonne nella tabella sono etichettate da A a K.

Tipo di istanza	vCPU	T3 prezzo*/ ora	M5 prezzo*/ ora	Differenza a prezzo	Utilizzo di base T3 per vCPU (%)	Costo per vCPU/ ora per crediti extra	Costo per vCPU/ minuto	Minuti di burst aggiuntivi disponibili per vCPU	% CPU aggiuntiva disponibile	% CPU di break even
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	0,0835 USD	0,096 USD	0,0125 USD	30%	0,05 $	0,000833 USD	15	12,5%	42,5%

* Prezzo basato su us-east-1 e sistema operativo Linux.

La tabella fornisce le informazioni seguenti:

- La colonna A mostra il tipo di istanza, `t3.large`.
- La colonna B mostra il numero di vCPU per `t3.large`.
- La colonna C mostra il prezzo di un `t3.large` per ora.
- La colonna D mostra il prezzo di un `m5.large` per ora.
- La colonna E mostra la differenza di prezzo tra `t3.large` e `m5.large`.
- La colonna F mostra l'utilizzo di base per vCPU di `t3.large`, che è del 30%. Al livello base, il costo orario dell'istanza copre il costo di utilizzo della CPU.
- La colonna G mostra la tariffa fissa aggiuntiva per vCPU/ora che viene addebitata a un'istanza se emette picchi al 100% CPU dopo che ha esaurito i sui crediti guadagnati.
- La colonna H mostra la tariffa fissa aggiuntiva per vCPU/minuto che viene addebitata a un'istanza se emette picchi al 100% CPU dopo che ha esaurito i sui crediti guadagnati.
- La colonna I mostra il numero di minuti aggiuntivi in cui `t3.large` può emettere picchi all'ora al 100% CPU pagando lo stesso prezzo orario di un `m5.large`.

- La colonna J mostra l'utilizzo aggiuntivo della CPU (in %) rispetto alla baseline in cui l'istanza può emettere picchi pagando lo stesso prezzo orario di un `m5.large`.
- La colonna K mostra l'utilizzo della CPU di break even (in %) in cui `t3.large` può emettere picchi senza pagare più di `m5.large`. In caso di superamento, il costo di `t3.large` è maggiore di quello di `m5.large`.

La tabella seguente mostra l'utilizzo della CPU di break even (in %) per tipi di istanza T3 in confronto ai tipi di istanza M5 di dimensioni simili.

Tipo di istanza T3	Utilizzo della CPU di break even (in %) per T3 in confronto a M5
`t3.large`	42,5%
`t3.xlarge`	52,5%
`t3.2xlarge`	52,5%

Possibilità di addebito dei costi per i crediti extra

Se l'utilizzo medio della CPU di un'istanza corrisponde o è inferiore alla baseline, non vengono addebitati costi aggiuntivi per l'istanza. Dato che un'istanza guadagna un numero massimo di crediti in un periodo di 24 ore (ad esempio, un'istanza `t3.micro` può guadagnare un massimo di 288 crediti in un periodo di 24 ore), può spendere crediti extra fino a quel massimo senza alcun addebito.

Tuttavia, se l'utilizzo della CPU rimane al di sopra della baseline, l'istanza non può guadagnare abbastanza crediti per pagare i crediti extra spesi. I crediti extra che non vengono pagati, vengono addebitati a una tariffa fissa aggiuntiva all'ora vCPU. Per informazioni sulla tariffa, consulta prezzi T2/T3/T4G in modalità illimitata.

I crediti extra spesi in precedenza subiscono costi aggiuntivi quando si verifica uno dei seguenti casi:

- I crediti extra spesi vanno oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore. I crediti extra spesi, che eccedono il limite, subiscono costi aggiuntivi alla fine dell'ora;
- l'istanza viene arrestata o terminata;
- l'istanza passa da `unlimited` a `standard`.

I crediti in eccesso spesi vengono tracciati in base alla metrica. CloudWatch `CPUSurplusCreditBalance` I crediti in eccesso che vengono addebitati vengono tracciati in base alla metrica. CloudWatch `CPUSurplusCreditsCharged` Per ulteriori informazioni, consulta Metriche aggiuntive per istanze con prestazioni espandibili CloudWatch .

Assenza di crediti di lancio per istanze T2 in modalità illimitata

Le istanze T2 Standard ricevono crediti di lancio, mentre le istanze T2 Unlimited non li ricevono. Un'istanza T2 Unlimited può superare la baseline in qualsiasi momento senza alcun addebito fino a quando l'utilizzo medio della CPU dell'istanza corrisponde o è inferiore alla baseline per un periodo continuo di 24 ore o per la sua durata, a seconda di quale dei due è inferiore. Pertanto, le istanze T2 Unlimited non richiedono crediti di lancio per ottenere prestazioni elevate immediatamente dopo l'avvio.

Se un'istanza T2 passa da `standard` a `unlimited`, tutti i crediti di lancio accumulati vengono rimossi da `CPUCreditBalance` prima di trasferire il `CPUCreditBalance` restante.

Le istanze T4g, T3a e T3 non ricevono mai crediti di avvio perché supportano la modalità Illimitato. La configurazione del credito in modalità Illimitato consente alle istanze T4g, T3a e T3 di utilizzare tutta la CPU necessaria per superare la baseline e per tutto il tempo necessario.

Abilitazione della modalità illimitata

È possibile passare da `unlimited` a `standard` e da `standard` a `unlimited` in qualsiasi momento su un'istanza in esecuzione o interrotta. Per ulteriori informazioni, consulta Avvio di un'istanza a prestazioni espandibili in modalità Standard o illimitata e Modifica della specifica crediti di un'istanza a prestazioni espandibili.

Puoi impostarla `unlimited` come opzione di credito predefinita a livello di account per AWS regione, per famiglia di istanze Burstable Performance, in modo che tutte le nuove istanze Burstable Performance presenti nell'account vengano avviate utilizzando l'opzione di credito predefinita. Per ulteriori informazioni, consulta Impostazione della specifica crediti predefinita per l'account.

Puoi verificare se l'istanza espandibile è configurata come `unlimited` o `standard` utilizzando la console Amazon EC2 o AWS CLI. Per ulteriori informazioni, consulta Visualizzazione della specifica crediti di un'istanza a prestazioni espandibili e Visualizzazione della specifica crediti predefinita.

Cosa succede ai crediti quando si passa dalla modalità illimitata a Standard e viceversa

`CPUCreditBalance`è una CloudWatch metrica che tiene traccia del numero di crediti accumulati da un'istanza. `CPUSurplusCreditBalance`è una CloudWatch metrica che tiene traccia del numero di crediti in eccesso spesi da un'istanza.

Quando si modifica un'istanza configurata come `unlimited` in `standard`, si verifica quanto segue:

- Il valore `CPUCreditBalance` rimane invariato e viene trasferito.
- Il valore `CPUSurplusCreditBalance` viene immediatamente addebitato.

Quando un'istanza `standard` passa a `unlimited`, si verifica quanto segue:

- Il valore `CPUCreditBalance` contenente i crediti guadagnati accumulati viene trasferito.
- Per le istanze T2 Standard, tutti i crediti di lancio accumulati vengono rimossi dal valore `CPUCreditBalance`, mentre il valore `CPUCreditBalance` residuo, contenente i crediti guadagnati accumulati, viene trasferito.

Monitoraggio dell'utilizzo del credito

Per verificare se la tua istanza sta spendendo più crediti di quelli forniti dalla linea di base, puoi utilizzare le CloudWatch metriche per monitorare l'utilizzo e puoi impostare allarmi orari per ricevere notifiche sull'utilizzo del credito. Per ulteriori informazioni, consulta Monitoraggio dei crediti CPU per istanze espandibili.

Esempi di modalità illimitata

Di seguito vengono forniti esempi che spiegano l'utilizzo del credito per le istanze configurate come `unlimited`.

Esempi

- Esempio 1: spiegazione dell'uso del credito con T3 in modalità illimitata
- Esempio 2: spiegazione dell'uso del credito con T2 in modalità illimitata

Esempio 1: spiegazione dell'uso del credito con T3 in modalità illimitata

Questo esempio illustra l'utilizzo della CPU di un'istanza `t3.nano` avviata come `unlimited` e in che modo spende i crediti guadagnati ed extra per sostenere l'utilizzo della CPU.

Un'istanza `t3.nano` guadagna 144 crediti CPU in un periodo continuo di 24 ore, che può utilizzare per 144 minuti di utilizzo di vCPU. Quando esaurisce il saldo del credito della CPU (rappresentato dalla CloudWatch metrica`CPUCreditBalance`), può spendere i crediti CPU in eccesso, che non ha ancora guadagnato, per funzionare per tutto il tempo necessario. Dato che un'istanza `t3.nano` guadagna un massimo di 144 crediti in un periodo di 24 ore, può spendere crediti extra fino a quel valore massimo senza alcun addebito immediato. Se spende più di 144 crediti CPU, viene addebitata la differenza alla fine dell'ora.

L'intento dell'esempio, illustrato dal seguente grafico, è quello di mostrare come un'istanza possa ottimizzare le prestazioni utilizzando i crediti extra anche dopo aver esaurito il suo `CPUCreditBalance`. I seguente flusso di lavoro fa riferimento ai punti numerati sul grafico:

P1 - All'ora– 0 sul grafico l'istanza viene avviata come `unlimited` e inizia immediatamente a guadagnare crediti. L'istanza rimane inattiva dal momento in cui viene avviata —(l'utilizzo della CPU è pari allo 0%)— e non vengono spesi crediti. Tutti i crediti non spesi vengono accumulati nel saldo del credito. Per le prime 24 ore, `CPUCreditUsage` è a 0 e il valore `CPUCreditBalance` raggiunge il suo massimo di 144.

P2 – per le 12 ore successive, l'utilizzo della CPU è al 2,5%, ovvero inferiore al 5% della baseline. L'istanza guadagna più crediti di quanti ne spende, ma il valore `CPUCreditBalance` non può superare il suo massimo di 144 crediti.

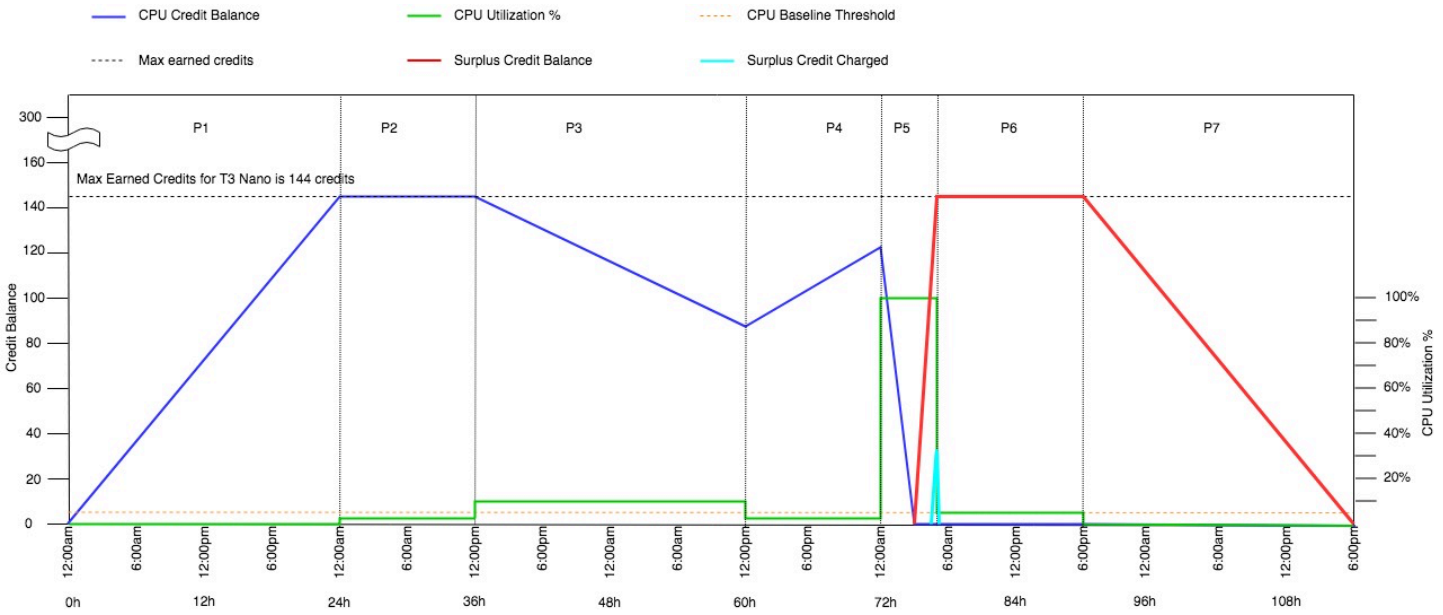
P3 – per le 24 ore successive, l'utilizzo della CPU è al 7% (superiore alla baseline), il che richiede una spesa del 57,6% dei crediti. L'istanza spende più crediti di quanti ne guadagna e il valore `CPUCreditBalance` si riduce a 86,4 crediti.

P4 – per le 12 ore successive, l'utilizzo della CPU si riduce al 2,5% (inferiore alla baseline), il che richiede una spesa di 36 crediti. Allo stesso tempo, l'istanza guadagna 72 crediti. L'istanza guadagna più crediti di quanti ne spende e il valore `CPUCreditBalance` aumenta a 122 crediti.

P5 – per le 5 ore successive, l'istanza aumenta al 100% dell'utilizzo della CPU e spende un totale di 570 crediti per sostenere l'espansione. Dopo circa un'ora, l'istanza esaurisce il suo intero `CPUCreditBalance` di 122 crediti e inizia a spendere crediti extra per sostenere l'utilizzo elevato della CPU, per un totale di 448 crediti extra in questo periodo di tempo (570-122=448). Quando il valore `CPUSurplusCreditBalance` raggiunge 144 crediti della CPU (il massimo che un'istanza `t3.nano` può guadagnare in un periodo di 24 ore), tutti i crediti extra spesi successivamente non possono essere compensati con crediti guadagnati. I crediti extra spesi successivamente ammontano a 304 crediti (448-144=304), il che si traduce in un piccolo costo aggiuntivo al termine dell'ora per 304 crediti.

P6 – per le 13 ore successive, l'utilizzo della CPU è al 5% (pari alla baseline). L'istanza guadagna lo stesso numero di crediti che spende, senza eccessi da ripagare il `CPUSurplusCreditBalance`. Il valore `CPUSurplusCreditBalance` rimane a 144 crediti.

P7 – per le ultime 24 ore di questo esempio, l'istanza è inattiva e l'utilizzo della CPU è allo 0%. In questo arco di tempo, l'istanza guadagna 144 crediti, che utilizza per ripagare il `CPUSurplusCreditBalance`.



Esempio 2: spiegazione dell'uso del credito con T2 in modalità illimitata

Questo esempio illustra l'utilizzo della CPU di un'istanza `t2.nano` avviata come `unlimited` e in che modo spende i crediti guadagnati ed extra per sostenere l'utilizzo della CPU.

Un'istanza `t2.nano` guadagna 72 crediti CPU in un periodo continuo di 24 ore, che può utilizzare per 72 minuti di utilizzo di vCPU. Quando esaurisce il saldo di credito della CPU (rappresentato dalla CloudWatch metrica*`CPUCreditBalance`*), può spendere i crediti CPU in eccesso, che non ha ancora guadagnato, per esaurirli per tutto il tempo necessario. Dato che un'istanza `t2.nano` guadagna un massimo di 72 crediti in un periodo di 24 ore, può spendere crediti extra fino a quel valore massimo senza alcun addebito immediato. Se spende più di 72 crediti CPU, viene addebitata la differenza alla fine dell'ora.

L'intento dell'esempio, illustrato dal seguente grafico, è quello di mostrare come un'istanza possa ottimizzare le prestazioni utilizzando i crediti extra anche dopo aver esaurito il suo `CPUCreditBalance`. È possibile presumere che, all'inizio della linea temporale nel grafico, l'istanza abbia un saldo del credito accumulato uguale al numero massimo di crediti che può guadagnare in 24 ore. l seguente flusso di lavoro fa riferimento ai punti numerati sul grafico:

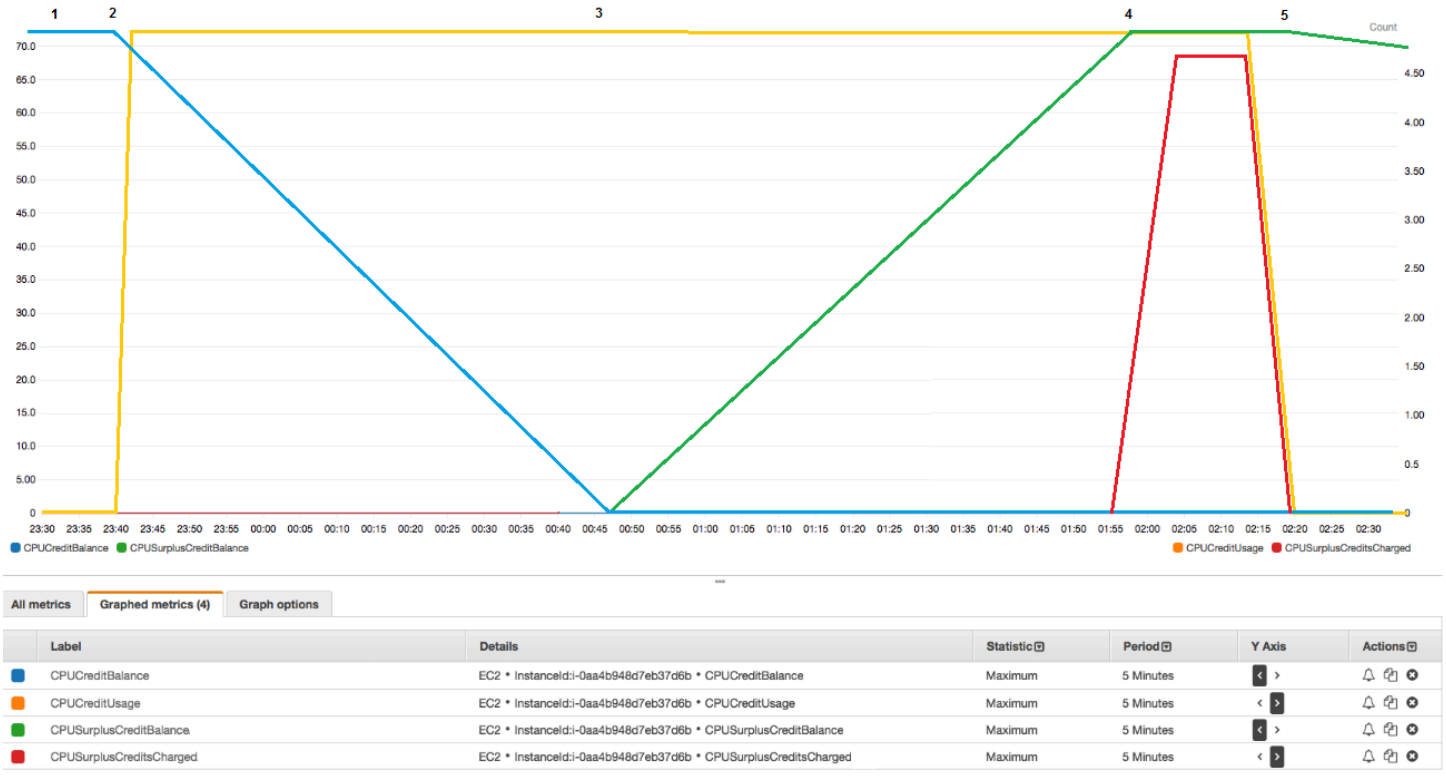
1 – nei primi 10 minuti, `CPUCreditUsage` è a 0 e il valore `CPUCreditBalance` rimane al suo massimo di 72.

2 – alle 23:40, con l'aumentare dell'utilizzo della CPU, l'istanza spende i crediti della CPU e il valore `CPUCreditBalance` diminuisce.

3 – intorno alle 00:47, l'istanza esaurisce l'intero `CPUCreditBalance` e inizia a spendere crediti extra per sostenere l'utilizzo elevato della CPU.

4 – i crediti extra vengono spesi fino all'01:55, quando il valore `CPUSurplusCreditBalance` raggiunge 72 crediti CPU. Questo corrisponde al massimo che un'istanza `t2.nano` può guadagnare in un periodo di 24 ore. Eventuali crediti extra spesi successivamente non possono essere compensati con crediti guadagnati nel periodo di 24 ore, il che si traduce in un piccolo costo aggiuntivo al termine dell'ora.

5 – l'istanza continua a spendere crediti extra fino a circa le 02:20. A questo punto, l'utilizzo della CPU è inferiore alla baseline e l'istanza inizia a guadagnare crediti a 3 crediti all'ora (o 0,25 crediti ogni 5 minuti), utilizzati per pagare il `CPUSurplusCreditBalance`. Dopo che il valore `CPUSurplusCreditBalance` si riduce a 0, l'istanza inizia ad accumulare crediti guadagnati nel suo `CPUCreditBalance` a 0,25 crediti ogni 5 minuti.



Calcolo della fattura (istanza Linux)

I crediti in eccesso costano 0,05 USD per ora di vCPU. L'istanza ha speso circa 25 crediti extra tra le 01:55 e le 02:20, che equivalgono a 0,42 vCPU/ora. I costi aggiuntivi per questa istanza sono 0,42 ore vCPU x 0,05 USD/vCPU-ora = 0,021 USD, arrotondati a 0,02 USD. Ecco la fattura di fine mese per questa istanza T2 Unlimited:

Amazon Elastic Compute Cloud running Linux/UNIX		
$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.02

Calcolo della fattura (istanza Windows)

I crediti in eccesso costano 0,096 USD per vCPU all'ora. L'istanza ha speso circa 25 crediti extra tra le 01:55 e le 02:20, che equivalgono a 0,42 vCPU/ora. I costi aggiuntivi per questa istanza sono 0,42 ore vCPU x 0,096 USD/vCPU-ora = 0,04032 USD, arrotondati a 0,04 USD. Ecco la fattura di fine mese per questa istanza T2 Unlimited:

Amazon Elastic Compute Cloud running Windows		
$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.04

È possibile impostare gli avvisi di fatturazione per essere avvisati ogni ora di eventuali addebiti accumulati e agire, se necessario.

Modalità standard per istanze a prestazioni espandibili

Un'istanza a prestazioni espandibili configurata come `standard` è adatta ai carichi di lavoro con un utilizzo medio della CPU costantemente inferiore all'utilizzo di base dell'istanza. Per superare la baseline, l'istanza spende i crediti accumulati nel suo saldo del credito CPU. Se l'istanza sta esaurendo i crediti accumulati, l'utilizzo della CPU viene gradualmente ridotto al livello di prestazioni di base, in modo che l'istanza non subisca una forte riduzione delle prestazioni una volta esaurito il saldo del credito CPU. Per ulteriori informazioni, consulta Concetti e definizioni chiave per istanze espandibili.

Indice

Concetti della modalità Standard

La modalità `standard` è un'opzione di configurazione per le istanze a prestazioni espandibili. Può essere abilitata o disabilitata in qualsiasi momento per un'istanza in esecuzione o arrestata. È possibile impostare `standard` come opzione di credito predefinita a livello di account per AWS regione, per famiglia di istanze Burstable Performance, in modo che tutte le nuove istanze Burstable Performance presenti nell'account vengano avviate utilizzando l'opzione di credito predefinita.

Come funzionano le istanze a prestazioni espandibili Standard

Quando un'istanza a prestazioni espandibili configurata come `standard` è in fase di esecuzione, guadagna continuamente (a una risoluzione a livello di millisecondo) un tasso fisso di crediti guadagnati all'ora. Quando un'istanza T2 Standard viene interrotta, perde tutti i crediti accumulati e il suo saldo attivo viene azzerato. Quando viene riavviata, riceve una nuova serie di crediti di lancio e inizia ad accumulare crediti guadagnati. Per istanze Standard T4g, T3a e T3, il saldo di crediti della CPU viene conservato per sette giorni, trascorsi i quali l'istanza viene arrestata e i crediti vengono persi. Se avvii l'istanza entro sette giorni, non viene perso alcun credito.

Le istanze T2 Standard ricevono due tipi di crediti CPU: crediti guadagnati e crediti di lancio. Quando un'istanza di T2 Standard è in fase di esecuzione, guadagna continuamente (a una risoluzione a livello di millisecondo) un tasso fisso di crediti guadagnati all'ora. All'inizio, non ha guadagnato ancora i crediti necessari per una buona esperienza di avvio; pertanto, per fornire una buona esperienza di startup, riceve inizialmente i crediti di lancio, che spende mentre accumula crediti guadagnati.

Le istanze T4g, T3a e T3 non ricevono mai crediti di avvio perché supportano la modalità Illimitato. La configurazione del credito in modalità Illimitato consente alle istanze T4g, T3a e T3 di utilizzare tutta la CPU necessaria per superare la baseline e per tutto il tempo necessario.

Crediti di lancio

Le istanze T2 Standard ottengono 30 crediti di lancio per vCPU al lancio o all'avvio, mentre le istanze T1 Standard ottengono 15 crediti di lancio. Ad esempio, un'istanza `t2.micro` ha un vCPU e ottiene 30 crediti di lancio, mentre un'istanza `t2.xlarge` ha quattro vCPU e ottiene 120 crediti di lancio. I crediti di lancio sono progettati per fornire una buona esperienza di startup in modo da consentire immediatamente dopo l'avvio l'ottimizzazione delle istanze prima che abbiano accumulato crediti guadagnati.

Per primi vengono spesi i crediti di lancio, prima dei crediti guadagnati. I crediti di lancio non spesi vengono accumulati nel saldo del credito CPU, ma non contano per il limite del saldo del credito CPU. Ad esempio, un'istanza `t2.micro` ha un limite del saldo del credito CPU di 144 crediti guadagnati. Se viene avviata e rimane inattiva per 24 ore, il suo saldo del credito CPU raggiunge 174 (30 crediti di lancio + 144 crediti guadagnati), che è oltre il limite. Tuttavia, una volta che l'istanza spende i 30 crediti di lancio, il saldo del credito non può superare 144. Per ulteriori informazioni sul limite del saldo del credito CPU per ciascuna dimensione dell'istanza, consulta la tabella del credito.

La tabella seguente elenca l'allocazione iniziale del credito CPU ricevuta all'avvio e il numero di vCPU.

Tipo di istanza	Crediti di lancio	vCPU
`t1.micro`	15	1
`t2.nano`	30	1
`t2.micro`	30	1
`t2.small`	30	1

Tipo di istanza	Crediti di lancio	vCPU
`t2.medium`	60	2
`t2.large`	60	2
`t2.xlarge`	120	4
`t2.2xlarge`	240	8

Limiti dei crediti di lancio

Il numero di volte in cui le istanza T2 Standard possono ricevere crediti di lancio è limitato. Il limite predefinito è di 100 avvii di tutte le istanze T2 Standard combinate per account, per regione, per periodo continuo di 24 ore. Ad esempio, il limite viene raggiunto quando un'istanza viene interrotta e avviata 100 volte in un periodo di 24 ore oppure quando vengono avviate 100 istanze in un periodo di 24 ore o se vengono avviate altre combinazioni equivalenti a 100 avvii. I nuovi account potrebbero avere un limite inferiore, che aumenta nel tempo in base al tuo utilizzo.

> **Tip**
>
> Per garantire che i carichi di lavoro ottengano sempre le prestazioni di cui hanno bisogno, passa a Modalità illimitata per istanze a prestazioni espandibili o prendi in considerazione l'utilizzo di una dimensione di istanza più grande.

Differenze tra crediti di lancio e crediti guadagnati

La seguente tabella elenca le differenze tra i crediti di lancio e i crediti guadagnati.

	Crediti di lancio	Crediti guadagnati
Tasso di guadagno di crediti	Le istanze T2 Standard ottengono 30 crediti di lancio per vCPU all'avvio. Se un'istanza T2 passa da `unlimited` a `standard`, non ottiene i crediti di lancio al momento del passaggio.	Ogni istanza T2 guadagna continuam ente (a una risoluzione a livello di millisecondo) un tasso fisso di crediti CPU all'ora, a seconda delle dimension i dell'istanza. Per ulteriori informazioni sul numero di crediti CPU guadagnat

	Crediti di lancio	Crediti guadagnati
		i per dimensione dell'istanza, consulta tabella del credito.
Limite di guadagno di crediti	Il limite per la ricezione di crediti di lancio è di 100 avvii di tutte le istanze T2 Standard combinate per account, per regione, per periodo continuo di 24 ore. I nuovi account potrebbero avere un limite inferiore, che aumenta nel tempo in base al tuo utilizzo.	Un'istanza T2 può accumulare più crediti rispetto al limite del saldo del credito CPU. Se il saldo del credito CPU ha raggiunto il suo limite, tutti i crediti guadagnati dopo il raggiungi mento del limite vengono scartati. I crediti di lancio non contano per il limite. Per ulteriori informazioni sul limite del saldo del credito CPU per ciascuna dimensione dell'istanza T2, consulta la tabella del credito.
Utilizzo crediti	Per primi vengono spesi i crediti di lancio, prima dei crediti guadagnati.	I crediti guadagnati vengono spesi solo dopo aver speso tutti i crediti di lancio.
Scadenza crediti	Quando è in esecuzione un'istanza T2 Standard, i crediti di lancio non scadono. Quando un'istanza di T2 Standard si interrompe o passa a T2 Unlimited, tutti i crediti di lancio vengono persi.	Quando un'istanza T2 è in esecuzion e, i crediti guadagnati accumulati non scadono. Quando l'istanza T2 si interrompe, tutti i crediti guadagnati accumulati vengono persi.

Il numero di crediti di lancio accumulati e di crediti accumulati guadagnati viene monitorato dalla metrica. CloudWatch `CPUCreditBalance` Per ulteriori informazioni, consulta la tabella delle metriche. `CPUCreditBalance` CloudWatch

Esempi di modalità Standard

Di seguito vengono forniti esempi che spiegano l'utilizzo del credito quando le istanze sono configurate come `standard`.

Esempi

- Esempio 1: spiegazione dell'uso del credito con T3 Standard

Esempio 1: spiegazione dell'uso del credito con T3 Standard

In questo esempio, è possibile vedere in che modo un'istanza `t3.nano` avviata come `standard` guadagna, accumula e spende crediti guadagnati. Viene mostrato in che modo il saldo dei crediti rispecchia i crediti guadagnati accumulati.

Un'istanza `t3.nano` in esecuzione guadagna 144 crediti ogni 24 ore. Il suo limite del saldo del credito è 144 crediti guadagnati. Una volta che il limite viene raggiunto, i nuovi crediti guadagnati vengono scartati. Per ulteriori informazioni sul numero di crediti che può essere guadagnato e accumulato, consulta la tabella del credito.

È possibile avviare un'istanza T3 Standard e utilizzarla immediatamente. In alternativa, è possibile avviare un'istanza T3 Standard e lasciarla inattiva per alcuni giorni prima di eseguire applicazioni su di essa. L'utilizzo o l'inattività di un'istanza determina se i crediti vengono spesi o accumulati. Se un'istanza rimane inattiva per 24 ore dal momento in cui viene avviata, il saldo del credito raggiunge il limite, ovvero il numero massimo di crediti guadagnati che possono essere accumulati.

Questo esempio descrive un'istanza che rimane inattiva per 24 ore dal momento in cui viene avviata e illustra sette periodi di tempo per 96 ore, mostrando la frequenza a cui i crediti vengono guadagnati, accumulati, spesi e scartati e il valore del saldo del credito alla fine di ciascun periodo.

I seguente flusso di lavoro fa riferimento ai punti numerati sul grafico:

P1 - All'ora– 0 sul grafico l'istanza viene avviata come `standard` e inizia immediatamente a guadagnare crediti. L'istanza rimane inattiva dal momento in cui viene avviata —(l'utilizzo della CPU è pari allo 0%)— e non vengono spesi crediti. Tutti i crediti non spesi vengono accumulati nel saldo del credito. Per le prime 24 ore, `CPUCreditUsage` è a 0 e il valore `CPUCreditBalance` raggiunge il suo massimo di 144.

P2 – per le 12 ore successive, l'utilizzo della CPU è al 2,5%, ovvero inferiore al 5% della baseline. L'istanza guadagna più crediti di quanti ne spende, ma il valore `CPUCreditBalance` non può superare il suo massimo di 144 crediti. Tutti i crediti guadagnati in eccesso rispetto al limite vengono scartati.

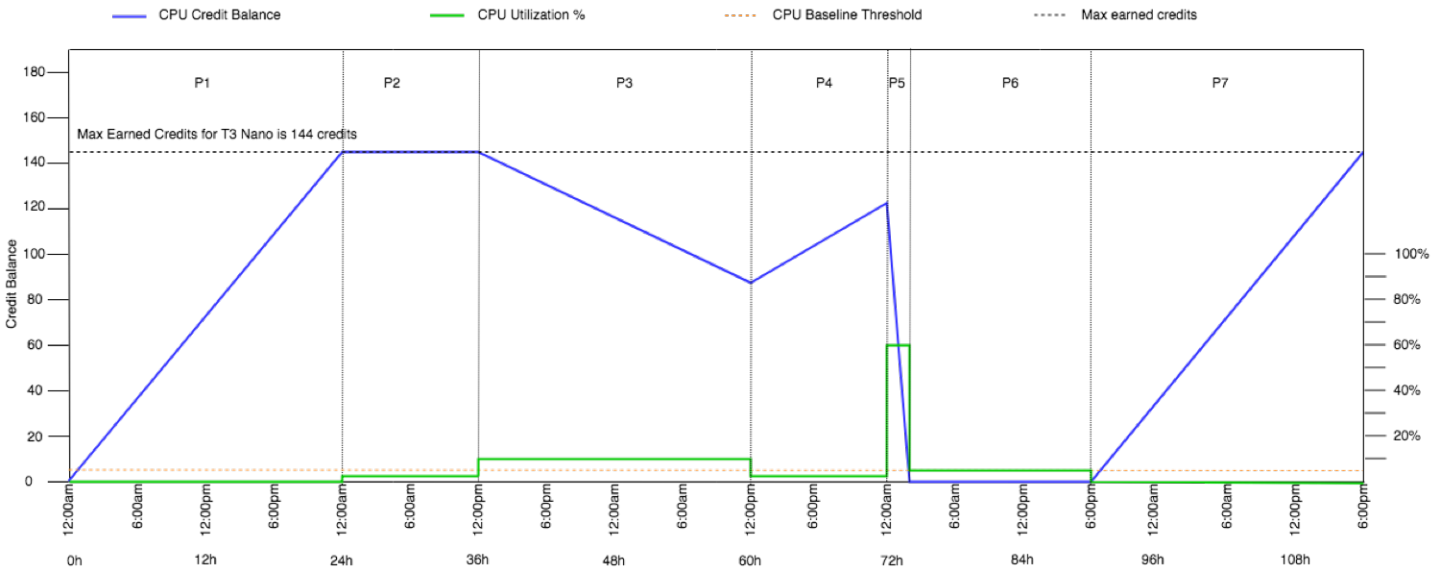
P3 – per le 24 ore successive, l'utilizzo della CPU è al 7% (superiore alla baseline), il che richiede una spesa del 57,6% dei crediti. L'istanza spende più crediti di quanti ne guadagna e il valore `CPUCreditBalance` si riduce a 86,4 crediti.

P4 – per le 12 ore successive, l'utilizzo della CPU si riduce al 2,5% (inferiore alla baseline), il che richiede una spesa di 36 crediti. Allo stesso tempo, l'istanza guadagna 72 crediti. L'istanza guadagna più crediti di quanti ne spende e il valore `CPUCreditBalance` aumenta a 122 crediti.

P5: per le 2 ore successive, l'istanza raggiunge il 60% di utilizzo della CPU ed esaurisce il suo intero valore `CPUCreditBalance` di 122 crediti. Al termine di questo periodo, con il `CPUCreditBalance` a zero, l'utilizzo di base scende al livello delle prestazioni di base del 5%. Al livello base, l'istanza guadagna lo stesso numero di crediti che spende.

P6 – per le 14 ore successive, l'utilizzo della CPU è al 5% (livello baseline). L'istanza guadagna lo stesso numero di crediti che spende. Il valore `CPUCreditBalance` rimane a 0.

P7 – per le ultime 24 ore di questo esempio, l'istanza è inattiva e l'utilizzo della CPU è allo 0%. In questo arco di tempo, l'istanza guadagna 144 crediti, che accumula nel suo `CPUCreditBalance`.



Esempio 2: spiegazione dell'uso del credito con T2 Standard

In questo esempio, è possibile vedere in che modo un'istanza `t2.nano` avviata come `standard` guadagna, accumula e spende crediti di lancio e guadagnati. Viene mostrato in che modo il saldo dei crediti riflette non solo i crediti guadagnati accumulati, ma anche i crediti di lancio accumulati.

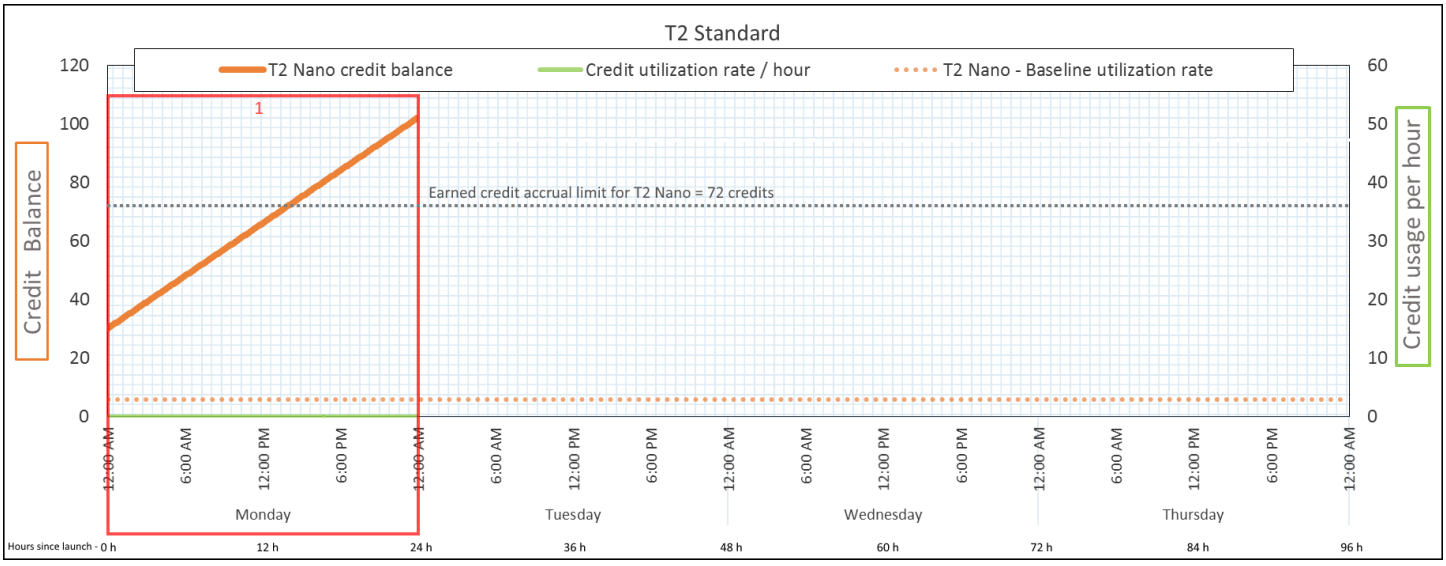
Un'istanza `t2.nano` ottiene 30 crediti di lancio quando viene avviata e guadagna 72 crediti ogni 24 ore. Il suo limite del saldo del credito è di 72 crediti guadagnati; i crediti di lancio non contano per il limite. Una volta che il limite viene raggiunto, i nuovi crediti guadagnati vengono scartati. Per ulteriori informazioni sul numero di crediti che può essere guadagnato e accumulato, consulta la tabella del credito. Per ulteriori informazioni sui limiti, consulta Limiti dei crediti di lancio.

È possibile avviare un'istanza T2 Standard e utilizzarla immediatamente. In alternativa, è possibile avviare un'istanza T2 Standard e lasciarla inattiva per alcuni giorni prima di eseguire applicazioni su di essa. L'utilizzo o l'inattività di un'istanza determina se i crediti vengono spesi o accumulati. Se un'istanza rimane inattiva per 24 ore dal momento in cui viene avviata, il saldo del credito sembra superare il limite poiché il saldo riflette sia i crediti guadagnati accumulati sia i crediti di lancio accumulati. Tuttavia, una volta utilizzata la CPU, i crediti di lancio vengono spesi per primi. Successivamente, il limite riflette sempre il numero massimo di crediti guadagnati che può essere accumulato.

Questo esempio descrive un'istanza che rimane inattiva per 24 ore dal momento in cui viene avviata e illustra sette periodi di tempo per 96 ore, mostrando la frequenza a cui i crediti vengono guadagnati, accumulati, spesi e scartati e il valore del saldo del credito alla fine di ciascun periodo.

Periodo 1: 1 – 24 ore

All'ora 0 sul grafico, l'istanza T2 viene avviata come `standard` e ottiene immediatamente 30 crediti di lancio. Guadagna crediti mentre è in fase di esecuzione. L'istanza rimane inattiva dal momento in cui viene avviata —(l'utilizzo della CPU è pari allo 0%)— e non vengono spesi crediti. Tutti i crediti non spesi vengono accumulati nel saldo del credito. A circa 14 ore dopo l'avvio, il saldo del credito è 72 (30 crediti di lancio + 42 crediti guadagnati), che equivale a ciò che l'istanza può guadagnare in 24 ore. A 24 ore dopo il lancio, il saldo del credito supera 72 crediti perché i crediti di lancio non spesi vengono accumulati nel— saldo del credito e il saldo del credito è 102 crediti: 30 crediti di lancio + 72 crediti guadagnati.



Tasso di spesa di crediti	0 crediti in 24 ore (0% di utilizzo della CPU)

Tasso di guadagno di crediti	72 crediti in 24 ore
Tasso di scarto di crediti	0 crediti in 24 ore
Saldo del credito	102 crediti (30 crediti di lancio + 72 crediti guadagnati)

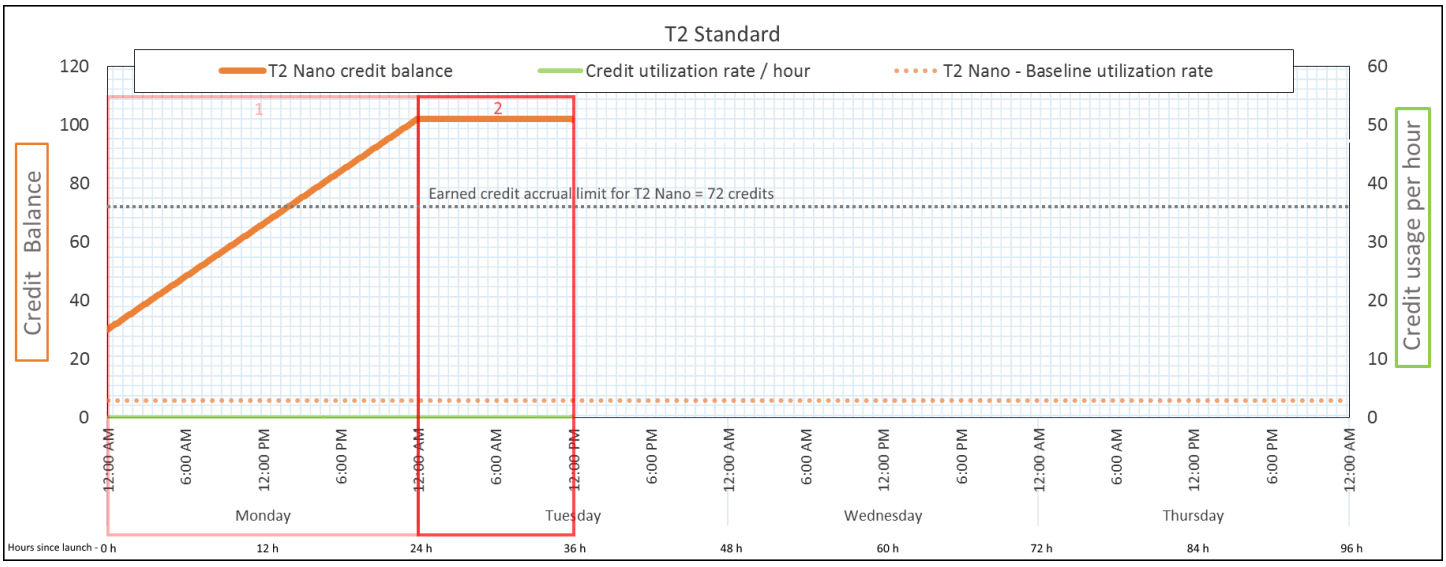
Conclusioni

Se dopo l'avvio non viene utilizzata CPU, l'istanza accumula più crediti di quanto possa guadagnare in 24 ore (30 crediti di lancio + 72 crediti guadagnati = 102 crediti).

In uno scenario reale, un'istanza EC2 consuma un numero ridotto di crediti durante l'avvio e l'esecuzione, il che impedisce al saldo di raggiungere il valore teorico massimo in questo esempio.

Periodo 2: 25 – 36 ore

Per le successive 12 ore, l'istanza continua a rimanere inattiva e guadagna crediti, ma il saldo del credito non aumenta. Si stabilizza a 102 crediti (30 crediti di lancio + 72 crediti guadagnati). Il saldo del credito ha raggiunto il limite di 72 crediti guadagnati accumulati, pertanto i crediti appena guadagnati vengono scartati.



Tasso di spesa di crediti	0 crediti in 24 ore (0% di utilizzo della CPU)
Tasso di guadagno di crediti	72 crediti in 24 ore (3 crediti all'ora)

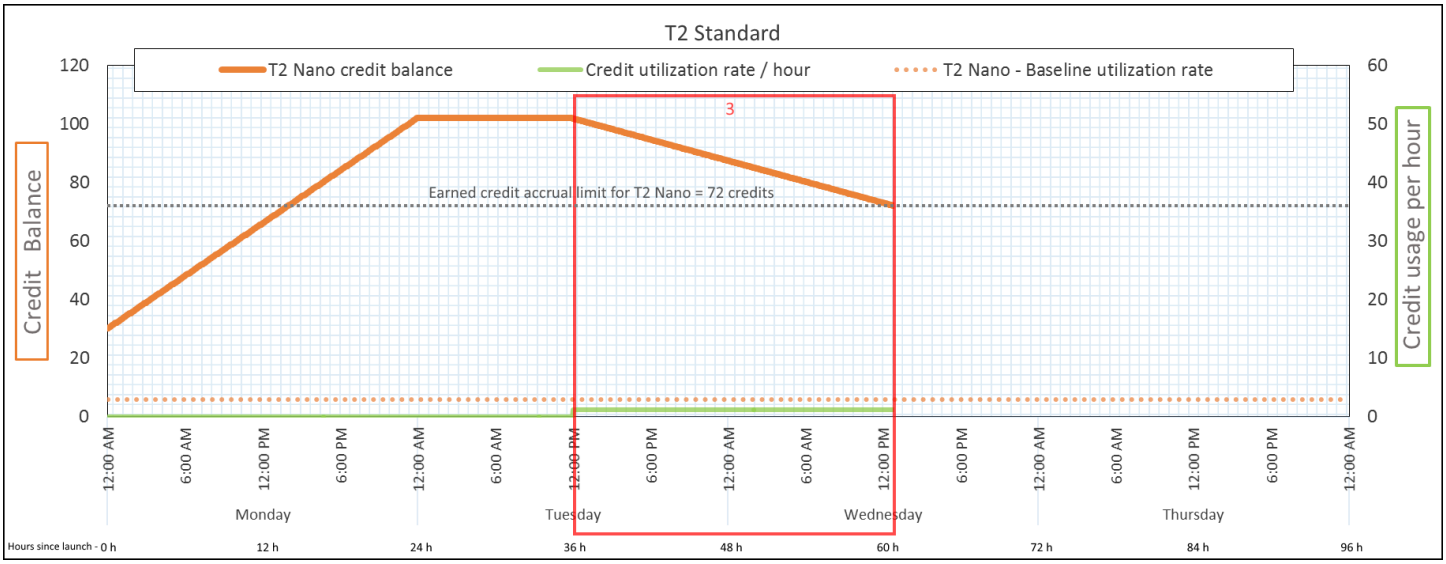
Tasso di scarto di crediti	72 crediti in 24 ore (100% del tasso di guadagno di crediti)
Saldo del credito	102 crediti (30 crediti di lancio + 72 crediti guadagnati),— il saldo è invariato

Conclusioni

Un'istanza guadagna costantemente crediti, ma non può accumulare ulteriori crediti guadagnati se il saldo del credito ha raggiunto il suo limite. Una volta che il limite viene raggiunto, i nuovi crediti guadagnati vengono scartati. I crediti di lancio non contano per il limite del saldo del credito. Se il saldo include crediti di lancio accumulati, il saldo sembra superare il limite.

Periodo 3: 37 – 61 ore

Per le successive 25 ore, l'istanza utilizza il 2% di CPU, cosa che richiede 30 crediti. Nello stesso periodo, guadagna 75 crediti, ma il saldo del credito diminuisce. Il saldo diminuisce perché i crediti di lancio accumulati vengono spesi per primi, mentre i crediti appena guadagnati vengono scartati perché il saldo del credito è già al limite di 72 crediti guadagnati.



Tasso di spesa di crediti	28,8 crediti in 24 ore (1,2 crediti all'ora, 2% di utilizzo della CPU, 40% del tasso di guadagno di crediti) e 30 crediti— in 25 ore
Tasso di guadagno di crediti	72 crediti in 24 ore

Tasso di scarto di crediti	72 crediti in 24 ore (100% del tasso di guadagno di crediti)
Saldo del credito	72 crediti (30 crediti di lancio sono stati spesi, 72 crediti guadagnati rimangono non spesi)

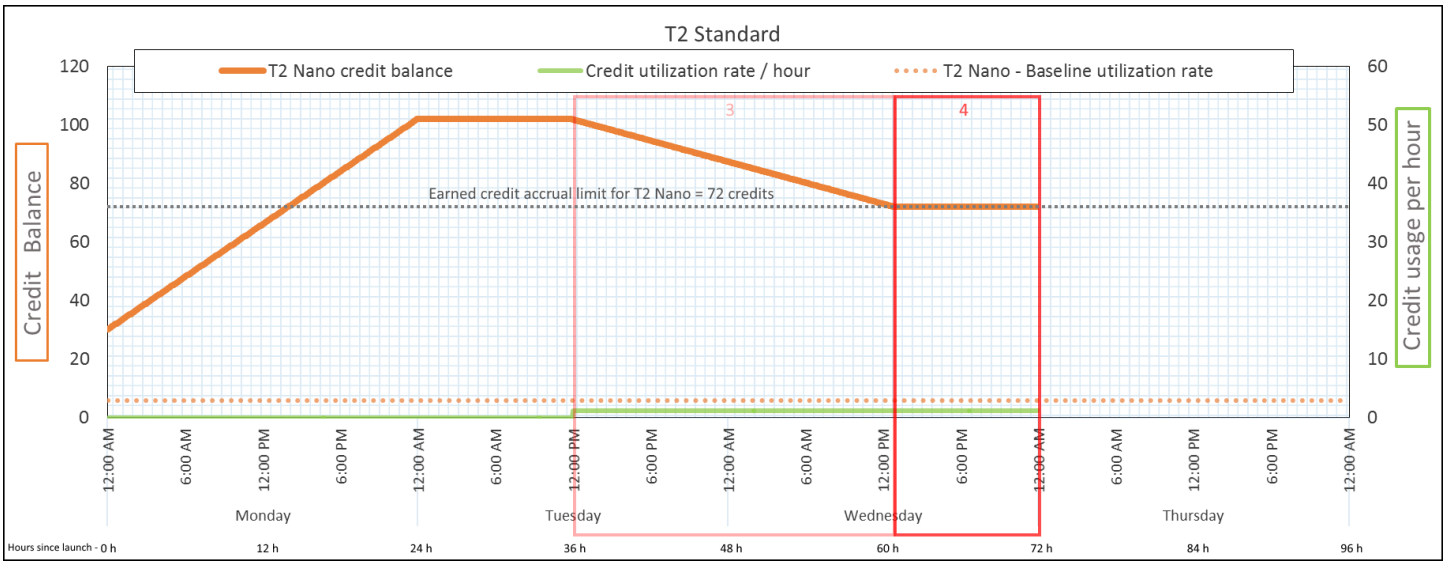
Conclusioni

Un'istanza spende per primi i crediti di lancio, prima dei crediti guadagnati. I crediti di lancio non contano per il limite del credito. Dopo l'avvio, i crediti vengono spesi, il saldo non può mai superare il numero di crediti che si può guadagnare in 24 ore. Inoltre, mentre un'istanza è in esecuzione, non è possibile ottenere più crediti di lancio.

Periodo 4: 62 – 72 ore

Per le successive 11 ore, l'istanza utilizza il 2% di CPU, cosa che richiede 13,2 crediti. Questo è lo stesso utilizzo della CPU del periodo precedente, ma il saldo non diminuisce. Rimane a 72 crediti.

Il saldo non diminuisce perché il tasso di guadagno di crediti è superiore al tasso di spesa di crediti. Nel periodo in cui l'istanza spende 13,2 crediti, guadagna anche 33 crediti. Tuttavia, il limite del saldo è 72 crediti, quindi tutti i crediti guadagnati che superano il limite vengono scartati. Il saldo si stabilizza a 72 crediti, non a 102 crediti durante il periodo 2, perché non sono presenti crediti di lancio accumulati.



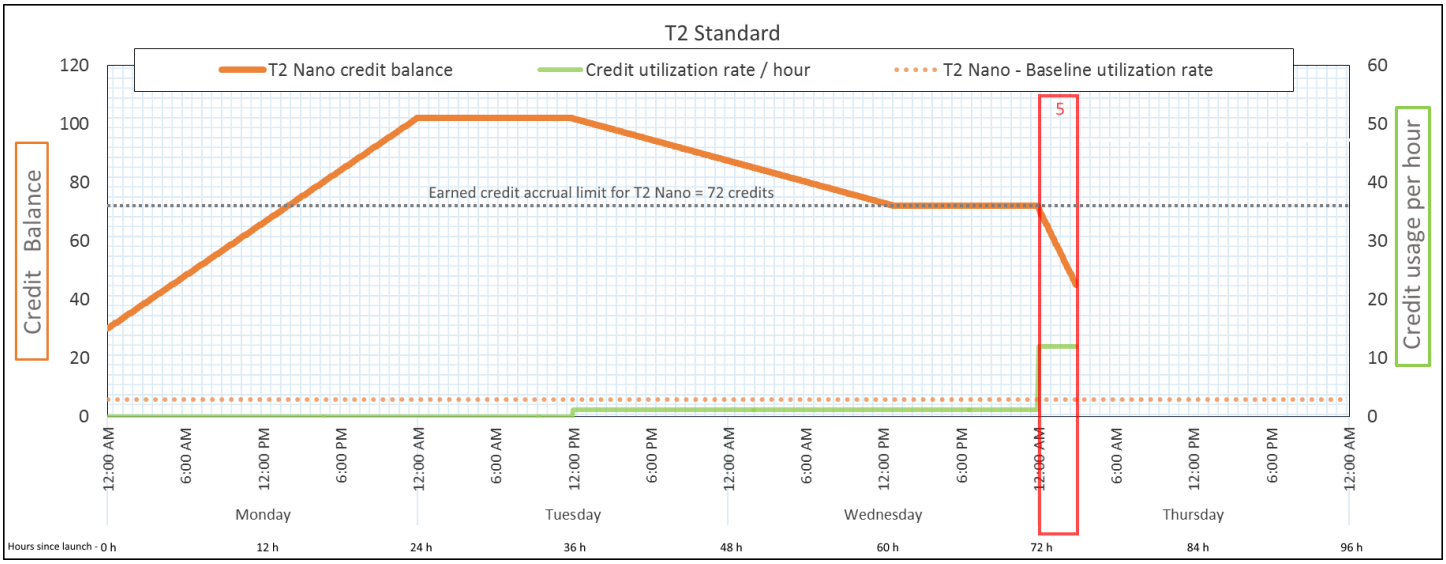
Tasso di spesa di crediti	28,8 crediti in 24 ore (1,2 crediti all'ora, 2% di utilizzo della CPU, 40% del tasso di guadagno di crediti) e 13.2— crediti in 11 ore
Tasso di guadagno di crediti	72 crediti in 24 ore
Tasso di scarto di crediti	43,2 crediti in 24 ore (60% del tasso di guadagno di crediti)
Saldo del credito	72 crediti (0 crediti di lancio + 72 crediti guadagnati), —il saldo è al limite

Conclusioni

Quando i crediti di lancio sono stati spesi, il limite del saldo del credito viene determinato dal numero di crediti che un'istanza può guadagnare in 24 ore. Se l'istanza guadagna più crediti di quelli che spende, i crediti appena guadagnati oltre il limite vengono scartati.

Periodo 5: 73 – 75 ore

Per le successive 3 ore, l'istanza è caratterizzata da picchi al 20% di utilizzo della CPU, cosa che richiede 36 crediti. L'istanza guadagna nove crediti nelle stesse tre ore, il che si traduce in una diminuzione del saldo netto di 27 crediti. Al termine delle tre ore, il saldo del credito è di 45 crediti guadagnati.



Tasso di spesa di crediti	288 crediti in 24 ore (12 crediti all'ora, 20% di utilizzo della CPU, 400% del— tasso di guadagno di crediti) e 36 crediti in 3 ore
Tasso di guadagno di crediti	72 crediti in 24 ore (9 crediti in 3 ore)
Tasso di scarto di crediti	0 crediti in 24 ore
Saldo del credito	45 crediti (saldo precedente [72] – crediti spesi [36] + crediti guadagnati [9]); il saldo diminuisc e a un tasso— di 216 crediti in 24 ore (tasso di spesa 288/24 + tasso di guadagno 72/24 = tasso di diminuzione del saldo 216/24)

Conclusioni

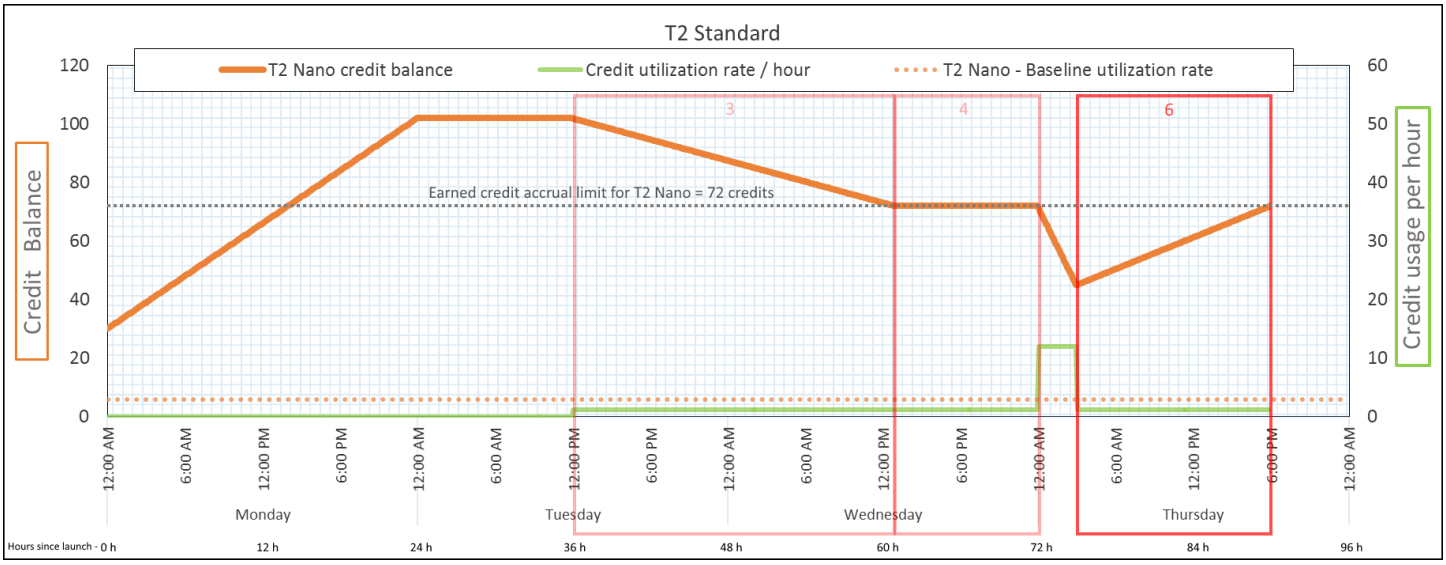
Se un'istanza spende più crediti di quanti ne guadagna, il suo saldo del credito diminuisce.

Periodo 6: 76 – 90 ore

Per le successive 15 ore, l'istanza utilizza il 2% di CPU, cosa che richiede 18 crediti. Questo è lo stesso utilizzo della CPU nei periodi 3 e 4. Tuttavia, il saldo aumenta in questo periodo, mentre è diminuito nel periodo 3 e si è stabilizzato nel periodo 4.

Nel periodo 3, i crediti di lancio accumulati sono stati spesi, mentre i crediti guadagnati che superano il limite del credito vengono scartati, causando una diminuzione del saldo del credito. Nel periodo 4, l'istanza ha speso meno crediti rispetto a quelli guadagnati. Inoltre, i crediti guadagnati che superavano il limite del credito sono stati scartati, quindi il saldo si è stabilizzato al massimo di 72 crediti.

In questo periodo, non sono presenti crediti di lancio accumulati e il numero di crediti guadagnati accumulati nel saldo è inferiore al limite. Nessun credito guadagnato viene scartato. Inoltre, l'istanza guadagna più crediti di quanti ne spende, causando un aumento del credito del saldo.



Tasso di spesa di crediti	28,8 crediti in 24 ore (1,2 crediti all'ora, 2% di utilizzo della CPU, 40% del tasso di guadagno di crediti) e 18 crediti —in 15 ore
Tasso di guadagno di crediti	72 crediti in 24 ore (45 crediti in 15 ore)
Tasso di scarto di crediti	0 crediti in 24 ore
Saldo del credito	72 crediti (il saldo aumenta a un tasso di 43,2 crediti ogni 24 ore; il— tasso di cambio = tasso di spesa 28,8/24 + tasso di guadagno 72/24)

Conclusioni

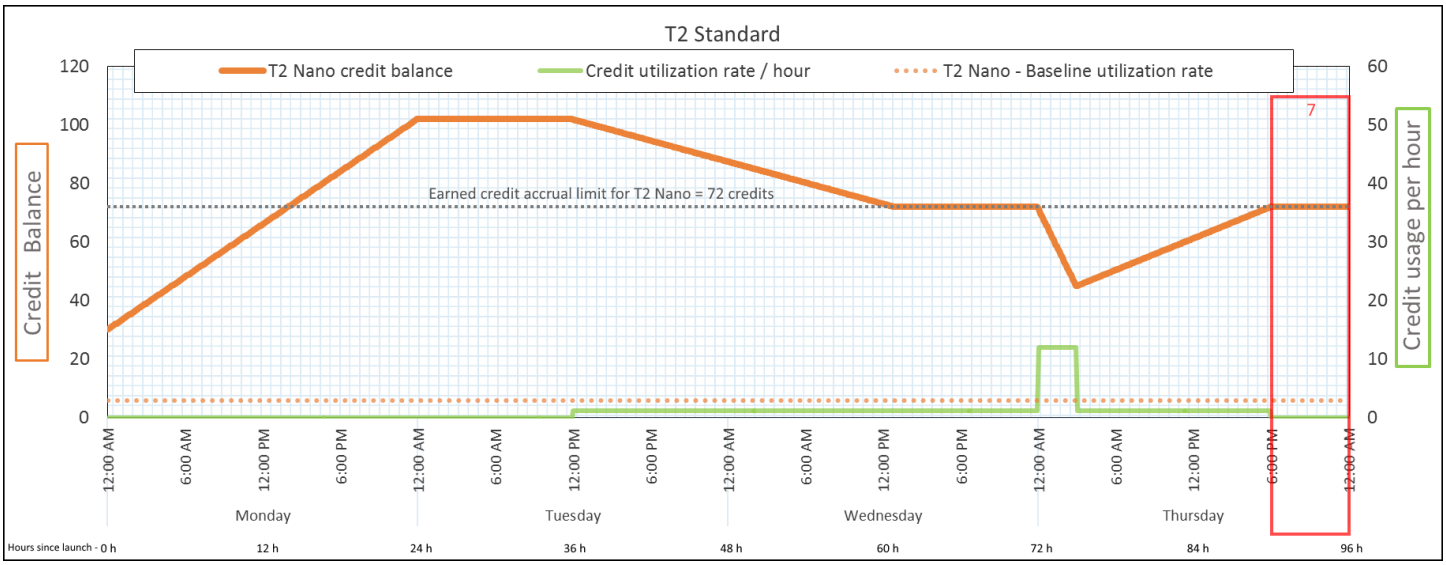
Se un'istanza spende meno crediti di quanti ne guadagna, il suo saldo del credito aumenta.

Periodo 7: 91 – 96 ore

Per le successive sei ore, l'istanza rimane— inattiva (l'utilizzo della CPU è pari allo 0%) e non vengono— spesi crediti. Questo è lo stesso utilizzo della CPU del periodo 2, ma il saldo non si stabilizza a 102 crediti, ma a 72 crediti, che è il limite —di saldo del credito per l'istanza.

Nel periodo 2, il saldo del credito includeva 30 crediti di lancio accumulati. I crediti di lancio sono stati spesi nel periodo 3. Un'istanza in esecuzione non può ottenere più crediti di lancio. Una volta

raggiunto il limite del saldo del credito, tutti i crediti guadagnati che superano il limite vengono scartati.



Tasso di spesa di crediti	0 crediti in 24 ore (0% di utilizzo della CPU)
Tasso di guadagno di crediti	72 crediti in 24 ore
Tasso di scarto di crediti	72 crediti in 24 ore (100% del tasso di guadagno di crediti)
Saldo del credito	72 crediti (0 crediti di lancio, 72 crediti guadagnati)

Conclusioni

Un'istanza guadagna costantemente crediti, ma non può accumulare ulteriori crediti guadagnati se è stato raggiunto il limite del saldo del credito. Una volta che il limite viene raggiunto, i nuovi crediti guadagnati vengono scartati. Il limite del saldo del credito è determinato dal numero di crediti che un'istanza può guadagnare in 24 ore. Per ulteriori informazioni sui limiti del saldo del credito, consulta la tabella del credito.

Utilizzo di istanze a prestazioni espandibili

I passaggi per l'avvio, il monitoraggio e la modifica delle istanze burstable con prestazioni (istanze T) sono simili. La differenza principale è la specifica crediti predefinita all'avvio delle istanze.

Ogni famiglia di istanze T viene fornita con le seguenti specifiche di credito predefinite:

- Le istanze T4g, T3a e T3 vengono avviate come `unlimited`
- Le istanze T3 su un host dedicato possono essere avviate come `standard`
- Le istanze T2 vengono avviate come `standard`

È possibile modificare la specifica crediti predefinita per l'account.

Indice

Avvio di un'istanza a prestazioni espandibili in modalità Standard o illimitata

Puoi avviare le tue istanze T come `unlimited` o `standard` utilizzando la console Amazon EC2, AWS un SDK, uno strumento da riga di comando o con un gruppo di Auto Scaling.

Le seguenti procedure descrivono come utilizzare la console EC2 o il. AWS CLI Per informazioni sull'utilizzo di un gruppo Auto Scaling, vedere. Utilizzo di un gruppo Auto Scaling per avviare un'istanza a prestazioni espandibili in modalità illimitata

Console

Per avviare un'istanza T come Unlimited o Standard

1. Segui la procedura per avviare un'istanza.
2. In Instance type (Tipo di istanza), seleziona un tipo di istanza T.
3. Espandi Advanced details (Dettagli avanzati) e in Credit specification (Specifica del credito) seleziona una specifica del credito. Se non si effettua una selezione, viene utilizzata l'impostazione predefinita, che è `standard` per T2 e per T4g, T3a e `unlimited` T3.

4. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

AWS CLI

Per avviare un'istanza T come Unlimited o Standard

Utilizzare il comando run-instances per avviare le istanze. Indicare la specifica crediti utilizzando il parametro `--credit-specification CpuCredits=`. Sono specifiche dei crediti valide `unlimited` e `standard`.

- Per T4g, T3a e T3, se non si include il `--credit-specification` parametro, l'istanza viene avviata come impostazione predefinita. `unlimited`
- Per T2, se non viene incluso il parametro `--credit-specification`, l'istanza viene avviata come `standard` per impostazione predefinita.

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --credit-specification "CpuCredits=unlimited"
```

Utilizzo di un gruppo Auto Scaling per avviare un'istanza a prestazioni espandibili in modalità illimitata

Quando le istanze T vengono avviate o avviate, richiedono crediti CPU per una buona esperienza di avvio. Se viene utilizzato un gruppo Auto Scaling per avviare le istanze, è consigliabile configurare le istanze come `unlimited`. In questo modo, le istanze utilizzeranno i crediti extra quando vengono avviate o riavviate automaticamente dal gruppo Auto Scaling. L'uso di crediti extra previene le limitazioni di prestazioni.

Creazione di un modello di avvio

È necessario utilizzare un modello di avvio per avviare le istanze come `unlimited` in un gruppo Auto Scaling. Una configurazione di lancio non supporta il lancio di istanze come `unlimited`.

> **Note**
>
> La modalità `unlimited` non è supportata per le istanze T3 avviate su un host dedicato.

Console

Per creare un modello di avvio che avvii le istanze come Unlimited

1. Segui la procedura Crea un modello di lancio utilizzando le impostazioni avanzate nella Guida per l'utente di Amazon EC2 Auto Scaling.
2. In Launch template contents (Contenuti modello di avvio), per Instance type (Tipo di istanza), scegliere una dimensione di istanza.
3. Per avviare le istanze come `unlimited` in un gruppo Auto Scaling, in Advanced details (Dettagli avanzati), per Credit specification (Specifica credito), scegliere Unlimited (Illimitato).
4. Una volta definiti i parametri del modello di avvio, scegliere Create launch template (Crea modello di avvio).

AWS CLI

Per creare un modello di avvio che avvii le istanze come Unlimited

Usa il create-launch-templatecomando e specifica `unlimited` come specifica del credito.

- Per T4g, T3a e T3, se non si include il `CreditSpecification={CpuCredits=unlimited}` valore, l'istanza viene avviata come impostazione predefinita. `unlimited`
- Per T2, se non viene incluso il valore `CreditSpecification={CpuCredits=unlimited}`, l'istanza viene avviata come `standard` per impostazione predefinita.

```
aws ec2 create-launch-template \
    --launch-template-name MyLaunchTemplate \
    --version-description FirstVersion \
    --launch-template-data
 ImageId=ami-8c1be5f6,InstanceType=t3.medium,CreditSpecification={CpuCredits=unlimited}
```

Associazione di un gruppo Auto Scaling a un modello di avvio

Per associare il modello di avvio a un gruppo Auto Scaling occorre creare il gruppo Auto Scaling utilizzando il modello di avvio o aggiungere il modello di avvio a un gruppo Auto Scaling esistente.

Console

Come creare un gruppo con scalabilità automatica utilizzando un modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Sulla barra di navigazione nella parte superiore della schermata, selezionare la stessa regione utilizzata durante la creazione del modello di avvio.
3. Nel riquadro di navigazione, selezionare Groups (Gruppi Auto Scaling), Create group (Crea gruppo Auto Scaling).
4. Scegliere Launch Template (Modello di lancio), selezionare il modello di avvio, quindi scegliere Next Step (Fase successiva).
5. Compilare i campi per il gruppo Auto Scaling. Dopo aver esaminato le impostazioni di configurazione in Review page (Pagina di revisione), scegliere Create Auto Scaling group (Crea gruppo Auto Scaling). Per ulteriori informazioni, consulta la sezione relativa alla creazione di un gruppo Auto Scaling utilizzando un modello di avvio della Guida per l'utente di Amazon EC2 Auto Scaling.

AWS CLI

Come creare un gruppo con scalabilità automatica utilizzando un modello di avvio

Utilizzate il create-auto-scaling-group AWS CLI comando e specificate il parametro. `--launch-template`

Console

Come aggiungere un modello di avvio a un gruppo con scalabilità automatica esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Sulla barra di navigazione nella parte superiore della schermata, selezionare la stessa regione utilizzata durante la creazione del modello di avvio.
3. Nel riquadro di navigazione, selezionare Groups (Gruppi Auto Scaling).

4. Nell'elenco dei gruppi Auto Scaling, selezionare un gruppo Auto Scaling e scegliere Actions (Operazioni), Edit (Modifica).
5. Nella scheda Details (Dettagli), per Launch Template (Modello di lancio), scegliere un modello di avvio, quindi scegliere Save (Salva).

AWS CLI

Come aggiungere un modello di avvio a un gruppo con scalabilità automatica esistente

Utilizzate il update-auto-scaling-group AWS CLI comando e specificate il `--launch-template` parametro.

Visualizzazione della specifica crediti di un'istanza a prestazioni espandibili

È possibile visualizzare la specifica di credito (`unlimitedostandard`) di un'istanza T in esecuzione o interrotta.

Console

Per visualizzare le specifiche di credito di un'istanza T

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Instances (Istanze).
3. Selezionare l'istanza.
4. Scegliere Details (Dettagli) e visualizzare il campo Credit specification (Specifica credito). Il valore è `unlimited` o `standard`.

AWS CLI

Per descrivere la specifica del credito di un'istanza T

Utilizza il comando describe-instance-credit-specifications. Se non vengono specificati uno o più ID istanza, vengono restituite tutte le istanze con specifica crediti `unlimited`, oltre alle istanze configurate in precedenza con specifica crediti `unlimited`. Ad esempio, se un'istanza T3 viene ridimensionata in un'istanza M4 mentre è configurata come `unlimited`, Amazon EC2 restituisce l'istanza M4.

```
aws ec2 describe-instance-credit-specifications --instance-id i-1234567890abcdef0
```

Output di esempio

```
{
  "InstanceCreditSpecifications": [
    {
        "InstanceId": "i-1234567890abcdef0",
        "CpuCredits": "unlimited"
    }
  ]
}
```

Modifica della specifica crediti di un'istanza a prestazioni espandibili

È possibile cambiare la specifica di credito di un'istanza T in esecuzione o interrotta in qualsiasi momento tra `unlimited` `estandard`.

Tieni presente che in modalità `unlimited`, un'istanza può spendere crediti extra, il che potrebbe comportare un costo aggiuntivo. Per ulteriori informazioni, consulta Possibilità di addebito dei costi per i crediti extra.

Console

Per modificare la specifica del credito di un'istanza T

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Instances (Istanze).
3. Selezionare l'istanza. Per modificare la specifica crediti per diverse istanze contemporaneamente, selezionare tutte le istanze applicabili.
4. Scegliere Actions (Operazioni), Instance settings (Impostazioni istanza), Change credit specification (Modifica specifica credito). Questa opzione è abilitata solo se è stata selezionata un'istanza T.
5. Per modificare la specifica del credito in `unlimited`, selezionare la casella di controllo accanto all'ID istanza. Per modificare la specifica del credito in `standard`, deselezionare la casella di controllo accanto all'ID istanza.

AWS CLI

Per modificare la specifica del credito di un'istanza T

Utilizza il comando modify-instance-credit-specification. Specificare l'istanza e la relativa specifica crediti utilizzando il parametro `--instance-credit-specification`. Sono specifiche dei crediti valide `unlimited` e `standard`.

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

Output di esempio

```
{
  "SuccessfulInstanceCreditSpecifications": [
    {
      "InstanceId": "i- 1234567890abcdef0"
    }
  ],
  "UnsuccessfulInstanceCreditSpecifications": []
}
```

Impostazione della specifica crediti predefinita per l'account

Ogni famiglia di istanze T è dotata di una specifica di credito predefinita. È possibile modificare le specifiche di credito predefinite per ogni famiglia di istanze T a livello di account per AWS regione.

Se utilizzi la procedura guidata di avvio istanze nella console EC2 per avviare le istanze, il valore selezionato per la specifica del credito sostituisce la specifica crediti predefinita a livello di account. Se utilizzi l'opzione AWS CLI per avviare le istanze, tutte le nuove istanze T dell'account vengono avviate utilizzando la specifica di credito predefinita. La specifica crediti per le istanze esistenti in esecuzione o arrestate non è interessata.

Considerazione

La specifica crediti predefinita per una famiglia di istanze può essere modificata solo una volta in un periodo di 5 minuti e fino a quattro volte in un periodo di 24 ore.

Console

Per impostare la specifica crediti predefinita a livello di account per regione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione a sinistra, selezionare EC2 Dashboard (Pannello di controllo EC2).
4. Da Account attributes (Attributi account, scegliere Default credit specification (Specifica credito predefinita).
5. Scegliere Gestisci.
6. Per ogni famiglia di istanze, scegliere Unlimited (Illimitato) o Standard (Standard), quindi scegliere Update (Aggiorna).

AWS CLI

Per impostare la specifica crediti predefinita a livello di account (AWS CLI)

Utilizza il comando modify-default-credit-specification. Specifica la regione AWS , la famiglia di istanze e la specifica crediti di default utilizzando il parametro `--cpu-credits`. Le specifiche crediti predefinite valide sono `unlimited` e `standard`.

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

Visualizzazione della specifica crediti predefinita

È possibile visualizzare le specifiche di credito predefinite di una famiglia di istanze T a livello di account per regione. AWS

Console

Per visualizzare le specifiche di credito predefinite a livello di account

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione a sinistra, selezionare EC2 Dashboard (Pannello di controllo EC2).

4. Da Account attributes (Attributi account, scegliere Default credit specification (Specifica credito predefinita).

AWS CLI

Per visualizzare le specifiche di credito predefinite a livello di account

Utilizza il comando get-default-credit-specification. Specifica la regione AWS e la famiglia di istanze.

```
aws ec2 get-default-credit-specification --region us-east-1 --instance-family t2
```

Monitoraggio dei crediti CPU per istanze espandibili

EC2 invia i parametri ad Amazon. CloudWatch Puoi visualizzare i parametri del credito della CPU nei parametri per istanza di Amazon EC2 della console o utilizzare per elencare CloudWatch AWS CLI i parametri per ogni istanza. Per ulteriori informazioni, consulta Elencare i parametri tramite la console e Elenca le metriche utilizzando il AWS CLI.

Indice

Metriche aggiuntive per istanze con prestazioni espandibili CloudWatch

Le istanze Burstable Performance hanno queste CloudWatch metriche aggiuntive, che vengono aggiornate ogni cinque minuti:

- `CPUCreditUsage` – Il numero di crediti CPU spesi durante il periodo di misurazione.
- `CPUCreditBalance` - Il numero di– crediti CPU accumulati da un'istanza. Questo saldo è esaurito quando la CPU ottimizza le prestazioni e i crediti CPU vengono spesi più rapidamente di quanto guadagnati.
- `CPUSurplusCreditBalance` – Il numero di crediti CPU extra spesi per sostenere l'utilizzo della CPU quando il valore `CPUCreditBalance` è zero.
- `CPUSurplusCreditsCharged` – Il numero di crediti CPU extra che supera il numero massimo di crediti della CPU che un'istanza può guadagnare in un periodo di 24 ore e che può quindi implicare costi aggiuntivi.

Gli ultimi due parametri si applicano solo alle istanze configurate come `unlimited`.

La tabella seguente descrive le CloudWatch metriche per le istanze con prestazioni espandibili. Per ulteriori informazioni, consulta Elenca le CloudWatch metriche disponibili per le tue istanze.

Parametro	Descrizione
`CPUCreditUsage`	Il numero di crediti CPU spesi dall'istanza per l'utilizzo della CPU. Un credito CPU equivale a un vCPU che viene eseguito al 100% dell'utilizzo per un minuto o una combinazione equivalente di vCPU, utilizzo e tempo (per esempio, un vCPU che viene eseguito al 50% dell'utilizzo per due minuti o due vCPU che vengono eseguiti al 25% dell'utilizzo per due minuti). I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti. Se specifichi un periodo superiore a 5 minuti, usa la statistica `Sum` al posto di quella `Average`. Unità: Crediti (vCPU/minuti)
`CPUCreditBalance`	Il numero di crediti CPU ottenuti, che un'istanza ha accumulato o da quando è stata lanciata o avviata. Per le T2 Standard `CPUCreditBalance` include anche il numero di crediti di lancio che sono stati accumulati. I crediti vengono accumulati nel saldo del credito dopo che sono stati ottenuti e rimossi dal saldo del credito una volta spesi. Il saldo del credito ha un limite massimo, determinato dalla dimensione dell'istanza. Una volta che il limite viene raggiunto, tutti i nuovi crediti guadagnati vengono scartati. Per le T2 Standard, i crediti di lancio non contano per il limite. I crediti in `CPUCreditBalance` sono disponibili affinché l'istanza li spenda per andare oltre l'utilizzo di base della CPU. Quando l'istanza è in fase di esecuzione, i crediti in `CPUCreditBalance` non scadono. Quando un'istanza T4g, T3a o T3 si interrompe, il valore persiste per sette giorni. `CPUCreditBalance` Successivamente, tutti i crediti accumulati vengono

Parametro	Descrizione
	persi. Quando un'istanza T2 si arresta, il valore `CPUCredit Balance` non persiste e tutti i crediti accumulati vengono persi. I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti. Unità: Crediti (vCPU/minuti)
`CPUSurplusCreditBa lance`	Il numero di crediti extra spesi da un'istanza `unlimited` quando il rispettivo valore `CPUCreditBalance` è pari a zero. Il valore `CPUSurplusCreditBalance` viene saldato con i crediti CPU ottenuti. Se il numero dei crediti extra va oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore, i crediti extra spesi, eccedenti il limite, incorreranno in costi aggiuntivi. Unità: Crediti (vCPU/minuti)
`CPUSurplusCreditsC harged`	Il numero di crediti extra spesi da un'istanza, che non sono saldati con i crediti CPU ottenuti e che pertanto incorrono in costi aggiuntivi. I crediti extra spesi subiscono costi aggiuntivi quando si verifica uno dei seguenti casi: • I crediti extra spesi vanno oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore. I crediti extra spesi, che eccedono il limite, subiscono costi aggiuntivi alla fine dell'ora; • l'istanza viene arrestata o terminata; • l'istanza passa da `unlimited` a `standard`. Unità: Crediti (vCPU/minuti)

Calcolo dell'utilizzo dei crediti CPU

L'utilizzo del credito CPU delle istanze viene calcolato utilizzando le CloudWatch metriche delle istanze descritte nella tabella precedente.

Amazon EC2 invia i parametri CloudWatch ogni cinque minuti. Un riferimento a un valore precedente di un parametro in qualsiasi momento implica il valore precedente del parametro inviato cinque minuti fa.

Calcolo dell'utilizzo dei crediti CPU per istanze standard

- Il saldo dei crediti della CPU aumenta se l'utilizzo della CPU è inferiore alla baseline, quando i crediti spesi sono meno dei crediti guadagnati nell'intervallo precedente di cinque minuti.
- Il saldo dei crediti della CPU diminuisce se l'utilizzo della CPU è superiore alla baseline, quando i crediti spesi sono più dei crediti guadagnati nell'intervallo precedente di cinque minuti.

La seguente equazione rappresenta matematicamente questa operazione:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

La dimensione dell'istanza determina il numero di crediti che l'istanza può guadagnare all'ora e il numero di crediti guadagnati che può accumulare nel saldo del credito. Per ulteriori informazioni sul numero di crediti guadagnati all'ora e sul limite del saldo del credito per ogni dimensione di istanza, consulta la tabella del credito.

Esempio

In questo esempio viene utilizzata l'istanza `t3.nano`. Per calcolare il valore `CPUCreditBalance` dell'istanza, utilizzare l'equazione precedente come segue:

- `CPUCreditBalance` – L'attuale saldo del credito da calcolare.
- `prior CPUCreditBalance` – Il saldo del credito di cinque minuti fa. In questo esempio, un'istanza ha accumulato due crediti.
- `Credits earned per hour` – Un'istanza `t3.nano` guadagna sei crediti all'ora.
- `5/60`— Rappresenta l'intervallo di cinque minuti tra la pubblicazione delle metriche. CloudWatch Moltiplicare i crediti guadagnati all'ora per 5/60 (cinque minuti) per ottenere il numero di crediti

guadagnati dall'istanza negli ultimi cinque minuti. Un'istanza `t3.nano` guadagna 0,5 crediti ogni cinque minuti.

- `CPUCreditUsage` – Quanti crediti sono stati spesi dall'istanza negli ultimi cinque minuti. In questo esempio, l'istanza ha speso un credito negli ultimi cinque minuti.

Con questi valori, è possibile calcolare il valore `CPUCreditBalance`:

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Calcolo dell'utilizzo dei crediti CPU per istanze in modalità illimitata

Quando un'istanza di prestazioni espandibile deve superare la baseline, spende sempre i crediti accumulati prima di spendere crediti extra. Quando esaurisce il suo saldo di credito CPU accumulato, può spendere i crediti extra per espandere la CPU finché necessario. Quando l'utilizzo della CPU è inferiore alla baseline, i crediti extra vengono sempre pagati prima che l'istanza accumuli crediti guadagnati.

Utilizziamo il termine `Adjusted balance` nelle seguenti equazioni per riflettere l'attività che si verifica in questo intervallo di cinque minuti. Utilizziamo questo valore per ottenere i valori per le metriche e. `CPUCreditBalance` `CPUSurplusCreditBalance` CloudWatch

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

Un valore di `0` per `Adjusted balance` indica che l'istanza ha speso tutti i suoi crediti guadagnati per l'ottimizzazione e non sono stati spesi crediti extra. Di conseguenza, sia `CPUCreditBalance` sia `CPUSurplusCreditBalance` sono impostati su `0`.

Un valore `Adjusted balance` positivo indica che i crediti guadagnati accumulati dall'istanza e i precedenti crediti extra, se presenti, sono stati pagati. Di conseguenza, il valore `Adjusted balance` è assegnato a `CPUCreditBalance` e il `CPUSurplusCreditBalance` è impostato su `0`. Le dimensioni dell'istanza determinano il numero massimo di crediti che può accumulare.

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
```

```
CPUSurplusCreditBalance = 0
```

Un valore `Adjusted balance` negativo indica che l'istanza ha speso tutti i suoi crediti guadagnati che ha accumulato e, inoltre, ha anche speso crediti extra per l'ottimizzazione. Di conseguenza, il valore `Adjusted balance` viene assegnato a `CPUSurplusCreditBalance` e `CPUCreditBalance` è impostato su `0`. Anche in questo caso, le dimensioni dell'istanza determinano il numero massimo di crediti che può accumulare.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]
CPUCreditBalance = 0
```

Se i crediti extra spesi superano il numero massimo di crediti che un'istanza può accumulare, il saldo del credito extra è impostato al massimo, come mostrato nell'equazione precedente. I restanti crediti extra sono addebitati come rappresentato dal parametro `CPUSurplusCreditsCharged`.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Infine, quando l'istanza termina, vengono addebitati eventuali crediti extra monitorati dal `CPUSurplusCreditBalance`. Se l'istanza passa da `unlimited` a `standard`, viene addebitato anche qualsiasi `CPUSurplusCreditBalance` restante.

Accelerazione delle prestazioni con istanze GPU

Le istanze basate su GPU forniscono l'accesso alle GPU NVIDIA con migliaia di componenti di calcolo. Puoi utilizzare queste istanze per accelerare le applicazioni scientifiche, tecniche e di rendering sfruttando i framework di elaborazione in parallelo CUDA o Open Computing Language (OpenCL). Puoi utilizzarle anche per le applicazioni grafiche, inclusi i giochi e le applicazioni 3D in streaming e altri carichi di lavoro grafici.

Prima di poter attivare o ottimizzare un'istanza basata su GPU, devi installare i driver appropriati, come segue:

- Per installare i driver NVIDIA su un'istanza con una GPU NVIDIA collegata, ad esempio un'istanza P3 o G4dn, consulta. Installare i driver NVIDIA

- Per installare i driver AMD su un'istanza con una GPU AMD collegata, ad esempio un'istanza G4ad, vedi. Installare i driver AMD

Indice

Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze basate su GPU Amazon EC2

Per attivare le applicazioni virtuali GRID su istanze basate su GPU che dispongono di GPU NVIDIA (NVIDIA GRID Virtual Workstation è abilitata per impostazione predefinita), è necessario definire il tipo di prodotto per il driver, come segue.

Attiva le applicazioni virtuali GRID su istanze Linux

1. Creare il file `/etc/nvidia/gridd.conf` a partire dal file modello fornito.

```
[ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
```

2. Aprire il file `/etc/nvidia/gridd.conf` nell'editor di testo preferito.
3. Trova la riga `FeatureType` e impostala uguale a `0`. quindi aggiungere una riga con `IgnoreSP=TRUE`.

```
FeatureType=0 IgnoreSP=TRUE
```

4. Salvare il file e uscire.
5. Riavviare l'istanza per rendere effettiva la nuova configurazione.

```
[ec2-user ~]$ sudo reboot
```

Attiva le applicazioni virtuali GRID sulle istanze Windows

Attiva le applicazioni virtuali GRID sulle istanze Windows

1. Eseguire regedit.exe per aprire l'editor del registro.
2. Accedere a `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global\GridLicensing`.
3. Aprire il menu contestuale (pulsante destro del mouse) nel riquadro a destra e scegliere New (Nuovo), DWORD.
4. Per Nome, immettere FeatureTypee digitare`Enter`.
5. Apri il menu contestuale (fai clic con il pulsante destro del mouse) FeatureTypee scegli Modifica.
6. Per Value data (Dati valore), digitare `0` per le applicazioni NVIDIA GRID Virtual e scegliere OK.
7. Aprire il menu contestuale (pulsante destro del mouse) nel riquadro a destra e scegliere New (Nuovo), DWORD.
8. Per Name (Nome), inserire IgnoreSP e digitare `Enter`.
9. Aprire il menu contestuale (pulsante destro del mouse) su IgnoreSP e scegliere Modify (Modifica).
10. Per Value data (Dati valore), digitare 1 e scegliere OK.
11. Chiudere l'editor del Registro di sistema.

Ottimizza le impostazioni della GPU sulle istanze Amazon EC2

Esistono molte ottimizzazioni delle impostazioni GPU che puoi effettuare per raggiungere le prestazioni ottimali sulle istanze NVIDIA GPU. Con alcuni di questi tipi di istanze, il driver NVIDIA utilizza una funzione autoboost, che varia le velocità di clock della GPU. Disattivando l'autoboost e impostando le velocità di clock delle GPU sulla loro frequenza massima è possibile ottenere prestazioni ottimali costanti delle istanze GPU.

Ottimizza le impostazioni della GPU su Linux

1. Configurare le impostazioni GPU per renderle persistenti. L'esecuzione di questo comando può richiedere diversi minuti.

```
[ec2-user ~]$ sudo nvidia-persistenced
```

2. [Solo istanze G3 e P2] Disattiva la funzionalità di potenziamento automatico per tutte le GPU dell'istanza.

```
[ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
```

3. Impostare tutte le velocità di clock delle GPU sulla frequenza massima. Utilizzare le velocità di clock di memoria e grafica specificate nei comandi seguenti.

   Alcune versioni del driver NVIDIA non supportano l'impostazione della velocità di clock dell'applicazione e visualizzano l'errore `"Setting applications clocks is not supported for GPU..."`, che può essere ignorato.

   - Istanze G3:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
     ```

   - Istanze G4dn:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
     ```

   - Istanze G5:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
     ```

   - Istanze G6 e Gr6:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
     ```

   - Istanze P2:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,875
     ```

   - Istanze P3 e P3dn:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 877,1530
     ```

   - Istanze P4d:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
     ```

   - Istanze P4de:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Istanze P5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Ottimizza le impostazioni della GPU su Windows

1. Apri una PowerShell finestra e vai alla cartella di installazione di NVIDIA.

```
cd "C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\"
```

2. [Solo istanze G3 e P2] Disattiva la funzionalità di potenziamento automatico per tutte le GPU dell'istanza.

```
.\nvidia-smi --auto-boost-default=0
```

3. Impostare tutte le velocità di clock delle GPU sulla frequenza massima. Utilizzare le velocità di clock di memoria e grafica specificate nei comandi seguenti.

   Alcune versioni del driver NVIDIA non supportano l'impostazione della velocità di clock dell'applicazione e visualizzano l'errore `"Setting applications clocks is not supported for GPU..."`, che può essere ignorato.

   - Istanze G3:

```
.\nvidia-smi -ac "2505,1177"
```

   - Istanze G4dn:

```
.\nvidia-smi -ac "5001,1590"
```

   - Istanze G5:

```
.\nvidia-smi -ac "6250,1710"
```

   - Istanze G6 e Gr6:

```
.\nvidia-smi -ac "6251,2040"
```

- Istanze P2:

```
.\nvidia-smi -ac "2505,875"
```

- Istanze P3 e P3dn:

```
.\nvidia-smi -ac "877,1530"
```

- Istanze P4d:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- Istanze P4de:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Istanze P5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Configura due display 4K su istanze G4ad Linux

Avvio di un'istanza G4ad

1. Collegati alla tua istanza di Linux per ottenere l'indirizzo del bus PCI della GPU da come destinazione per il doppio 4K (2×4k):

   ```
   lspci -vv | grep -i amd
   ```

   Otterrai un output simile al seguente:

   ```
   00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
    c3)
   Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
   ```

2. Tieni presente che l'indirizzo del bus PCI nell'output precedente è 00:1e.0. Crea un file denominato `/etc/modprobe.d/amdgpu.conf` e aggiungi:

```
options amdgpu virtual_display=0000:00:1e.0,2
```

3. Per installare i driver AMD su Linux, vediInstalla i driver AMD sulla tua istanza Amazon EC2. Se hai già installato il driver AMD della GPU, occorrerà rigenerare i moduli del kernel amdgpu tramite dkms.
4. Utilizza il file xorg.conf seguente per definire la topologia dello schermo doppio (2×4K) e salva il file in `/etc/X11/xorg.conf`:

```
~$ cat /etc/X11/xorg.conf
Section "ServerLayout"
    Identifier     "Layout0"
    Screen          0 "Screen0"
    Screen        1 "Screen1"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
    Option          "Xinerama" "1"
EndSection
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection

Section "Monitor"
```

```
    Identifier     "Virtual"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

```
Section "Screen"
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

5. Configura DCV seguendo le istruzioni nella configurazione di un desktop interattivo.
6. Una volta completata la configurazione di DCV, riavvia.
7. Controlla se il driver funziona:

```
 dmesg | grep amdgpu
```

   La risposta dovrebbe essere simile alla seguente:

```
Initialized amdgpu
```

8. Dovresti vedere nell'output per`DISPLAY=:0 xrandr -q`a cui sono collegati 2 display virtuali:

```
~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
 0mm x 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
```

```
   1280x800 59.96
   1280x720 59.97
   1152x768 59.95
   1024x768 60.00 59.95
   800x600  60.32 59.96 56.25
   848x480  60.00 59.94
   720x480  59.94
   640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
   0mm
   4096x3112  60.00
   3656x2664  59.99
   4096x2160  60.00
   3840x2160  60.00
   1920x1200  59.95
   1920x1080  60.00
   1600x1200  59.95
   1680x1050  60.00
   1400x1050  60.00
   1280x1024  59.95
   1440x900 59.99
   1280x960 59.99
   1280x854 59.95
   1280x800 59.96
   1280x720 59.97
   1152x768 59.95
   1024x768 60.00 59.95
   800x600  60.32 59.96 56.25
   848x480  60.00 59.94
   720x480  59.94
  640x480  59.94 59.94
```

9. Quando ti colleghi in DCV, modifica la risoluzione su 2×4K, confermando che il supporto per due monitor è registrato da DCV.

Inizia a usare le istanze P5 per Linux

Le istanze P5 forniscono 8 GPU NVIDIA H100 con 640 GB di memoria GPU a larghezza di banda elevata. Sono dotati di processori AMD EPYC di terza generazione e forniscono 2 TB di memoria di

sistema, 30 TB di archiviazione locale su istanze NVMe, larghezza di banda della rete aggregata di 3.200 Gbps e supporto GPUDirect RDMA. Le istanze P5 supportano anche la tecnologia Amazon UltraCluster EC2, che offre una latenza inferiore e prestazioni di rete migliorate utilizzando EFA.

La tabella seguente fornisce un riepilogo delle specifiche di `p5.48xlarge`.

vCPU	Memoria di sistema	GPU	Memo GPU	Larghezza di banda di rete	GPUDirect RDMA	Peer-to-peer GPU	Archiviazione dell'istanza
192	2 TiB	8 GPU NVIDIA H100	HBM3 da 640 GB	3200 Gbps con EFAv2	Supportato	NVSw 900 Gb/s	8 volumi SSD NVMe da 3.800 GB ciascuno

Configurazione software

Il modo più semplice per iniziare a utilizzare le istanze P5 consiste nell'avviare un'istanza tramite un' AWS Deep Learning AMI preconfigurata con tutto il software richiesto. Per le ultime novità AWS Deep Learning AMI da utilizzare con le istanze P5, consulta l'AMI GPU AWS Deep Learning Base (Ubuntu 20.04).

Se devi creare un'AMI personalizzata da utilizzare con le istanze P5, consigliamo di installare le seguenti versioni software minime:

- Driver NVIDIA 535.54.03 o versione successiva
- CUDA 12.1 o versione successiva
- NVIDIA GDRCopy 2.3 o versione successiva
- Programma di installazione EFA 1.24.1 o versione successiva
- NCCL 2.18.3 o versione successiva
- aws-ofi-nccl plugin 1.7.2-aws o successivo

Inoltre, consigliamo di configurare l'istanza in modo che non utilizzi stati C più profondi. Per ulteriori informazioni, consulta Prestazioni elevate e bassa latenza limitando gli stati C più profondi nella

Guida per l'utente di Amazon Linux 2. L'ultima AMI GPU AWS Deep Learning Base è preconfigurata per non utilizzare stati C più profondi.

Suggerimenti specifici per Ubuntu 20.04

I seguenti suggerimenti per Ubuntu 20.04 sono utili per prevenire la denominazione non prevedibile dell'interfaccia all'avvio:

- Assicurati di eseguire `systemd 245.4-4ubuntu3.19` o versioni successive con il comando seguente:

```
systemd --version
```

- Assicurati di aver configurato GRUB:
  - Apri il file di configurazione `/etc/default/grub` in un editor di testo.
  - Modifica la voce `GRUB_CMDLINE_LINUX_DEFAULT` affinché includa `net.naming-scheme=v247`.
  - Riavvia l'istanza eseguendo `sudo update-grub`.

Configurazione di rete ed EFA

Le istanze P5 forniscono 3.200 Gbps di larghezza di banda della rete utilizzando più interfacce EFA. Le istanze P5 supportano 32 schede di rete. Consigliamo di definire una singola interfaccia di rete EFA per scheda di rete. Per configurare queste interfacce all'avvio, consigliamo le seguenti impostazioni:

- Per l'interfaccia di rete `0`, specifica l'indice del dispositivo `0`
- Per le interfacce di rete `1` attraverso `31`, specifica l'indice del dispositivo `1`

Per ulteriori informazioni su come configurare le istanze P5 per EFA, consulta Inizia a utilizzare le istanze P5 ed EFA.

Istanze Amazon EC2 Mac

Le istanze Mac di EC2 sono ideali per sviluppare, creare, testare e firmare applicazioni per piattaforme Apple, come iPhone, iPad, Mac, Vision Pro, Apple Watch, Apple TV e Safari. Puoi connetterti all'istanza del Mac utilizzando SSH o Apple Remote Desktop (ARD).

> **Note**
>
> L'unità di fatturazione è l'host dedicato. Le istanze in esecuzione su tale host non hanno alcun costo aggiuntivo.

Le istanze Mac Amazon EC2 supportano in modo nativo il sistema operativo macOS.

- Le istanze EC2 Mac x86 (`mac1.metal`) si basano su hardware Mac mini 2018 con processori Intel Core i7 di ottava generazione (Coffee Lake) a 3,2 GHz.
- Le istanze Mac M1 di EC2 (`mac2.metal`) si basano su hardware Mac mini 2020 con processori Apple M1.
- Le istanze Mac EC2 M1 Ultra (`mac2-m1ultra.metal`) sono costruite su hardware Mac Studio 2022 alimentato da processori Apple M1 Ultra in silicio.
- Le istanze Mac M2 di EC2 (`mac2-m2.metal`) si basano su hardware Mac mini 2023 con processori Apple M2.
- Le istanze Mac M2 Pro di EC2 (`mac2-m2pro.metal`) si basano su hardware Mac mini 2023 con processori Apple M2 Pro.

Indice

- Sottoscrizione alle notifiche delle AMI macOS
- Recupera gli AWS Systems Manager ID AMI macOS utilizzando l'API Parameter Store
- Note di rilascio delle AMI macOS di Amazon EC2

Considerazioni

Le seguenti considerazioni si applicano alle istanze Mac:

- Le istanze Mac sono disponibili solo come istanze bare metal su Host dedicati, con un periodo di allocazione minimo di 24 ore prima di poter rilasciare Host dedicato. È possibile avviare un'istanza Mac per ogni Host dedicato. Puoi condividere l'host dedicato con AWS gli account o le unità organizzative all'interno della tua AWS organizzazione o con l'intera organizzazione. AWS
- Le istanze Mac sono disponibili in diversi Regioni AWS formati. Per un elenco della disponibilità delle istanze Mac in ciascuna di esse Regioni AWS, consulta Tipi di istanze Amazon EC2 per regione.
- Le istanze Mac sono disponibili solo come Istanze on demand. Non sono disponibili come Istanze spot o Istanze riservate. È possibile contenere le spese sulle istanze Mac acquistando un Savings Plan.
- Le istanze Mac possono essere eseguite su uno dei seguenti sistemi operativi:
  - macOS Mojave (versione 10.14) (solo istanze Mac x86)
  - macOS Catalina (versione 10.15) (solo istanze Mac x86)
  - macOS Big Sur (versione 11) (istanze x86 e Mac M1)
  - macOS Monterey (versione 12) (istanze x86 e Mac M1)
  - macOS Ventura (versione 13) (tutte le istanze Mac, le istanze Mac M2 e M2 Pro supportano macOS Ventura versione 13.2 o successiva)
  - macOS Sonoma (versione 14) (tutte le istanze Mac)
- EBSè supportato l'hotplug.
- AWS non gestisce o supporta l'SSD interno dell'hardware Apple. Ti consigliamo vivamente di utilizzare invece i volumi Amazon EBS. EBSi volumi offrono gli stessi vantaggi in termini di elasticità, disponibilità e durabilità sulle istanze Mac come su qualsiasi altra istanza EC2.
- Per prestazioni ottimali, consigliamo di utilizzare SSD General Purpose (`gp2`and`gp3`) e Provisioned IOPS SSD (`io1`e`io2`) con istanze Mac. EBS
- Le istanze Mac ora supportano Dimensionamento automatico Amazon EC2.

- Su istanze Mac x86, gli aggiornamenti automatici del software sono disabilitati. Consigliamo di applicare gli aggiornamenti e di testarli sull'istanza prima di mettere l'istanza in produzione. Per ulteriori informazioni, consulta Aggiorna il sistema operativo e il software sulle istanze Mac.
- Quando arresti o termini un'istanza Mac, viene eseguito un flusso di lavoro di scrubbing su Host dedicato. Per ulteriori informazioni, consulta Interrompi o termina la tua istanza Amazon EC2 per Mac.

> **Warning**
>
> FileVaultNon utilizzare. L'attivazione FileVault comporterà il mancato avvio dell'host a causa del blocco delle partizioni. Se è necessaria la crittografia dei dati, utilizza la crittografia Amazon EBS per evitare problemi di avvio e impatto sulle prestazioni. Con la crittografia Amazon EBS, le operazioni di crittografia avvengono sui server che ospitano le istanze, garantendo la sicurezza di entrambe data-at-rest e data-in-transit tra un'istanza e lo storage EBS collegato. Per ulteriori informazioni, consulta la crittografia di Amazon EBS nella Guida per l'utente di Amazon EBS

Preparazione dell'istanza

Dopo avere avviato un'istanza Mac, dovrai attendere che l'istanza sia pronta prima di poterti connettere ad essa. Per un'AMI AWS fornita con un'istanza Mac x86 o un'istanza Mac Apple in silicio, il tempo di avvio può variare da circa 6 minuti a 20 minuti. A seconda delle dimensioni del volume Amazon EBS scelto, dell'inclusione di script aggiuntivi nei dati utente o del software aggiuntivo caricato su un'AMI macOS personalizzata, il tempo di avvio potrebbe aumentare.

Puoi usare un piccolo script di shell, come quello riportato di seguito, per interrogare l' describe-instance-status API e sapere quando l'istanza è pronta per la connessione. Nel comando seguente, sostituisci il l'ID dell'istanza di esempio con il tuo.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-
ids=i-0123456789example \
    --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

AMI macOS EC2

Amazon EC2 macOS è progettato per fornire un ambiente stabile, sicuro e ad alte prestazioni per i carichi di lavoro degli sviluppatori in esecuzione su istanze Amazon EC2 Mac. Le AMI macOS EC2 includono pacchetti che consentono una facile integrazione AWS con, ad esempio, strumenti di configurazione di avvio e librerie e strumenti AWS popolari.

Per ulteriori informazioni sulle AMI EC2 macOS, consulta. Note di rilascio delle AMI macOS di Amazon EC2

AWS fornisce regolarmente AMI EC2 macOS aggiornate che includono aggiornamenti ai pacchetti di proprietà di AWS e all'ultima versione di macOS completamente testata. Inoltre, AWS fornisce AMI aggiornate con gli ultimi aggiornamenti della versione secondaria o gli aggiornamenti della versione principale non appena questi possono essere completamente testati e controllati. Se non è necessario conservare i dati o le personalizzazioni delle istanze Mac, è possibile ottenere gli aggiornamenti più recenti avviando una nuova istanza utilizzando l'AMI corrente e quindi terminando l'istanza precedente. In caso contrario, è possibile scegliere gli aggiornamenti da applicare alle istanze Mac.

Per informazioni su come iscriversi alle notifiche dell'AMI macOS, consulta. Sottoscrizione alle notifiche delle AMI macOS

EC2 macOS Init

EC2macOS Init viene utilizzato per inizializzare le istanze EC2 Mac all'avvio. Utilizza gruppi di priorità per eseguire gruppi logici di attività contemporaneamente.

Il file launchd plist è `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. I file per EC2 macOS Init si trovano in `/usr/local/aws/ec2-macos-init`.

Per ulteriori informazioni, visitare https://github.com/aws/ec2-macos-init.

Monitor di sistema Amazon EC2 per macOS

Amazon EC2 System Monitor per macOS fornisce parametri di utilizzo della CPU ad Amazon. CloudWatch Invia questi parametri a CloudWatch più di un dispositivo seriale personalizzato in periodi di 1 minuto. È possibile abilitare o disabilitare questo agente come segue. È abilitato per impostazione predefinita.

```
sudo setup-ec2monitoring [enable | disable]
```

> **Note**
>
> Amazon EC2 System Monitor per macOS non è attualmente supportato sulle istanze Mac Apple Silicon.

Risorse correlate

Per informazioni sui prezzi, consulta Prezzi di .

Per ulteriori informazioni sulle istanze Mac, consulta la sezione relativa alle Istanze Amazon EC2 Mac.

Per ulteriori informazioni sulle specifiche hardware e sulle prestazioni di rete delle istanze Mac, consulta Istanze per uso generico.

Avvia un'istanza Mac utilizzando o AWS Management ConsoleAWS CLI

Le istanze Mac EC2 richiedono un host dedicato. Devi prima allocare un host al tuo account e quindi avviare l'istanza sull'host.

Puoi avviare un'istanza Mac utilizzando AWS Management Console o il AWS CLI.

Avviare un'istanza Mac utilizzando la console

Per avviare un'istanza Mac su un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Alloca l'host dedicato, come indicato di seguito:
   a. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
   b. Scegliere Allocate Host dedicato (Alloca host dedicato), quindi effettuare le seguenti operazioni:
      i. Per la famiglia Instance, scegli mac1, mac2, mac2-m2, mac2-m2pro o mac2-m1ultra. Se la famiglia di istanze non appare nell'elenco, non è supportata nella regione selezionata.
      ii. Per il tipo di istanza, scegli mac1.metal, mac2.metal, mac2-m2.metal, mac2-m2pro.metal o mac2-m1ultra.metal in base alla famiglia di istanze scelta.

iii. Per Availability Zone (Zona di disponibilità), scegliere la zona di disponibilità per il Host dedicato.

iv. Per Quantity (Quantità), mantieni il valore 1.

v. Scegli Alloca.

3. Avvia l'istanza sull'host, come indicato di seguito:

a. Selezionare il Host dedicato che è stato creato e quindi effettuare le seguenti operazioni:

i. Scegli Actions (Azioni), Launch instance(s) onto host (Avvia istanze sull'host).

ii. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), seleziona un'AMI macOS.

iii. In Tipo di istanza, selezionate il tipo di istanza appropriato (mac1.metal, mac2.metal, mac2-m2.metal, mac2-m2pro.metal o mac2-m1ultra.metal).

iv. In Advanced details (Dettagli avanzati), verifica che Tenancy, Tenancy host by (Host tenancy di) e Tenancy host ID (ID host tenancy) siano preconfigurati in base all'host dedicato creato. Aggiorna Tenancy affinity (Affinità tenancy) in base alle necessità.

v. Completare la procedura guidata specificando volumi EBS, gruppi di sicurezza e coppie di chiavi in base alle esigenze.

vi. Nel pannello Summary (Riepilogo), scegliere Launch instance (Avvia istanza).

b. Una pagina di conferma indicherà che l'istanza si sta avviando. Scegli View Instances (Visualizza istanze) per chiudere la pagina di conferma e tornare alla console. Lo stato iniziale di un'istanza è `pending`. L'istanza è pronta quando il suo stato cambia in `running` e passa i controlli di stato.

Avvia un'istanza Mac utilizzando AWS CLI

Allocazione dell'host dedicato

Usa il seguente comando allocate-hosts per allocare un host dedicato per la tua istanza Mac, sostituendolo `instance-type` con`mac1.metal`,`mac2.metal`, `mac2-m2.metal` `mac2-m2pro.metal`mac2-m1ultra.metal, o `region` e `availability-zone` con quelli appropriati per il tuo ambiente.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-
zone us-east-1b --auto-placement "on" --quantity 1
```

Avvio dell'istanza sull'host

Usa il seguente comando run-instances per avviare un'istanza Mac, sostituendo nuovamente l'istanza `instance-type` con`mac1.metal`,, `mac2.metal` `mac2-m2.metal` `mac2-m2pro.metal`mac2-m1ultra.metal, o e e con quelle utilizzate in precedenza. `region` `availability-zone`

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement
 Tenancy=host --image-id ami_id --key-name my-key-pair
```

Lo stato iniziale di un'istanza è `pending`. L'istanza è pronta quando il suo stato cambia in `running` e passa i controlli di stato. Utilizzate il describe-instance-statuscomando seguente per visualizzare le informazioni sullo stato dell'istanza.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Di seguito è riportato un esempio di output per un'istanza in esecuzione che ha superato i controlli di stato.

```
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1b",
            "InstanceId": "i-017f8354e2dc69c4f",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "InstanceStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
```

```
                ],
                "Status": "ok"
            }
        }
    ]
}
```

Connect all'istanza Mac tramite SSH o una GUI

Puoi connetterti alla tua istanza Mac utilizzando SSH o un'interfaccia utente grafica (GUI).

Connettersi all'istanza tramite SSH

> **Important**
>
> Più utenti possono accedere al sistema operativo contemporaneamente. In genere esiste una sessione User:GUI 1:1 a causa del servizio Screen Sharing integrato sulla porta 5900. L'utilizzo di SSH all'interno di macOS supporta più sessioni fino al limite "Max Sessions" nel file sshd_config.

Le istanze Amazon EC2 Mac non consentono l'SSH root remoto per impostazione predefinita. L'autenticazione delle password è disabilitata per evitare attacchi di forza bruta alle password. L'account ec2-user è configurato per accedere in remoto utilizzando SSH. Anche l'account ec2-user dispone di privilegi sudo. Dopo aver effettuato la connessione all'istanza, è possibile aggiungere altri utenti.

Per supportare la connessione all'istanza tramite SSH, avviare l'istanza utilizzando una coppia di chiavi e un gruppo di sicurezza che consente l'accesso SSH e assicurarsi che l'istanza disponga di connettività Internet. Fornire il file `.pem` per la coppia di chiavi quando ci si connette all'istanza.

Utilizza la seguente procedura per stabilire una connessione a un'istanza Mac tramite un client SSH. Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risolvi i problemi di connessione alla tua istanza Linux.

Per connettersi all'istanza tramite SSH

1. Verificare che nel computer locale sia installato un client SSH immettendo ssh nella riga di comando. Se il computer non riconosce il comando, cercare un client SSH per il sistema operativo e installarlo.

2. Ottenere il nome DNS pubblico dell'istanza. Utilizzando la console Amazon EC2 è possibile trovare il nome DNS pubblico sia nelle schede Details (Dettagli) che nelle schede Networking (Rete). Utilizzando AWS CLI, puoi trovare il nome DNS pubblico usando il comando describe-instances.
3. Individuare il file `.pem` per la coppia di chiavi specificata al momento dell'avvio dell'istanza.
4. Connettersi all'istanza utilizzando il seguente comando ssh, specificando il nome DNS pubblico dell'istanza e il file `.pem`.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

Connessione all'interfaccia utente grafica (GUI) dell'istanza

Per connettersi all'interfaccia utente grafica dell'istanza utilizzando VNC, Apple Remote Desktop (ARD) o l'applicazione di condivisione schermo di Apple, attenersi alla procedura seguente (inclusa in macOS).

> **Note**
>
> macOS 10.14 e versioni successive permette di controllare solo se la condivisione dello schermo è abilitata tramite le Preferenze di sistema.

Connessione all'istanza tramite client ARD o client VNC

1. Verificare che il computer locale disponga di un client ARD o di un client VNC che supporti ARD installato. Su macOS è possibile sfruttare l'applicazione Condivisione schermo integrata. In caso contrario, cercare un ARD per il sistema operativo e installarlo.
2. Dal computer locale, connettersi all'istanza utilizzando SSH.
3. Impostare una password per l'account ec2-user utilizzando il comando passwd come segue.

```
[ec2-user ~]$ sudo passwd ec2-user
```

4. Installa e avvia macOS Screen Sharing utilizzando il comando seguente.

```
[ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

5. Disconnettiti dall'istanza digitando exit e premendo Invio.
6. Dal computer, connettersi all'istanza utilizzando il seguente comando ssh. Oltre alle opzioni illustrate nella sezione precedente, utilizzare l'opzione -L per abilitare l'inoltro alla porta e inoltrare tutto il traffico sulla porta locale 5900 al server ARD sull'istanza.

```
ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

7. Dal computer locale, utilizza il client ARD o VNC che supporta ARD per connetterti a localhost su `localhost:5900`. Ad esempio, utilizzare l'applicazione Condivisione schermo su macOS come segue:
   a. Apri il Finder e seleziona Vai.
   b. Seleziona Connetti al server.
   c. Nel campo Indirizzo del server, inserisci `vnc://localhost:5900`.
   d. Accedere come richiesto, utilizzando **`ec2-user`** come nome utente e password creati per l'account ec2-user.

Modifica della risoluzione dello schermo macOS sulle istanze Mac

Dopo avere stabilito la connessione all'istanza Mac di EC2 utilizzando ARD o un client VNC che supporta ARD, puoi modificare la risoluzione dello schermo dell'ambiente macOS utilizzando uno qualsiasi degli strumenti o delle utilità macOS disponibili pubblicamente, come displayplacer.

Modifica della risoluzione dello schermo mediante displayplacer

1. Installa displayplacer.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Visualizza le informazioni correnti sullo schermo e le possibili risoluzioni dello schermo.

```
[ec2-user ~]$ displayplacer list
```

3. Applica la risoluzione dello schermo desiderata.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
 degree:0"
```

Per esempio:

```
RES="2560x1600"
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
 origin:(0,0) degree:0"
```

Aggiorna il sistema operativo e il software sulle istanze Mac

Warning

L'installazione delle versioni beta o in anteprima di macOS è disponibile solo sulle istanze Mac Amazon EC2 M1. Amazon EC2 non qualifica le versioni beta o in anteprima di macOS e non garantisce che le istanze rimarranno funzionanti dopo un aggiornamento a una versione macOS di pre-produzione.
Cercare di installare versioni beta o in anteprima di macOS sulle istanze Mac Amazon EC2 x86 comporterà un peggioramento dell'host dedicato Mac EC2 quando arresti o termini l'istanza e ti impedirà di avviare o lanciare una nuova istanza su quell'host.

Passaggi per aggiornare il software su istanze Mac x86 e Mac con processore Apple.

- Aggiornamento del software su istanze Mac x86
- Aggiornamento del software su istanze Mac con processore Apple

Aggiornamento del software su istanze Mac x86

Su istanze Mac x86 puoi installare aggiornamenti del sistema operativo da Apple utilizzando il comando `softwareupdate`.

Per installare aggiornamenti del sistema operativo da Apple su istanze Mac x86

1. Elencare i pacchetti con gli aggiornamenti disponibili utilizzando il seguente comando.

   ```
   [ec2-user ~]$ softwareupdate --list
   ```

2. Installare tutti gli aggiornamenti o solo aggiornamenti specifici. Per installare aggiornamenti specifici, utilizzare il seguente comando.

```
[ec2-user ~]$ sudo softwareupdate --install label
```

Per installare invece tutti gli aggiornamenti, utilizzare il seguente comando.

```
[ec2-user ~]$ sudo softwareupdate --install --all --restart
```

Gli amministratori di sistema possono utilizzarlo AWS Systems Manager per distribuire aggiornamenti del sistema operativo preapprovati su istanze Mac x86. Per ulteriori informazioni, consulta la Guida per l'utente AWS Systems Manager.

Puoi usare Homebrew per installare gli aggiornamenti ai pacchetti nelle AMI EC2 macOS, in modo da avere la versione più recente di questi pacchetti sulle tue istanze. È possibile anche utilizzare Homebrew per installare ed eseguire applicazioni macOS comuni su Amazon EC2 macOS. Per ulteriori informazioni, consulta la documentazione di Homebrew.

Per installare gli aggiornamenti utilizzando Homebrew

1. Aggiornare Homebrew utilizzando il seguente comando.

   ```
   [ec2-user ~]$ brew update
   ```

2. Elencare i pacchetti con gli aggiornamenti disponibili utilizzando il seguente comando.

   ```
   [ec2-user ~]$ brew outdated
   ```

3. Installare tutti gli aggiornamenti o solo aggiornamenti specifici. Per installare aggiornamenti specifici, utilizzare il seguente comando.

   ```
   [ec2-user ~]$ brew upgrade package name
   ```

   Per installare invece tutti gli aggiornamenti, utilizzare il seguente comando.

   ```
   [ec2-user ~]$ brew upgrade
   ```

Aggiornamento del software su istanze Mac con processore Apple

Considerazioni

Driver Adattatore elastico di rete (ENA)

A causa di un aggiornamento nella configurazione del driver di rete, la versione 1.0.2 del driver ENA non è compatibile con macOS 13.3 o versioni successive. Se desideri installare una versione macOS 13.3 o successiva in versione beta, in anteprima o in produzione e non hai installato il driver ENA più recente, utilizza la procedura seguente per installare una nuova versione del driver.

Installazione di una nuova versione del driver ENA

1. In una finestra del terminale, connettiti all'istanza Mac con processore Apple utilizzando SSH.
2. Scarica l'applicazione ENA nel file `Applications` con il seguente comando.

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

> **Suggerimento per la risoluzione dei problemi:**
>
> Se ricevi l'avviso `No available formula with the name amazon-ena-ethernet-dext`, esegui il comando riportato di seguito.
>
> ```
> [ec2-user ~]$ brew update
> ```

3. Disconnettiti dall'istanza digitando exit e premendo Invio.
4. Usa il client VNC per attivare l'applicazione ENA.
   a. Configura il client VNC utilizzando Connessione all'interfaccia utente grafica (GUI) dell'istanza.
   b. Dopo avere effettuato la connessione all'istanza utilizzando l'applicazione Screen Sharing, vai alla cartella Applicazioni e apri l'applicazione ENA.
   c. Scegli Attiva.
   d. Per confermare che il driver sia stato attivato correttamente, esegui il comando riportato di seguito nella finestra del terminale. L'output del comando mostra che il vecchio driver è nello stato di terminazione in corso e il nuovo driver è nello stato attivato.

```
systemextensionsctl list;
```

e. Dopo aver riavviato l'istanza, sarà presente solo il nuovo driver.

Aggiornamento del software su istanze Mac con processore Apple

Sulle istanze Mac con processore Apple, è necessario completare diversi passaggi per eseguire un aggiornamento del sistema operativo in loco. Innanzitutto, accedi al disco interno dell'istanza utilizzando la GUI con un client VNC (Virtual Network Computing). Questa procedura utilizza macOS Screen Sharing, il client VNC integrato. Quindi, delega la proprietà all'utente amministrativo (`ec2-user`) accedendo come `aws-managed-user` nel volume Amazon EBS.

Durante questa procedura si creano due password: una per l'utente amministrativo (`ec2-user`) e l'altra per un utente amministrativo speciale (`aws-managed-user`). Ricorda queste password poiché le utilizzerai durante la procedura.

> **Note**
>
> Su macOS Big Sur, con questa procedura puoi eseguire solo aggiornamenti minori come l'aggiornamento da macOS Big Sur 11.7.3 a macOS Big Sur 11.7.4. Per macOS Monterey o versioni successive, puoi eseguire aggiornamenti software importanti.

Per accedere al disco interno

1. Dal computer locale, nel terminale, connettiti all'istanza Mac con processore Apple tramite SSH con il seguente comando. Per ulteriori informazioni, consulta Connettersi all'istanza tramite SSH.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

2. Installa e avvia macOS Screen Sharing utilizzando il comando seguente.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

3. Imposta una password per `ec2-user` con il comando seguente. Ricorda la password perché la userai in seguito.

```
[ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

4. Disconnettiti dall'istanza digitando exit e premendo INVIO.
5. Dal computer locale, nel Terminale, riconnettiti all'istanza con un tunnel SSH alla porta VNC usando il seguente comando.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-dns-name
```

> **Note**
>
> Non uscire da questa sessione SSH fino a quando non sono stati completati i seguenti passaggi di connessione VNC e GUI. Quando l'istanza viene riavviata, la connessione si chiude automaticamente.

6. Dal computer locale, connettiti a `localhost:5900` seguendo la procedura seguente:
   a. Apri il Finder e seleziona Vai.
   b. Seleziona Connetti al server.
   c. Nel campo Indirizzo del server, inserisci `vnc://localhost:5900`.
7. Nella finestra macOS, connettiti alla sessione remota dell'istanza Mac con processore Apple come `ec2-user`, utilizzando la password creata nel passaggio 3.
8. Accedi al disco interno, denominato InternalDisk, utilizzando una delle seguenti opzioni.
   a. Per macOS Ventura o versioni successive: apri Impostazioni di sistema, seleziona Generale nel riquadro sinistro, quindi Disco di startup nella parte inferiore destra del riquadro.
   b. Per macOS Monterey o versioni precedenti: apri Preferenze di Sistema, seleziona Disco di startup, quindi sblocca il riquadro selezionando l'icona del lucchetto nella parte inferiore sinistra della finestra.

> **Suggerimento per la risoluzione dei problemi:**
>
> Se devi montare il disco interno, esegui il seguente comando nel Terminale.

```
APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep
 "Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;
 diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
```

9. Scegli il disco interno, denominato InternalDisk, e seleziona Riavvia. Seleziona nuovamente Riavvia quando richiesto.

> **Important**
>
> Se il disco interno si chiama Macintosh HD anziché InternalDisk, l'istanza deve essere arrestata e riavviata per poter aggiornare l'host dedicato. Per ulteriori informazioni, consulta Interrompi o termina la tua istanza Amazon EC2 per Mac.

Utilizza la procedura seguente per delegare la proprietà all'utente amministrativo. Quando ti riconnetti all'istanza con SSH, esegui l'avvio dal disco interno utilizzando l'utente amministrativo speciale (`aws-managed-user`). La password iniziale per `aws-managed-user` è vuota, quindi è necessario sovrascriverla alla prima connessione. Ripeti quindi i passaggi per installare e avviare macOS Screen Sharing poiché il volume di avvio è cambiato.

Per delegare la proprietà all'amministratore di un volume Amazon EBS

1. Dal computer locale, nel terminale, connettiti all'istanza Mac con processore Apple con il seguente comando.

```
ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
```

2. Quando visualizzi l'avviso `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, esegui una delle operazioni seguenti per risolvere il problema.

   a. Cancella gli host noti usando il seguente comando. Quindi, ripeti il passaggio precedente.

   ```
   rm ~/.ssh/known_hosts
   ```

   b. Aggiungi la stringa seguente al comando SSH del passaggio precedente.

   ```
   -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
   ```

3. Imposta la password per `aws-managed-user` con il seguente comando. La password iniziale per `aws-managed-user` è vuota, quindi è necessario sovrascriverla alla prima connessione.

   a.
   ```
   [aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-user password
   ```

   b. Quando ricevi il messaggio `Permission denied. Please enter user's old password:`, premi INVIO.

   > Suggerimento per la risoluzione dei problemi:
   >
   > Se ricevi il messaggio di errore `passwd: DS error: eDSAuthFailed`, usa il seguente comando.
   >
   > ```
   > [aws-managed-user ~]$ sudo passwd aws-managed-user
   > ```

4. Installa e avvia macOS Screen Sharing utilizzando il comando seguente.

   ```
   [aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

5. Disconnettiti dall'istanza digitando exit e premendo INVIO.

6. Dal computer locale, nel Terminale, riconnettiti all'istanza con un tunnel SSH alla porta VNC usando il seguente comando.

   ```
   ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-public-dns-name
   ```

7. Dal computer locale, connettiti a `localhost:5900` seguendo la procedura seguente:

   a. Apri il Finder e seleziona Vai.

   b. Seleziona Connetti al server.

   c. Nel campo Indirizzo del server, inserisci `vnc://localhost:5900`.

8. Nella finestra macOS, connettiti alla sessione remota dell'istanza Mac con processore Apple come `aws-managed-user`, utilizzando la password creata nel passaggio 3.

> **Note**
>
> Quando ti viene richiesto di accedere con il tuo ID Apple, seleziona Configura in seguito.

9. Accedi al volume Amazon EBS utilizzando una delle opzioni seguenti.

   a. Per macOS Ventura o versioni successive: apri Impostazioni di sistema, seleziona Generale nel riquadro sinistro, quindi Disco di avvio nella parte inferiore destra del riquadro.

   b. Per macOS Monterey o versioni precedenti: apri Preferenze di sistema, seleziona Disco di avvio, quindi sblocca il riquadro tramite l'icona del lucchetto nella parte inferiore sinistra della finestra.

   > **Note**
   >
   > Fino al riavvio, quando viene richiesta una password di amministratore, usa quella configurata in precedenza per `aws-managed-user`. La password potrebbe essere diversa da quella impostata per `ec2-user` o dall'account amministratore predefinito dell'istanza. Le istruzioni seguenti indicano quando utilizzare la password di amministratore dell'istanza.

10. Seleziona il volume Amazon EBS (il volume non denominato InternalDisknella finestra del disco di avvio) e scegli Riavvia.

    > **Note**
    >
    > Se disponi di più volumi Amazon EBS avviabili collegati all'istanza Mac con processore Apple, assicurati di utilizzare un nome univoco per ogni volume.

11. Conferma il riavvio, quindi scegli Autorizza utenti quando richiesto.
12. Nel riquadro Autorizza utente per questo volume, verifica che l'utente amministrativo (per impostazione predefinita, `ec2-user`) sia selezionato, quindi scegli Autorizza.
13. Inserisci la password `ec2-user` creata nel passaggio 3 della procedura precedente, quindi seleziona Continua.
14. Quando richiesto, inserisci la password per l'utente amministrativo speciale (`aws-managed-user`).

15. Dal computer locale, nel Terminale, riconnettiti all'istanza utilizzando SSH con nome utente `ec2-user`.

    > Suggerimento per la risoluzione dei problemi:
    >
    > Se visualizzi l'avviso `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, esegui il comando seguente e riconnettiti all'istanza tramite SSH.
    >
    > ```
    > rm ~/.ssh/known_hosts
    > ```

16. Per eseguire l'aggiornamento del software, usa i comandi in Aggiornamento del software su istanze Mac x86.

Aumentare le dimensioni di un volume EBS sull'istanza Mac

Puoi aumentare le dimensioni dei tuoi volumi Amazon EBS sull'istanza Mac. Per ulteriori informazioni, consulta Amazon EBS Elastic Volumes nella Amazon EBS User Guide.

Dopo aver aumentato le dimensioni del volume, è necessario aumentare le dimensioni del container APFS come segue.

Aumentare lo spazio su disco disponibile per l'uso

1. Determinare se è necessario riavviare. Se si ridimensiona un volume EBS esistente su un'istanza Mac in esecuzione, è necessario riavviare l'istanza per rendere disponibile la nuova dimensione. Se la modifica dello spazio su disco è stata eseguita durante l'avvio, non sarà necessario riavviare il sistema.

   Visualizzare lo stato corrente delle dimensioni del disco:

   ```
   [ec2-user ~]$  diskutil list external physical
   /dev/disk0 (external, physical):
      #:                       TYPE NAME                    SIZE       IDENTIFIER
      0:                 GUID_partition_scheme           *322.1 GB     disk0
      1:                 EFI EFI                          209.7 MB     disk0s1
      2:                 Apple_APFS Container disk2       321.9 GB     disk0s2
   ```

2. Copia e incolla il comando seguente.

```
[ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -
d" " -f8)
yes | sudo diskutil repairDisk $PDISK
```

3. Copia e incolla il comando seguente.

```
[ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
```

Interrompi o termina la tua istanza Amazon EC2 per Mac

Quando interrompi un'istanza Mac, questa rimane nello stato `stopping` per circa 15 minuti prima di entrare nello stato `stopped`.

Quando arresti o interrompi un'istanza Mac, Amazon EC2 esegue un flusso di lavoro di scrubbing sull'host dedicato sottostante per cancellare l'SSD interno, per cancellare le variabili NVRAM persistenti e per aggiornare il dispositivo con il firmware più recente. Ciò garantisce che le istanze Mac offrano la stessa sicurezza e privacy dei dati delle altre istanze EC2 Nitro. Consente inoltre di eseguire le AMI macOS più recenti. Durante il flusso di lavoro di scrubbing, l'host dedicato entra temporaneamente in stato di sospensione. Su istanze Mac x86, il completamento del flusso di lavoro di scrubbing può richiedere fino a 50 minuti. Sulle istanze Mac con processore Apple, il completamento del flusso di lavoro di scrubbing può richiedere fino a 110 minuti. Su istanze Mac x86, inoltre, se il firmware del dispositivo deve essere aggiornato, il completamento del flusso di lavoro di scrubbing può richiedere fino a 3 ore.

Non è possibile avviare l'istanza Mac interrotta o avviare una nuova istanza Mac fino al termine del flusso di lavoro di scrubbing, a quel punto Host dedicato entra nello stato `available`.

La misurazione e la fatturazione vengono sospese quando l'host dedicato entra nello stato `pending`. Non viene addebitato alcun addebito per la durata del flusso di lavoro di scrubbing.

Rilasciare l'Host dedicato per l'istanza Mac

Quando hai finito di utilizzare l'istanza Mac, puoi rilasciare l'Host dedicato. Prima di poter rilasciare il Host dedicato, è necessario interrompere o terminare l'istanza Mac. Non è possibile rilasciare l'host finché il periodo di allocazione non superi il periodo minimo di 24 ore.

Per rilasciare l'Host dedicato

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza e scegliere Instance State (Stato istanza), quindi scegliere Stop instance (Interrompi istanza) o Terminate instance (Termina istanza).
4. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
5. Selezionare il Host dedicato e scegliere Actions (Azioni), Release host (Rilascia host).
6. Quando viene richiesta la conferma, scegliere Release (Rilascia).

Trova le versioni macOS supportate per il tuo host dedicato Mac Amazon EC2

Puoi visualizzare le ultime versioni di macOS supportate dal tuo host dedicato Mac Amazon EC2. Con questa funzionalità, puoi verificare se il tuo host dedicato è in grado di supportare il lancio di istanze con le tue versioni macOS preferite.

Ogni versione di macOS richiede una versione firmware minima sull'Apple Mac sottostante per avviarsi correttamente. La versione del firmware per Apple Mac può diventare obsoleta se un Mac Dedicated Host allocato è rimasto inattivo per un periodo di tempo prolungato o se contiene un'istanza in esecuzione da molto tempo.

Per garantire la supportabilità per le ultime versioni di macOS, puoi interrompere o terminare le istanze sull'host dedicato Mac allocato. Ciò attiva il flusso di lavoro di pulizia dell'host e aggiorna il firmware sull'Apple Mac sottostante per supportare le ultime versioni di macOS. Un host dedicato con un'istanza in esecuzione di lunga durata verrà aggiornato automaticamente quando si arresta o si termina un'istanza in esecuzione.

Per ulteriori informazioni sul flusso di lavoro di pulizia, consulta. Interrompi o termina la tua istanza Amazon EC2 per Mac

Per ulteriori informazioni sull'avvio delle istanze Mac, consulta. Avvia un'istanza Mac utilizzando o AWS Management ConsoleAWS CLI

Puoi visualizzare informazioni sulle ultime versioni di macOS supportate sul tuo host dedicato allocato utilizzando la console Amazon EC2 o il. AWS CLI

Console

Per visualizzare le informazioni sul firmware dell'host dedicato utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Nella pagina dei dettagli degli host dedicati, in Ultime versioni macOS supportate, puoi vedere le ultime versioni di macOS supportate dall'host.

AWS CLI

Per visualizzare le informazioni sul firmware degli host dedicati, utilizzare AWS CLI

Utilizzare il `describe-mac-hosts`comando, sostituendolo `region` con il comando appropriato Regione AWS.

```
$ aws ec2 describe-mac-hosts --region us-east-1
  {
      "MacHosts": [
          {
              "HostId": "h-07879acf49EXAMPLE",
              "MacOSLatestSupportedVersions": [
                  "14.3",
                  "13.6.4",
                  "12.7.3"
              ]
          }
      ]
  }
```

Sottoscrizione alle notifiche delle AMI macOS

Per ricevere una notifica quando vengono rilasciate nuove AMI o quando bridgeOS è stato aggiornato, sottoscrivi le notifiche tramite Amazon SNS.

Per ulteriori informazioni sulle AMI macOS EC2, consulta. Note di rilascio delle AMI macOS di Amazon EC2

Come sottoscrivere le notifiche delle AMI macOS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario utilizzare questa regione in quanto le notifiche SNS per le quali hai effettuato la sottoscrizione sono state create in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Create Subscription (Crea sottoscrizione).
5. Nella finestra di dialogo Create subscription (Crea sottoscrizione) eseguire le seguenti operazioni:

   a. In Topic ARN (ARN argomento) copiare e incollare uno dei seguenti nome della risorsa Amazon (ARN):

      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates`**
      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates`**

   b. Per Protocollo, scegli una delle seguenti opzioni:

      - E-mail:

        In Endpoint digita l'indirizzo e-mail utilizzabile per ricevere le notifiche. Dopo aver creato la sottoscrizione, riceverai un messaggio di conferma con oggetto `AWS Notification - Subscription Confirmation`. Apri l'e-mail e seleziona Conferma sottoscrizione per completare la sottoscrizione.

      - SMS:

        In Endpoint digita un numero di telefono utilizzabile per ricevere le notifiche.

      - AWS Lambda, Amazon SQS, Amazon Data Firehose (le notifiche sono disponibili in formato JSON):

        Per Endpoint inserisci l'ARN per la funzione Lambda, la coda SQS o il flusso Firehose utilizzabile per ricevere le notifiche.

   c. Scegli Create Subscription (Crea sottoscrizione).

Quando le AMI macOS vengono rilasciate, inviamo notifiche ai sottoscrittori dell'argomento `amazon-ec2-macos-ami-updates`. Quando bridgeOS viene aggiornato, verranno inviate notifiche ai

sottoscrittori dell'argomento `amazon-ec2-bridgeos-updates`. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Annullamento della sottoscrizione alle notifiche delle AMI macOS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario utilizzare questa regione in quanto le notifiche SNS sono state create in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Selezionare la sottoscrizione, quindi selezionare Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni). Quando viene richiesta la conferma, selezionare Delete (Cancella).

Recupera gli AWS Systems Manager ID AMI macOS utilizzando l'API Parameter Store

Puoi visualizzare tutte le AMI macOS in un'unica API macOS Regione AWS e recuperare l'ultima AMI macOS interrogando l'API Parameter Store. AWS Systems Manager Utilizzando questi parametri pubblici, non è necessario cercare manualmente gli ID AMI macOS. I parametri pubblici sono disponibili sia per le x86 AMI ARM64 macOS che per macOS e possono essere integrati con i modelli esistenti. AWS CloudFormation

Autorizzazioni

Il principale IAM che utilizzi deve disporre dell'autorizzazione `ssm:GetParameter` IAM.

Per visualizzare un elenco di tutte le AMI macOS presenti nella versione corrente, utilizzare Regione AWSAWS CLI

Usa il get-parameters-by-pathcomando seguente per visualizzare un elenco di tutte le AMI macOS nella regione corrente.

```
aws ssm get-parameters-by-path --–path /aws/service/ec2-macos --–query
 "Parameters[].Name"
```

Per recuperare l'ID AMI dell'ultima delle principali AMI macOS utilizzando AWS CLI

Usa il seguente comando get-parameter con il sottoparametro. `image_id` Nell'esempio seguente, sostituiscilo `sonoma` con una versione principale supportata da macOS, `x86_64_mac` con il

processore e `region-code` con una versione supportata Regione AWS per la quale desideri l'ID AMI macOS più recente.

```
aws ssm get-parameter --name /aws/service/ec2-macos/sonoma/x86_64_mac/latest/image_id
 --region region-code
```

Per ulteriori informazioni, consulta Chiamata dei parametri pubblici dell'AMI per macOS nella Guida per l'AWS Systems Manager utente.

Note di rilascio delle AMI macOS di Amazon EC2

Le seguenti informazioni forniscono dettagli sui pacchetti inclusi di default nelle AMI EC2 macOS e riepilogano le modifiche per ogni versione di macOS AMI. EC2

Per informazioni su come iscriversi alle notifiche dell'AMI macOS, consulta. Sottoscrizione alle notifiche delle AMI macOS

Pacchetti predefiniti inclusi nelle AMI macOS di Amazon EC2

La tabella seguente descrive i pacchetti inclusi per impostazione predefinita nelle AMI macOS EC2.

Pacchetti	Note di rilascio
EC2inizializzazione macOS	https://github.com/aws/ec2-macos-init/tags
EC2Utilità macOS	https://github.com/aws/ec2-macos-utils/tags
AmazonAgente SSM	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI) versione 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Strumenti della riga di comando per Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
EC2 Instance Connect	https://github.com/aws/aws-ec2-instance-connect-config/releases

Pacchetti	Note di rilascio
Safari	https://developer.apple.com/documentation/safari-release-notes

Aggiornamenti alle AMI macOS di Amazon EC2

La tabella seguente descrive le modifiche incluse nelle versioni dell'AMI macOS di EC2. Tieni presente che alcune modifiche si applicano a tutte le AMI macOS EC2, mentre altre si applicano solo a un sottoinsieme di queste AMI.

Aggiornamenti alle AMI macOS EC2

Versione	Modifiche
2024.06.07	Tutte le AMI • Homebrew aggiornato alla versione 4.3.1-1 • `aws-cli`Aggiornato alla 2.15.56 • Aggiornato `amazon-ssm-agent` alla versione 3.3.380.0-1 Rilascio di macOS Sonoma 14.5 (tutte le istanze Mac) • Contenuti di sicurezza di macOS Sonoma 14.5 Rilascio di macOS Ventura 13.6.7 (tutte le istanze Mac) • Contenuti di sicurezza di macOS Ventura 13.6.7 • Safari aggiornato alla versione 17.5 • Contenuti di sicurezza di Safari 17.5 Rilascio di macOS Monterey 12.7.5 (tutte le istanze Mac) • Contenuti di sicurezza di macOS Monterey 12.7.5 • Safari aggiornato alla versione 17.5

Versione	Modifiche
	• Contenuti di sicurezza di Safari 17.5
2024.04.12	Tutte le AMI • Homebrew aggiornato alla versione 4.2.16-1 • `aws-cli`Aggiornato alla 2.15.36 Rilascio di macOS Sonoma 14.4.1 (tutte le istanze Mac) • Contenuti di sicurezza di macOS Sonoma 14.4.1 Rilascio di macOS Ventura 13.6.6 (tutte le istanze Mac) • Contenuti di sicurezza di macOS Ventura 13.6.6 • Safari aggiornato alla versione 17.4.1 • Contenuti di sicurezza di Safari 17.4.1 Per macOS Monterey (tutte le istanze Mac) • Safari aggiornato alla versione 17.4.1 • Contenuti di sicurezza di Safari 17.4.1

Amazon EBS: tipi di istanza ottimizzati

Le istanze ottimizzate per Amazon EBS utilizzano uno stack di configurazione ottimizzato e forniscono larghezza di banda aggiuntiva dedicata per l'I/O di Amazon EBS. Questa ottimizzazione offre le migliori prestazioni per i tuoi volumi EBS riducendo al minimo la contesa tra l'I/O di Amazon EBS e altro traffico proveniente dall'istanza.

Se collegati a un'istanza ottimizzata per EBS, i volumi General Purpose SSD (`gp2`e`gp3`) sono progettati per fornire almeno il 90% delle prestazioni IOPS assegnate il 99% delle volte in un determinato anno, mentre i volumi Provisioned IOPS SSD (`io1`e`io2`) sono progettati per fornire almeno il 90% delle prestazioni IOPS fornite il 99,9% delle volte in un determinato anno. Throughput Optimized HDD (`st1`) e Cold HDD (`sc1`) offrono almeno il 90 percento delle prestazioni di throughput

previste il 99 percento delle volte in un determinato anno. I periodi non conformi sono distribuiti in modo approssimativamente uniforme, con il 99% della velocità di trasmissione effettiva totale prevista ogni ora. Per ulteriori informazioni, consulta i tipi di volume di Amazon EBS nella Guida per l'utente di Amazon EBS.

Alcuni tipi di istanza sono ottimizzati per EBS per impostazione predefinita e non è necessario abilitarli e non hanno alcun effetto se si tenta di disabilitarli. Altri tipi di istanze supportano opzionalmente l'ottimizzazione EBS e puoi abilitarla durante o dopo il lancio pagando una tariffa oraria aggiuntiva. Alcuni tipi di istanze non supportano l'ottimizzazione EBS.

La Amazon EC2 Instance Types Guide indica quali tipi di istanze sono ottimizzati per EBS di default e quali tipi di istanze supportano opzionalmente l'ottimizzazione EBS, insieme alle loro prestazioni ottimizzate per Amazon EBS. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Specifiche di Amazon EBS: istanze per uso generico
- Specifiche di Amazon EBS: istanze ottimizzate per il calcolo
- Specifiche di Amazon EBS: istanze ottimizzate per la memoria
- Specifiche di Amazon EBS: istanze ottimizzate per lo storage
- Specifiche di Amazon EBS: istanze di elaborazione accelerata
- Specifiche di Amazon EBS: istanze di elaborazione ad alte prestazioni
- Specifiche di Amazon EBS: istanze di generazione precedente

Argomenti

- Ottieni le massime prestazioni ottimizzate per Amazon EBS
- Trova i tipi di istanze Amazon EC2 ottimizzati per Amazon EBS
- Abilita l'ottimizzazione di Amazon EBS per un'istanza Amazon EC2

Ottieni le massime prestazioni ottimizzate per Amazon EBS

Le prestazioni EBS di un'istanza sono limitate dai limiti di prestazioni del tipo di istanza o dalle prestazioni aggregate dei volumi collegati, a seconda di quale tra i due sia inferiore. Per ottenere le massime prestazioni EBS, un'istanza deve disporre di volumi collegati che forniscano prestazioni combinate pari o superiori alle prestazioni massime dell'istanza. Ad esempio, per ottenere `80,000` IOPS per`r6i.16xlarge`, l'istanza deve disporre di almeno `5` `gp3` volumi forniti con `16,000` IOPS ciascuno (`5` volumi x `16,000` IOPS = `80,000` IOPS). Ti consigliamo di scegliere un tipo di istanza

che offra un throughput Amazon EBS più dedicato rispetto alle esigenze dell'applicazione; in caso contrario, la connessione tra Amazon EBS e Amazon EC2 può diventare un collo di bottiglia a livello di prestazioni.

È possibile utilizzare i parametri `EBSIOBalance%` e `EBSByteBalance%` per determinare se le istanze sono dimensionate correttamente. Puoi visualizzare questi parametri nella CloudWatch console e impostare un allarme che viene attivato in base a una soglia specificata. Questi parametri sono espressi come percentuale. Le istanze con una percentuale costantemente bassa sono candidate per un aumento delle dimensioni. Le istanze la cui percentuale non scende mai al di sotto del 100% sono candidate per una riduzione delle dimensioni. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.

Le istanze a memoria elevata sono progettate per l'esecuzione di database di grandi dimensioni in memoria, incluse le distribuzioni di produzione del database in memoria SAP HANA all'interno del cloud. Per massimizzare le prestazioni EBS, utilizza istanze a memoria elevata con un numero pari di volumi `io1` o `io2` con prestazioni di provisioning identiche. Ad esempio, per carichi di lavoro IOPS gravosi, utilizza quattro volumi `io1` o `io2` con capacità di IOPS allocata da 40.000 per ottenere il numero massimo di 160.000 istanze IOPS. Analogamente, per carichi di lavoro ad elevata velocità di trasmissione effettiva, utilizza sei volumi `io1` o `io2` con capacità di IOPS allocata di 48.000 IOPS per ottenere la velocità di trasmissione effettiva massima di 4.750 MB/s. Per ulteriori suggerimenti, consultare Configurazione dell'archiviazione per SAP HANA.

Considerazioni

- Le istanze G4dn, I3en, M5a, M5ad, R5a, R5ad, T3, T3a e Z1d avviate dopo il 26 febbraio 2020 forniscono le prestazioni massime elencate nella tabella precedente. Per ottenere le massime prestazioni da un'istanza avviata prima del 26 febbraio 2020, interromperla e avviarla.
- Le istanze C5, C5d, C5n, M5, M5d, M5n, M5dn, R5, R5d, R5n, R5dn e P3dn avviate dopo il 3 dicembre 2019 forniscono le prestazioni massime elencate nella tabella precedente. Per ottenere le prestazioni massime da un'istanza avviata prima del 3 dicembre 2019, interromperla e avviarla.
- Le istanze `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` avviate dopo il 12 marzo 2020 forniscono le prestazioni indicate nella tabella precedente. Le istanze di questi tipi avviate prima del 12 marzo 2020 potrebbero fornire prestazioni inferiori. Per ottenere le prestazioni massime da un'istanza avviata prima del 12 marzo 2020, contattare il team dell'account per aggiornare l'istanza senza costi aggiuntivi.

Trova i tipi di istanze Amazon EC2 ottimizzati per Amazon EBS

Puoi utilizzare il AWS CLI per visualizzare i tipi di istanze nella regione corrente che supportano l'ottimizzazione EBS.

Per trovare tipi di istanze ottimizzati per Amazon EBS per impostazione predefinita

Utilizza il seguente comando della describe-instance-types. Se esegui questo comando da un prompt dei comandi di Windows, sostituisci i caratteri di continuazione\ line con il carattere ^.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=default --output=table
```

Output di esempio per `eu-west-1`:

```
-------------------------------------------------------------------------------
|                            DescribeInstanceTypes                            |
+-------------------+---------------------+-----------+-----------------------+
|   InstanceType    | MaxBandwidth(Mb/s)  |  MaxIOPS  |  MaxThroughput(MB/s)  |
+-------------------+---------------------+-----------+-----------------------+
|  m5dn.8xlarge     |  6800               |  30000    |  850.0                |
|  m6gd.xlarge      |  4750               |  20000    |  593.75               |
|  c4.4xlarge       |  2000               |  16000    |  250.0                |
|  r4.16xlarge      |  14000              |  75000    |  1750.0               |
|  m5ad.large       |  2880               |  16000    |  360.0                |
...
```

Per trovare tipi di istanze che supportano opzionalmente l'ottimizzazione di Amazon EBS

Utilizza il seguente comando della describe-instance-types.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=supported --output=table
```

Output di esempio per `eu-west-1`:

```
-------------------------------------------------------------------------
|                        DescribeInstanceTypes                          |
+--------------+----------------------+----------+----------------------+
| InstanceType | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
+--------------+----------------------+----------+----------------------+
|  i2.2xlarge  |  1000                |  8000    |  125.0                |
|  m2.4xlarge  |  1000                |  8000    |  125.0                |
|  m2.2xlarge  |  500                 |  4000    |  62.5                 |
|  c1.xlarge   |  1000                |  8000    |  125.0                |
|  i2.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.xlarge   |  500                 |  4000    |  62.5                 |
|  m1.xlarge   |  1000                |  8000    |  125.0                |
|  r3.4xlarge  |  2000                |  16000   |  250.0                |
|  r3.2xlarge  |  1000                |  8000    |  125.0                |
|  c3.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.2xlarge  |  1000                |  8000    |  125.0                |
|  r3.xlarge   |  500                 |  4000    |  62.5                 |
|  i2.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.2xlarge  |  1000                |  8000    |  125.0                |
|  m1.large    |  500                 |  4000    |  62.5                 |
+--------------+----------------------+----------+----------------------+
```

Abilita l'ottimizzazione di Amazon EBS per un'istanza Amazon EC2

Puoi abilitare manualmente l'ottimizzazione di Amazon EBS solo per i tipi di istanze che supportano facoltativamente l'ottimizzazione di Amazon EBS, ma non sono ottimizzate per Amazon EBS per impostazione predefinita. Per questi tipi di istanze puoi abilitare l'ottimizzazione di Amazon EBS durante o dopo il lancio pagando una tariffa oraria aggiuntiva.

Console

Per abilitare l'ottimizzazione di Amazon EBS durante il lancio

Nella procedura guidata Launch Instances, seleziona il tipo di istanza richiesto. Espandi la sezione Dettagli avanzati, quindi per l'istanza ottimizzata per EBS, seleziona Abilita.

Se il tipo di istanza selezionato non supporta l'ottimizzazione di Amazon EBS, il menu a discesa è disabilitato. Se il tipo di istanza è ottimizzato per Amazon EBS per impostazione predefinita, Enable è già selezionato.

Per abilitare l'ottimizzazione di Amazon EBS dopo il lancio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza.
3. Arrestare l'istanza. Scegliere Actions (Operazioni), Instance State (Stato istanza), Stop instance (Arresta istanza).

   > **Warning**
   >
   > Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

4. Con l'istanza ancora selezionata, scegliere Actions (Operazioni), Instance settings (Impostazioni istanza), Change instance type (Cambia tipo di istanza).
5. Seleziona EBS Optimized, quindi scegli Applica.

   Se il tipo di istanza è ottimizzato per Amazon EBS per impostazione predefinita o se non supporta l'ottimizzazione di Amazon EBS, la casella di controllo è disabilitata.
6. Riavvia l'istanza. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).

Command line

Per abilitare l'ottimizzazione di Amazon EBS durante il lancio

Puoi utilizzare uno dei seguenti comandi con l'opzione corrispondente.

- run-instances con `--ebs-optimized` (AWS CLI)
- New-EC2Instancecon `-EbsOptimized` ()AWS Tools for Windows PowerShell

Per abilitare l'ottimizzazione di Amazon EBS dopo il lancio

1. Se l'istanza è in esecuzione, interrompila utilizzando uno dei seguenti comandi.
   - stop-instances (AWS CLI)
   - Stop-EC2Instance (AWS Tools for Windows PowerShell)

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

2. Abilita l'ottimizzazione EBS utilizzando uno dei seguenti comandi con l'opzione corrispondente:

   - modify-instance-attributecon `--ebs-optimized` ()AWS CLI
   - Edit-EC2InstanceAttributecon `-EbsOptimized` (AWS Tools for Windows PowerShell)

Opzioni di acquisto delle istanze

Amazon EC2 fornisce le seguenti opzioni di acquisto per consentirti di ottimizzare i costi in base alle tue esigenze:

- Istanze on demand: pagamento al secondo per le istanze che vengono avviate.
- Savings Plans - Riduci i costi Amazon EC2 sottoscrivendo un impegno per una quantità consistente di utilizzo, in USD per ora, per un periodo di uno o tre anni.
- Istanze riservate - Puoi ridurre i costi Amazon EC2 utilizzando un'istanza specifica per una configurazione di istanza specifica, incluso il tipo di istanza e la Regione, per un periodo di uno o tre anni.
- Istanze spot - Consente di richiedere istanze EC2 inutilizzate, in grado di ridurre i costi di Amazon EC2 in modo significativo.
- Host dedicati - Puoi usufruire di un host fisico a pagamento completamente dedicato all'esecuzione delle istanze, riducendo i costi con le licenze software per socket, per core o per VM esistenti.
- Istanze dedicate - È possibile pagare all'ora per le istanze eseguite su un hardware a tenant singolo.
- Prenotazioni di capacità: riserva la capacità per le tue istanze EC2 in una zona di disponibilità specifica.

Se non puoi impegnarti per una configurazione specifica dell'istanza, ma puoi impegnarti per un importo di utilizzo, acquista Savings Plans per ridurre i costi delle istanze On-Demand.Se richiedi

una prenotazione di capacità, puoi acquistare Istanze riservate o Prenotazioni di capacità per una zona di disponibilità specifica. I blocchi di capacità possono essere utilizzati per prenotare un cluster di istanze GPU. Le istanze spot sono una scelta conveniente se si può essere flessibili su quando vengono eseguite le applicazioni e se queste possono essere interrotte. Gli host dedicati o le istanze dedicate possono aiutarti a rispettare i requisiti di conformità e a ridurre i costi utilizzando le tue licenze software esistenti collegate al server. Per ulteriori informazioni, consulta Prezzi di Amazon EC2.

Per ulteriori informazioni sui Savings Plans, consulta la Guida per l'utente di Savings Plans.

Indice

Identificazione del ciclo di vita dell'istanza

Il ciclo di vita di un'istanza inizia quando viene avviata e finisce quando viene terminata. L'opzione di acquisto che scegli influisce sul ciclo di vita dell'istanza. Ad esempio, un'Istanza on demand viene eseguita quando la avvii e finisce quando la termini. Un'istanza spot viene eseguita fin quando la capacità disponibile non si esaurisce e il prezzo massimo fissato dall'utente supera il prezzo Spot.

Utilizza uno dei metodi seguenti per determinare il ciclo di vita di un'istanza.

Per determinare il ciclo di vita dell'istanza tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Nella scheda Details (Dettagli) in Instance details (Dettagli istanza), trovare Lifecycle (Ciclo di vita). Se il valore è `spot`, l'istanza è un'Istanza spot. Se il valore è `normal`, l'istanza è un'Istanza on demand o un'Istanza riservata.

5. Nella scheda Details (Dettagli) in Host and placement group (Host e gruppo di collocamento), trovare Tenancy. Se il valore è `host`, l'istanza è in esecuzione su un Host dedicato. Se il valore è `dedicated`, l'istanza è un'Istanza dedicata.

Per determinare il ciclo di vita dell'istanza utilizzando AWS CLI

Utilizza il comando describe-instances seguente:

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0
```

Se l'istanza è in esecuzione su un Host dedicato, l'output contiene le informazioni seguenti:

```
"Tenancy": "host"
```

Se l'istanza è un'Istanza dedicata, l'output contiene le informazioni seguenti:

```
"Tenancy": "dedicated"
```

Se l'istanza è un'Istanza spot, l'output contiene le informazioni seguenti:

```
"InstanceLifecycle": "spot"
```

In caso contrario, l'output non contiene `InstanceLifecycle`.

Istanze on demand

Con Istanze on demand, sono previsti costi per la capacità di calcolo al secondo senza impegni a lungo termine. Hai il controllo completo del suo ciclo di vita: puoi decidere quando avviarla, arrestarla, ibernarla, avviarla, riavviarla o terminarla.

L'acquisto di Istanze on demand non richiede un impegno a lungo termine. Paghi solo per i secondi durante i quali le istanze on demand si trovano nello stato `running`, con un minimo di 60 secondi. Il prezzo al secondo per un'istanza on demand in esecuzione è fisso ed è riportato nella pagina dei prezzi on demand di Amazon EC2.

Consigliamo di utilizzare Istanze on demand per le applicazioni con carichi di lavoro irregolari o a breve termine che non possono essere interrotti.

Per risparmi significativi rispetto alle istanze on demand, utilizza AWS Savings Plans, Spot Instances o Istanze riservate.

Indice

Quote di istanze on demand

Esistono quote per il numero di istanze On-Demand in esecuzione per regione. Account AWS Le quote delle istanze on demand vengono gestite in termini di numero di unità di elaborazione centrale virtuali (vCPU) utilizzate dalle istanze on demand in esecuzione, indipendentemente dal tipo di istanza. Ogni tipo di quota specifica il numero massimo di vCPU per una o più famiglie di istanza.

Il tuo account include le seguenti quote per le istanze On-Demand. Le quote si applicano solo alle istanze in esecuzione. Se l'istanza è in sospeso, interrotta, interrotta o ibernata, non viene conteggiata ai fini delle quote.

Nome	Predefinita	Adattabile
Esecuzione di istanze DL on demand	0	Sì
Esecuzione di istanze F on demand	0	Sì
Esecuzione di tutte le istanze G e VT on demand	0	Sì
Istanze HPC on demand in esecuzione	0	Sì
Esecuzione delle istanze a memoria elevata on demand	0	Sì
Esecuzione di istanze Inf on demand	0	Sì
Esecuzione di istanze P on demand	0	Sì
Esecuzione di istanze on demand standard (A, C, D, H, I, M, R, T, Z)	5	Sì
Istanze Trn on demand in esecuzione	0	Sì

Nome	Predefinita	Adattabile
Esecuzione di istanze X on demand	0	Sì

Per informazioni sulle diverse famiglie, generazioni e dimensioni di istanze, consulta la Amazon EC2 Instance Types Guide.

È possibile avviare una qualsiasi combinazione di tipi di istanza che soddisfano le mutevoli esigenze dell'applicazione, a condizione che il numero di vCPU non superi la quota dell'account. Ad esempio, con una quota di istanze standard di 256 vCPU, puoi avviare 32 istanze `m5.2xlarge` (32 x 8 vCPU) oppure 16 istanze `c5.4xlarge` (16 x 16 vCPU). Per ulteriori informazioni, consulta Limiti Istanza on demand EC2.

Attività

- Monitoraggio delle quote e dell'utilizzo delle istanze on demand
- Richiesta di un aumento della quota

Monitoraggio delle quote e dell'utilizzo delle istanze on demand

Puoi visualizzare e gestire le quote delle istanze on demand utilizzando i seguenti metodi.

Visualizzazione delle quote correnti utilizzando la console Service Quotas

1. Aprire la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Nella barra di navigazione, selezionare una regione.
3. Nel campo di filtro, inserisci **`On-Demand`**.
4. La colonna Valore della quota applicata mostra il numero massimo di vCPU per ogni tipo di quota delle istanze on demand per il tuo account.

Per visualizzare le quote correnti utilizzando la console AWS Trusted Advisor

Apri la pagina dei limiti del servizio nella AWS Trusted Advisor console.

Per configurare gli CloudWatch allarmi

Con l'integrazione di Amazon CloudWatch Metrics, puoi monitorare l'utilizzo di EC2 rispetto alle tue quote. Puoi anche configurare gli allarmi per ricevere un avviso quando stai per raggiungere le quote. Per ulteriori informazioni, consulta Service Quotas e Amazon CloudWatch alarms nella Service Quotas User Guide.

Richiesta di un aumento della quota

Anche se Amazon EC2 aumenta automaticamente le quote delle istanze on demand in base al tuo utilizzo, se necessario puoi richiedere un aumento della quota. Ad esempio, se intendi avviare più istanze di quanto consentito dalla quota corrente, puoi richiedere un aumento della quota utilizzando la console Service Quotas, descritta nella pagina Service Quotas di Amazon EC2.

Eseguire una query sui prezzi delle Istanze on demand

Puoi utilizzare l'API Price List Service o l'API AWS Price List per richiedere i prezzi delle istanze On-Demand. Per ulteriori informazioni, consulta Utilizzo dell'API AWS Price List nella Guida per l'AWS Billing utente.

Istanze riservate

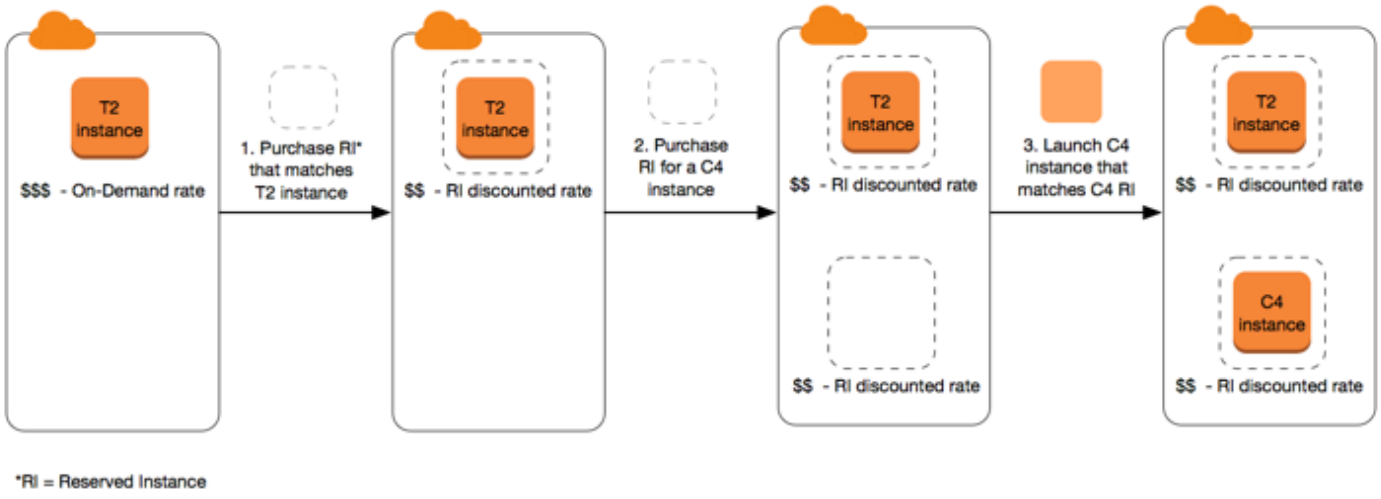
> **Important**
>
> Consigliamo Savings Plans rispetto alle istanze riservate. I piani di risparmio sono il modo più semplice e flessibile per risparmiare sui costi di AWS elaborazione e offrono prezzi più bassi (fino al 72% di sconto sui prezzi on demand), proprio come le istanze riservate. Tuttavia, i Savings Plans sono diversi dalle istanze riservate. Con Reserved Instances, ti impegni a rispettare una configurazione di istanza specifica, mentre con Savings Plans hai la flessibilità di utilizzare le configurazioni di istanza che meglio soddisfano le tue esigenze. Per utilizzare Savings Plans, ti impegni a garantire un importo di utilizzo costante, misurato in USD all'ora. Per ulteriori informazioni, consulta la AWS Guida per l'utente dei Savings Plans.

Le istanze riservate offrono una notevole riduzione sui costi Amazon EC2 rispetto ai prezzi delle istanze on demand. Le istanze riservate non sono istanze fisiche, ma piuttosto si tratta di uno sconto sulla fattura applicato all'uso delle istanze on demand nell'account. Per poter beneficiare dello sconto di fatturazione, queste Istanze on demand devono corrispondere a determinati attributi, ad esempio il tipo di istanza e la regione.

Argomenti di istanze riservate

Panoramica dell'Istanza riservata

Il diagramma seguente mostra una panoramica base dell'acquisto e dell'utilizzo di elementi di Istanze riservate.



In questo scenario, disponi di un'Istanza on demand (T2) in esecuzione nell'account per la quale paghi attualmente tariffe on-demand. Acquisti un'Istanza riservata che coincide con gli attributi dell'istanza in esecuzione e il vantaggio di fatturazione viene immediatamente applicato. Successivamente, acquisti un'Istanza riservata per un'istanza C4. Non hai istanze in esecuzione nell'account corrispondenti agli attributi di questa Istanza riservata. Nella fase finale, avvii

un'istanza corrispondente agli attributi dell'Istanza riservata C4 e il vantaggio di fatturazione viene immediatamente applicato.

Variabili chiave che determinano i prezzi di Istanza riservata

I prezzi di Istanza riservata sono determinati dalle seguenti variabili chiave.

Attributi istanza

Un'Istanza riservata ha quattro attributi che ne determinano il prezzo.

- Tipo di istanza: ad esempio, `m4.large`. Questo è composto dalla famiglia di istanze (ad esempio `m4`) e dalla dimensione dell'istanza (ad esempio `large`).
- Region (Regione): la regione in cui Istanza riservata è acquistata.
- Tenancy: indica se l'istanza è in esecuzione su hardware condiviso (per impostazione predefinita) o a singolo tenant (dedicato). Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.
- Piattaforma: il sistema operativo, ad esempio Windows o Linux/Unix. Per ulteriori informazioni, consulta Scelta di una piattaforma.

Scadenza impegno

Puoi acquistare un'Istanza riservata per un impegno di un anno o di tre anni, e l'impegno di tre anni presenta uno sconto maggiore.

- Un anno: un anno è definito come 31536000 secondi (365 giorni).
- Tre anni: tre anni sono definiti come 94608000 secondi (1095 giorni).

Gli elementi di Istanze riservate non si rinnovano automaticamente. Quando scadono, puoi continuare a utilizzare l'istanza EC2 senza interruzioni, ma verranno addebitate le tariffe on demand. Nell'esempio precedente, quando le Istanze riservate che coprono le istanze T2 e C4 scadono, vengono nuovamente applicate le tariffe on demand finché non termini le istanze o acquisti nuove Istanze riservate corrispondenti agli attributi dell'istanza.

> **Important**
>
> Dopo aver acquistato un'Istanza riservata, non è possibile annullare l'operazione. Tuttavia, è possibile modificare, scambiare o vendere l'Istanza riservata qualora le tue esigenze cambiassero.

Opzioni di pagamento

Le seguenti opzioni di pagamento sono disponibili per gli elementi di Istanze riservate:

- Pagamento anticipato totale: il pagamento viene effettuato per intero all'inizio del termine, senza altri costi o tariffe orarie aggiuntive per l'intervallo restante, indipendentemente dalle ore utilizzate.
- Pagamento anticipato parziale: è richiesto il pagamento anticipato di una parte del costo, mentre le restanti ore nel termine scelto vengono fatturate in base a una tariffa oraria scontata, indipendentemente dall'utilizzo dell'Istanza riservata.
- Nessun pagamento anticipato: viene applicata una tariffa oraria scontata per ogni ora entro il termine, indipendentemente dall'utilizzo dell'Istanza riservata. Non è richiesto alcun pagamento anticipato.

> **Note**
>
> Gli elementi di Istanze riservate senza pagamento anticipato si basano su un obbligo contrattuale mensile per l'intera durata della prenotazione. Per questo motivo, è necessario fornire una cronologia di fatturazione valida prima di poter acquistare elementi di Istanze riservate senza pagamento anticipato.

In linea generale, l'opzione più vantaggiosa consiste nello scegliere un pagamento anticipato più elevato per Istanze riservate. Puoi anche trovare istanze riservate offerte da venditori di terza parte a prezzi inferiori e per periodi più brevi sul Marketplace delle istanze riservate. Per ulteriori informazioni, consulta Vendita nel Marketplace delle istanze riservate.

Classe offerta

Se le tue esigenze di calcolo dovessero cambiare, potresti modificare o scambiare l'Istanza riservata in base alla classe di offerta.

- Standard: offre lo sconto maggiore, ma può essere solo modificata. La Istanze riservate standard non può essere scambiata.
- Modificabile: offre uno sconto rispetto alla Istanze riservate standard, ma può essere scambiata per un'altra Istanza riservata modificabile con differenti attributi di istanza. La Istanze riservate modificabile può inoltre essere modificata.

Per ulteriori informazioni, consulta Tipi di elementi di Istanze riservate (Classi di offerta).

> **Important**
>
> Dopo aver acquistato un'Istanza riservata, non è possibile annullare l'operazione. Tuttavia, è possibile modificare, scambiare o vendere l'Istanza riservata qualora le tue esigenze cambiassero.

Per ulteriori informazioni, consulta la pagina dei Prezzi delle istanze riservate di Amazon EC2.

Istanze riservate regionale e zonale (Ambito)

Quando acquisti una Istanza riservata, determini l'ambito della Istanza riservata. L'ambito può essere sia regionale che zonale.

- Regionale: quando acquisti una Istanza riservata per una regione, viene indicata come regionale Istanza riservata.
- Zonale: quando acquisti una Istanza riservata per una specifica zona di disponibilità viene indicata come zonale Istanza riservata.

L'ambito non influisce sul prezzo. Si paga lo stesso prezzo per una Istanza riservata regionale o zonale. Per ulteriori informazioni sui prezzi della Istanza riservata, consulta Variabili chiave che determinano i prezzi di Istanza riservata e Prezzi delle istanze riservate di Amazon EC2.

Per ulteriori informazioni sulla specifica dell'ambito di un'istanza riservata, consulta Attributi RI, specialmente il punto Zona di disponibilità.

Differenze tra Istanze riservate regionale e zonale

La tabella seguente evidenzia alcune differenze chiave tra Istanze riservate regionali e Istanze riservate zonali:

	Istanze riservate regionali	Istanze riservate zonali
Opzione di prenotazione di capacità	Un'Istanza riservata di regione non prenota la capacità.	Un'Istanza riservata di zona prenota la capacità nella zona di disponibilità specificata.

	Istanze riservate regionali	Istanze riservate zonali
Flessibilità zona di disponibilità	Lo sconto dell'Istanza riservata si applica all'utilizzo della istanza in qualsiasi zona di disponibilità in una regione specifica.	Nessuna flessibilità della zona di disponibilità—lo sconto della Istanza riservata si applica all'utilizzo dell'istanza nella sola zona di disponibilità specificata.
Flessibilità dimensioni istanza	Lo sconto della Istanza riservata si applica all'utilizzo dell'istanza nell'ambito della stessa famiglia di istanze, indipendentemente dalla dimensione. Supporto previsto solo su Istanze riservate Amazon Linux/Unix con tenancy di default. Per ulteriori informazioni, consulta La flessibilità della dimensione dell'istanza è determinata dal relativo fattore di normalizzazione..	Nessuna flessibilità della dimensione dell'istanza —lo sconto della Istanza riservata si applica solo all'utilizzo dell'istanza per il tipo e dimensione di istanza specificati.
Mettere in coda un acquisto	Puoi mettere in coda gli acquisti per le istanze riservate regionali.	Non puoi mettere in coda gli acquisti per le istanze riservate zonali.

Per maggiori informazioni ed esempi, consulta Applicazione degli elementi di Istanze riservate.

Tipi di elementi di Istanze riservate (Classi di offerta)

La classe di offerta di una Istanza riservata è Standard o Convertibile. Una Istanza riservata Standard offre un maggiore sconto rispetto a una Istanza riservata Convertibile, ma non è possibile scambiare

una Istanza riservata Standard. È possibile scambiare una Istanze riservate Convertibile. È possibile modificare una Istanze riservate Standard e Convertibile.

La configurazione della Istanza riservata comprende un tipo di istanza singola, piattaforma, ambito e tenancy per un termine. Se le tue esigenze di elaborazione cambiano, potresti essere in grado di modificare o scambiare la tua Istanza riservata.

Differenze tra Istanze riservate Standard e Convertibile

Di seguito vengono illustrate le differenze tra Istanze riservate Standard e Convertibile.

	Istanza riservata standard	Convertible Reserved Instance
Modificare le Istanze riservate	Alcuni attributi possono essere modificati. Per ulteriori informazioni, consulta Modificare le Istanze riservate.	Alcuni attributi possono essere modificati. Per ulteriori informazioni, consulta Modificare le Istanze riservate.
Cambio di istanze riservate	Non è possibile effettuare scambi.	Può essere scambiata durante il termine con un'altra Istanza riservata modificabile con nuovi attributi, tra cui famiglia di istanze, tipo di istanza, piattaforma, ambito o tenancy. Per ulteriori informazioni, consulta Scambiare le Istanze riservate modificabili.
Vendita nel Marketplace delle istanze riservate	Può essere venduta nel Marketplace delle istanze riservate.	Non può essere venduta nel Marketplace delle istanze riservate.
Acquisto nel Marketplace delle istanze riservate	Può essere acquistata nel Marketplace delle istanze riservate.	Non può essere acquistata nel Marketplace delle istanze riservate.

Applicazione degli elementi di Istanze riservate

Le istanze riservate non sono istanze fisiche, ma piuttosto si tratta di uno sconto sulla fattura applicato all'uso delle istanze on demand nell'account. Per poter beneficiare dello sconto, le istanze on demand devono presentare determinate specifiche delle istanze riservate.

Se si acquista un'istanza riservata e si dispone già di un'istanza on demand in esecuzione che corrisponde alle specifiche dell'istanza riservata, lo sconto di fatturazione viene applicato immediatamente e automaticamente. Non è necessario riavviare le tue istanze. Se non si possiede un'istanza on demand idonea in esecuzione, avviare un'istanza on demand con le stesse specifiche dell'istanza riservata. Per ulteriori informazioni, consulta Usa le tue Istanze riservate.

La classe di offerta (standard o convertibile) dell'istanza riservata non influisce sul modo in cui viene applicato lo sconto di fatturazione.

Argomenti

Applicazione degli elementi di Istanze riservate zonali

Un'istanza riservata acquistata per riservare la capacità in una zona di disponibilità specifica è denominata istanza riservata zonale.

- Lo sconto dell'istanza riservata si applica all'utilizzo della istanza corrispondente in quella zona di disponibilità.
- Gli attributi (tenancy, piattaforma, zona di disponibilità, tipo e dimensione) delle istanze in esecuzione devono corrispondere a quelli degli elementi di Istanze riservate.

Ad esempio, se si acquistano due Istanze riservate standard Linux/Unix con tenancy predefinita `c4.xlarge` nella zona di disponibilità us-east-1a, possono beneficiare dello sconto dell'istanza riservata fino a due istanze Linux/Unix con tenancy predefinita `c4.xlarge` in esecuzione nella zona di disponibilità us-east-1a.

Applicazione degli elementi di Istanze riservate regionali

Un'istanza riservata acquistata per una regione è detta istanza riservata regionale e fornisce la flessibilità della zona di disponibilità.

- Lo sconto dell'Istanza riservata si applica all'utilizzo della istanza in qualsiasi zona di disponibilità della regione.
- Lo sconto dell'istanza riservata si applica all'utilizzo dell'istanza nell'ambito della stessa famiglia di istanze, indipendentemente dalla dimensione: questo è noto come flessibilità della dimensione dell'istanza.

Flessibilità dimensioni istanza

Con la flessibilità sulle dimensioni dell'istanza, lo sconto dell'istanza riservata si applica all'utilizzo delle istanze con le medesime caratteristiche di famiglia, generazione e attributo. La flessibilità della dimensione dell'istanza viene applicata dall'istanza più piccola a quella più grande all'interno della famiglia di istanze sulla base del fattore di normalizzazione. Per un esempio di come viene applicato lo sconto dell'istanza riservata, consultare Scenario 2: Istanze riservate in un singolo account utilizzando il fattore di normalizzazione.

Limitazioni

- Supportata: la flessibilità delle dimensioni delle istanze è supportata solo per le istanze riservate regionali.
- Non supportata: la flessibilità delle dimensioni delle istanze non è supportata per le seguenti istanze riservate:
  - Istanze riservate acquistate pe una specifica zona di disponibilità, (Istanze riservate zonali)
  - Istanze riservate per istanze G4ad, G4dn, G5, G5g, Inf1 e Inf2
  - Istanze riservate per Windows Server, Windows Server con SQL Standard, Windows Server con SQL Server Enterprise, Windows Server con SQL Server Web, RHEL e SUSE Linux Enterprise Server
  - Istanze riservate con istanza dedicata a tenancy singola

La flessibilità della dimensione dell'istanza è determinata dal relativo fattore di normalizzazione.

La flessibilità della dimensione dell'istanza è determinata dal relativo fattore di normalizzazione. Lo sconto si applica totalmente o parzialmente alle istanze in esecuzione della stessa famiglia di istanze,

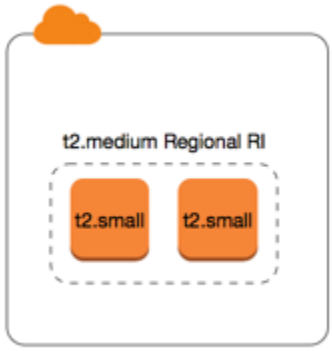
in base alla dimensione dell'istanza della prenotazione, in qualsiasi zona di disponibilità nella regione. Gli unici attributi che devono coincidere sono famiglia di istanze, tenancy e piattaforma.

La tabella seguente riporta le diverse dimensioni all'interno di una famiglia di istanze e il corrispondente fattore di normalizzazione. Questa scala viene utilizzata per applicare la tariffa scontata degli elementi di Istanze riservate all'utilizzo normalizzato della famiglia di istanze.

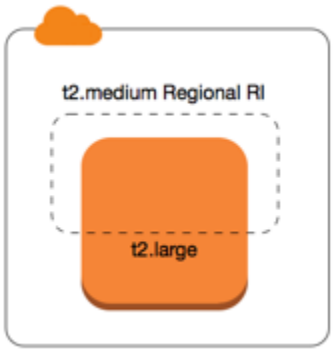
Dimensioni istanza	Fattore di normalizzazione
nano	0.25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192

Dimensioni istanza	Fattore di normalizzazione
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Ad esempio, il fattore di normalizzazione di un'istanza `t2.medium` è 2. Se acquisti un'Istanza riservata Amazon Linux/Unix con tenancy predefinita `t2.medium` nella regione US East (N. Virginia) e disponi di due istanze `t2.small` in esecuzione nel tuo account in quella regione, il vantaggio di fatturazione viene applicato per intero a entrambe le istanze.



In alternativa, se disponi di un'istanza `t2.large` in esecuzione sul tuo account nella regione US East (N. Virginia), il vantaggio di fatturazione viene applicato al 50% dell'utilizzo dell'istanza.



Il fattore di normalizzazione viene anche applicato quando si modificano gli elementi di Istanze riservate. Per ulteriori informazioni, consulta Modificare le Istanze riservate.

Fattore di normalizzazione per le istanze bare metal

La flessibilità della dimensione dell'istanza si applica inoltre alle istanze bare metal all'interno della famiglia di istanze. Se hai delle Istanze riservate Amazon Linux/Unix regionali con tenancy condivisa su istanze bare metal, puoi beneficiare dello sconto della Istanza riservata nell'ambito della medesima famiglia di istanze. Si verifica anche il contrario: se hai delle Istanze riservate Amazon Linux/Unix regionali con tenancy condivisa su istanze nella stessa famiglia come istanze bare metal, puoi beneficiare dello sconto della Istanza riservata sull'istanza bare metal.

Le dimensioni dell'istanza `metal` non hanno un singolo fattore di normalizzazione. Un'istanza bare metal ha lo stesso fattore di normalizzazione della dimensione dell'istanza virtualizzata equivalente all'interno della stessa famiglia di istanze. Ad esempio, un'istanza `i3.metal` ha lo stesso fattore di normalizzazione di un'istanza `i3.16xlarge`.

Dimensioni istanza	Fattore di normalizzazione
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128
`c5n.metal`	144
`c5.metal` | `c5d.metal` | `i3en.metal` | `m5.metal` | `m5d.metal` | `m5dn.metal` | `m5n.metal` | `r5.metal` | `r5b.metal` | `r5d.metal` | `r5dn.metal` | `r5n.metal`	192
`c6i.metal` | `c6id.metal` | `m6i.metal` | `m6id.metal` | `r6d.metal` | `r6id.metal`	256
`u-*.metal`	896

Ad esempio, il fattore di normalizzazione di un'istanza `i3.metal` è 128. Se acquisti una Istanza riservata Amazon Linux/Unix con tenancy di default `i3.metal` in US East (N. Virginia), il vantaggio di fatturazione può essere applicato come segue:

- In alternativa, se disponi di una `i3.16xlarge` in esecuzione sul tuo account nella regione, il vantaggio di fatturazione è applicato integralmente all'istanza `i3.16xlarge` (`i3.16xlarge` fattore di normalizzazione = 128).
- In alternativa, se disponi di due istanze `i3.8xlarge` in esecuzione sul tuo account nella regione, il vantaggio di fatturazione è applicato integralmente alle due istanze `i3.8xlarge` (`i3.8xlarge` fattore di normalizzazione = 64).
- In alternativa, se disponi di quattro istanze `i3.4xlarge` in esecuzione sul tuo account nella regione, il vantaggio di fatturazione è applicato integralmente alle quattro istanze `i3.4xlarge` (`i3.4xlarge` fattore di normalizzazione = 32).

È vero anche il contrario. Ad esempio, se acquisti due Istanze riservate Amazon Linux/Unix con tenancy predefinita `i3.8xlarge` in US East (N. Virginia), e disponi di una istanza `i3.metal` in quella regione, il vantaggio di fatturazione viene applicato per intero alla istanza `i3.metal`.

Esempi di applicazione di elementi di Istanze riservate

Gli scenari seguenti descrivono le modalità di applicazione degli elementi di Istanze riservate.

- Scenario 1: elementi di Istanze riservate in un singolo account
- Scenario 2: Istanze riservate in un singolo account utilizzando il fattore di normalizzazione
- Scenario 3: elementi di Istanze riservate regionali in account collegati
- Scenario 4: elementi di Istanze riservate zonali in un account collegato

Scenario 1: elementi di Istanze riservate in un singolo account

Stai eseguendo gli elementi di Istanze on demand seguenti nell'account A:

- 4 x istanze Linux `m3.large` con tenancy di default in zona di disponibilità us-east-1a
- 2 x istanze Amazon Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1b
- 1 x istanza Amazon Linux `c4.xlarge` con tenancy di default in zona di disponibilità us-east-1c

Acquisti gli elementi di Istanze riservate seguenti nell'account A:

- 4 x Istanze riservate Linux `m3.large` con tenancy predefinita nella zona di disponibilità us-east-1a (capacità riservata)
- 4 x Istanze riservate Amazon Linux `m4.large`con tenancy predefinita nella regione us-east-1

- 1 x Istanze riservate Amazon Linux `c4.large`con tenancy predefinita nella regione us-east-1

I vantaggi della Istanza riservata vengono applicati nel modo seguente:

- Lo sconto e la prenotazione di capacità delle quattro Istanze riservate `m3.large` di zona vengono utilizzati dalle quattro istanze `m3.large` perché i loro attributi (dimensione dell'istanza, regione, piattaforma, tenancy) coincidono.
- Le Istanze riservate `m4.large` forniscono flessibilità in termini di dimensione dell'istanza e zona di disponibilità perché sono Istanze riservate Amazon Linux regionali con tenancy predefinita.

  Un'istanza `m4.large` equivale a 4 unità normalizzate/ora.

  Hai acquistato quattro Istanze riservate `m4.large` regionali che, in totale, equivalgono a 16 unità normalizzate/ora (4x4). L'account A ha due istanze `m4.xlarge` in esecuzione, che equivalgono a 16 unità normalizzate/ora (2x8). In questo caso, le quattro Istanze riservate regionali `m4.large` forniscono il vantaggio della fatturazione completa per l'uso delle due istanze `m4.xlarge`.
- L' `c4.large` regionale Istanza riservata in us-east-1 fornisce flessibilità in termini di dimensione dell'istanza e zona di disponibilità perché è un'Istanza riservata Amazon Linux regionale con tenancy predefinita che si applica all'istanza `c4.xlarge`. Un'istanza `c4.large` equivale a 4 unità normalizzate/ora e un'istanza `c4.xlarge` equivale a 8 unità normalizzate/ora.

  In questo caso, l'Istanza riservata `c4.large` regionale fornisce un vantaggio parziale all'utilizzo di istanze `c4.xlarge`. Ciò dipende dal fatto che l'Istanza riservata `c4.large` equivale a 4 unità normalizzate/ora di utilizzo, ma l'istanza `c4.xlarge` richiede 8 unità normalizzate/ora. Pertanto, lo sconto di fatturazione dell'Istanza riservata `c4.large` si applica al 50% dell'uso di `c4.xlarge`. Il restante utilizzo di `c4.xlarge` viene addebitato alla tariffa on demand.

Scenario 2: Istanze riservate in un singolo account utilizzando il fattore di normalizzazione

Stai eseguendo gli elementi di Istanze on demand seguenti nell'account A:

- 2 x istanze Amazon Linux `m3.xlarge` con tenancy predefinita in zona di disponibilità us-east-1a
- 2 x istanze Amazon Linux `m3.large` con tenancy di default in zona di disponibilità us-east-1b

Si acquistano gli elementi di Istanze riservate seguenti nell'account A:

- 1 x Istanze riservate Amazon Linux `m3.2xlarge` con tenancy predefinita nella regione us-east-1

I vantaggi della Istanza riservata vengono applicati nel modo seguente:

- L'istanza riservata regionale `m3.2xlarge` in us-east-1 fornisce flessibilità in termini di dimensione dell'istanza e zona di disponibilità perché è un'istanza riservata Amazon Linux regionale con tenancy predefinita. Si applica prima alle istanze `m3.large` e poi alle istanze `m3.xlarge`, perché si applica dalla dimensione più piccola a quella più grande all'interno della famiglia di istanze in base al fattore di normalizzazione.

  Un'istanza `m3.large` equivale a 4 unità normalizzate/ora.

  Un'istanza `m3.xlarge` equivale a 8 unità normalizzate/ora.

  Un'istanza `m3.2xlarge` equivale a 16 unità normalizzate/ora.

  Il vantaggio viene applicato come segue:

  L'istanza riservata regionale `m3.2xlarge` offre il massimo vantaggio a 2 utilizzi `m3.large`, perché insieme queste istanze rappresentano 8 unità/ora normalizzate. Ciò lascia 8 unità/ora normalizzate da applicare alle istanze `m3.xlarge`.

  Con le restanti 8 unità/ora normalizzate, l'istanza riservata regionale `m3.2xlarge` offre pieno vantaggio a 1 x utilizzo `m3.xlarge`, perché ciascuna istanza `m3.xlarge` equivale a 8 unità normalizzate/ora. Il restante utilizzo di `m3.xlarge` viene addebitato alla tariffa on demand.

Scenario 3: elementi di Istanze riservate regionali in account collegati

Gli elementi di Istanze riservate vengono innanzitutto applicati all'utilizzo all'interno dell'account di acquisto e, successivamente, all'utilizzo idoneo in qualsiasi altro account nell'organizzazione. Per ulteriori informazioni, consulta Istanze riservate e fatturazione consolidata. Per gli elementi di Istanze riservate regionali che offrono flessibilità della dimensione dell'istanza viene applicata dall'istanza più piccola a quella più grande all'interno della famiglia di istanze sulla base del fattore di normalizzazione.

Stai eseguendo la seguente Istanze on demand nell'account A (l'account di acquisto):

- 2 x istanze Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1a
- 1 x istanza Linux `m4.2xlarge` con tenancy di default in zona di disponibilità us-east-1b
- 2 x istanze Linux `c4.xlarge` con tenancy di default in zona di disponibilità us-east-1a
- 1 x istanza Linux `c4.2xlarge` con tenancy di default in zona di disponibilità us-east-1b

Un altro cliente sta eseguendo le seguenti Istanze on demand nell'account B, —un account collegato:

- 2 x istanze Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1a

Stai acquistando i seguenti elementi di Istanze riservate regionali nell'account A:

- 4 x Istanze riservate Linux `m4.xlarge` con tenancy predefinita nella regione us-east-1
- 2 x Istanze riservate Linux `c4.xlarge` con tenancy predefinita nella regione us-east-1

I vantaggi della Istanza riservata regionale vengono applicati nel modo seguente:

- Lo sconto delle quattro Istanze riservate`m4.xlarge` è usato dalle due istanze `m4.xlarge` e dalla singola istanza `m4.2xlarge` nell'account A (account di acquisto). Tutte le tre istanze hanno i medesimi attributi (famiglia di istanze, regione, piattaforma, tenancy). Lo sconto è applicato prima alle istanze nell'account di acquisto (account A), anche se l'account B (account collegato) ha due `m4.xlarge` che anch'esse corrispondono alle Istanze riservate. Non è prevista la prenotazione di capacità perché le Istanze riservate sono Istanze riservate regionali.
- Lo sconto delle due Istanze riservate `c4.xlarge` si applica alle due istanze `c4.xlarge`, in quanto di dimensioni inferiori rispetto all'istanza`c4.2xlarge`. Non è prevista la prenotazione di capacità perché le Istanze riservate sono Istanze riservate regionali.

Scenario 4: elementi di Istanze riservate zonali in un account collegato

In generale, gli elementi di Istanze riservate di proprietà di un account vengono applicati innanzitutto all'utilizzo in quell'account. Tuttavia, in presenza di Istanze riservate idonee e non utilizzate per una zona di disponibilità specifica (Istanze riservate di zona) in altri account dell'organizzazione, queste vengono applicate all'account prima delle Istanze riservate regionali di proprietà dell'account. Questo mira a garantire il massimo utilizzo dell'Istanza riservata e una fattura ridotta. Per motivi di fatturazione, tutti gli account all'interno dell'organizzazione vengono trattati come se fossero un account unico. L'esempio seguente potrebbe aiutare a descrivere quanto illustrato in precedenza.

Stai eseguendo la seguente Istanza on demand nell'account A (l'account di acquisto):

- 1 x istanza Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1a

Un cliente sta eseguendo la seguente Istanza on demand nell'account collegato B:

- 1 x istanza Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1b

Stai acquistando i seguenti elementi di Istanze riservate regionali nell'account A:

- 1 x Istanza riservata Linux `m4.xlarge` con tenancy predefinita nella regione us-east-1

Un cliente acquista anche i seguenti elementi di Istanze riservate zonali nell'account collegato C:

- 1 x Istanze riservate Linux `m4.xlarge` con tenancy predefinita in zona di disponibilità us-east-1a

I vantaggi della Istanza riservata vengono applicati nel modo seguente:

- Lo sconto dell'Istanza riservata `m4.xlarge` di zona di proprietà dell'account C viene applicato all'utilizzo di `m4.xlarge` nell'account A.
- Lo sconto dell'Istanza riservata `m4.xlarge` regionale di proprietà dell'account A viene applicato all'utilizzo di `m4.xlarge` nell'account B.
- Se l'istanza riservata regionale di proprietà dell'account A era stata inizialmente applicata all'utilizzo nell'account A, l'istanza riservata di zona di proprietà dell'account C rimane inutilizzata e l'utilizzo nell'account B viene fatturato in base alle tariffe on demand.

Per ulteriori informazioni, consulta la sezione relativa alle Istanze riservate nel report Billing and Cost Management.

> **Note**
>
> Le istanze riservate zonali riservano la capacità solo all'account di proprietà e non possono essere condivise con altri Account AWS. Se hai bisogno di condividere la capacità con altri Account AWS, usa Prenotazione della capacità on demand.

Usa le tue Istanze riservate

Le Istanze riservate vengono applicate automaticamente alle Istanze on demand in esecuzione, purché le specifiche coincidano. Se non sono presenti Istanze on demand in esecuzione con specifiche coincidenti con quelle dell'Istanza riservata, l'Istanza riservata non verrà utilizzata finché non sarà avviata un'istanza con le specifiche richieste.

Se si sta avviando un'istanza on demand per usufruire del vantaggio di fatturazione di un'istanza riservata, assicurarsi di specificare le seguenti informazioni durante la configurazione dell'istanza on demand:

Platform (Piattaforma)

È necessario specificare una Amazon Machine Image (AMI) corrispondente alla piattaforma (descrizione del prodotto) dell'istanza riservata. Ad esempio, se si è specificato `Linux/UNIX` per l'istanza riservata, si può avviare un'istanza da un'AMI Amazon Linux o un'AMI Ubuntu.

Tipo di istanza

Se si è acquistata un'istanza riservata zonale, è necessario specificare lo stesso tipo di istanza dell'istanza riservata, ad esempio, `t3.large`. Per ulteriori informazioni, consulta Applicazione degli elementi di Istanze riservate zonali.

Se si è acquistata un'istanza riservata regionale, è necessario specificare un tipo di istanza della stessa famiglia di istanze del tipo di istanza dell'istanza riservata. Ad esempio, se si è specificato `t3.xlarge` per la propria istanza riservata, è necessario avviare l'istanza dalla famiglia T3, ma si può specificare qualsiasi dimensione, ad esempio `t3.medium`. Per ulteriori informazioni, consulta Applicazione degli elementi di Istanze riservate regionali.

Zona di disponibilità

Se si è acquistata un'Istanza riservata per una zona di disponibilità specifica, è necessario avviare l'istanza nella stessa zona di disponibilità.

Se si è acquistata un'istanza riservata regionale, è possibile avviare l'istanza in qualsiasi zona di disponibilità nella regione specificata per l'istanza riservata.

Tenancy

La tenancy (`dedicated` o `shared`) dell'istanza deve corrispondere alla tenancy dell'istanza riservata. Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.

Per esempi di come le istanze riservate vengono applicate alle istanze on demand in esecuzione, consulta Applicazione degli elementi di Istanze riservate. Per ulteriori informazioni, consulta Perché le mie istanze riservate di Amazon EC2 non si applicano alla mia AWS fatturazione nel modo previsto?

È possibile utilizzare vari metodi per avviare le istanze on demand che utilizzano lo sconto dell'istanza riservata. Per ulteriori informazioni sui diversi metodi di avvio, consultare Lancio

dell'istanza. Per avviare un'istanza, è possibile utilizzare Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Guida per l'utente di Amazon EC2 Auto Scaling.

Come avviene la fatturazione

Tutti gli elementi di Istanze riservate offrono uno sconto significativo rispetto al prezzo on demand. Con gli elementi di Istanze riservate, è previsto il pagamento per l'intero termine, indipendentemente dall'uso effettivo. Puoi scegliere di effettuare un pagamento anticipato, anticipato parziale o mensile per la tua Istanza riservata, in base all'opzione di pagamento specificata per l'Istanza riservata.

Quando gli elementi di Istanze riservate scadono, ti vengono addebitate tariffe on demand per l'utilizzo di istanze EC2. Puoi mettere in coda una Istanza riservata per l'acquisto con fino a tre anni di anticipo. Questo garantisce copertura continua. Per ulteriori informazioni, consulta Metti in coda il tuo acquisto.

Piano gratuito di AWS È disponibile per la nuova versione. Account AWS Se utilizzi Piano gratuito di AWS per eseguire istanze Amazon EC2 e acquisti un'istanza riservata, ti verrà addebitato il prezzo standard. Per informazioni, consulta Piano gratuito di AWS.

Indice

Fatturazione dell'utilizzo

Le Istanze riservate vengono fatturate ogni ora di orologio per l'intervallo di tempo selezionato, anche se non ci sono istanze in esecuzione. L'inizio dell'ora parte a zero minuti e zero secondi, in base a un orologio standard di 24 ore. Ad esempio, un'ora di orologio inizia a 1:00:00 e termina a 1:59:59. Per ulteriori informazioni sugli stati delle istanze, consulta Ciclo di vita dell'istanza.

Un vantaggio di fatturazione dell'Istanza riservata viene applicato a un'istanza in esecuzione su base al secondo. La fatturazione al secondo è disponibile per le istanze che utilizzano una distribuzione Linux open source, come Amazon Linux e Ubuntu. La fatturazione oraria viene utilizzata per le distribuzioni Linux commerciali, come Red Hat Enterprise Linux e SUSE Linux Enterprise Server.

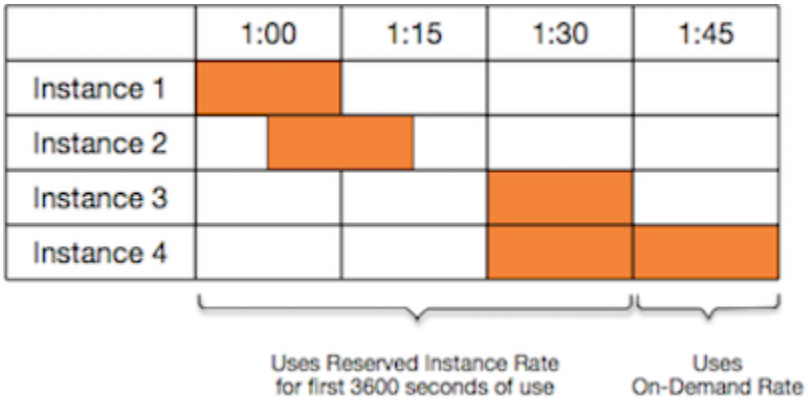
Il vantaggio di fatturazione della Istanza riservata può essere applicato a un massimo di 3600 secondi (un'ora) di utilizzo d'istanza per ora di orologio. È possibile eseguire più istanze

contemporaneamente, ma puoi solo ricevere il vantaggio dello sconto dell'Istanza riservata per un totale di 3600 secondi per ora di orologio. L'utilizzo dell'istanza superiore a 3600 secondi in un'ora di orologio viene fatturato alla tariffa on demand.

Ad esempio, se acquisti un `m4.xlarge` Istanza riservata ed esegui quattro istanze `m4.xlarge` contemporaneamente per un'ora, un'istanza viene fatturata alla tariffa di un'ora di utilizzo dell'Istanza riservata e le altre tre istanze alla tariffa di tre ore di utilizzo on demand.

Tuttavia, se acquisti un'`m4.xlarge` Istanza riservata ed esegui quattro istanze `m4.xlarge` per 15 minuti (900 secondi) ciascuna nella stessa ora, il tempo totale di esecuzione per le istanze è un'ora, il che supporrà un'ora di utilizzo dell'Istanza riservata e 0 ore di utilizzo on demand.

Se più istanze idonee sono in esecuzione contemporaneamente, il vantaggio di fatturazione dell'Istanza riservata viene applicato a tutte le istanze nello stesso momento, per un massimo di 3600 secondi in un'ora di orologio; successivamente, si applicano le tariffe on demand.



Cost Explorer sulla console Billing and Cost Management consente di analizzare i risparmi realizzati rispetto all'esecuzione di Istanze on demand. Le domande frequenti sulle Istanze riservate includono un esempio di calcolo del valore di listino.

Se chiudi l' AWS account, la fatturazione su richiesta per le tue risorse si interrompe. Tuttavia, se disponi di elementi di Istanze riservate nell'account, continuerai a ricevere la relativa fattura finché non scadono.

Visualizzazione di una fattura

Puoi trovare maggiori informazioni su addebiti e tariffe applicati al tuo account nella console AWS Billing and Cost Management.

- Il Dashboard (Pannello di controllo) mostra un riepilogo di spesa per l'account.
- Nella pagina Bills (Fatture), sotto Details (Dettagli), espandi la sezione Elastic Compute Cloud e la regione per ottenere le informazioni di fatturazione relative alle Istanze riservate.

Puoi visualizzare gli addebiti online o scarica un file CSV.

Puoi anche tenere traccia dell'utilizzo delle tue istanze riservate utilizzando il report AWS sui costi e sull'utilizzo. Per ulteriori informazioni, consulta Istanze riservate nel Report su costi e utilizzo nella Guida per l'utente di AWS Billing .

Istanze riservate e fatturazione consolidata

I vantaggi in termini di prezzi degli elementi di Istanze riservate sono condivisi quando l'account di acquisto appartiene a un insieme di account fatturati in un unico account pagamento della fatturazione consolidata. L'utilizzo delle istanze in tutti gli account membri viene aggregato mensilmente nell'account pagamento. In generale, questa modalità è utile per le aziende con diversi team o gruppi funzionali. Successivamente, viene applicata la logica normale di Istanza riservata per calcolare la fattura. Per ulteriori informazioni, consulta Fatturazione consolidata per AWS Organizations.

Se chiudi l'account che ha acquistato l'istanza riservata, l'account di pagamento continuerà ad essere addebitato per l'istanza riservata fino alla scadenza dell'istanza. L'account chiuso viene eliminato definitivamente dopo 90 giorni e gli account dei membri non beneficiano più dello sconto di fatturazione Istanza riservata.

> **Note**
>
> Le istanze riservate zonali riservano la capacità solo all'account di proprietà e non possono essere condivise con altri Account AWS. Se hai bisogno di condividere la capacità con altri Account AWS, usa Prenotazione della capacità on demand.

Livelli dei prezzi di sconto della Istanza riservata

Se il tuo account è idoneo per un livello di prezzi di sconto, riceve automaticamente sconti su pagamento anticipato e tariffe di utilizzo delle istanze per acquisti di Istanza riservata eseguiti all'interno di tale livello a partire da quel punto. Per risultare idonei per uno sconto, il valore di listino della tua Istanze riservate nella regione deve essere pari ad almeno $500.000 USD.

Si applicano le regole seguenti:

- I livelli di prezzi e relativi sconti si applicano solo agli acquisti di Istanze riservate standard Amazon EC2.
- I livelli di prezzi non si applicano alle Istanze riservate per Windows con SQL Server Standard, SQL Server Web e SQL Server Enterprise.
- I livelli di prezzi non si applicano alle Istanze riservate per Linux con SQL Server Standard, SQL Server Web e SQL Server Enterprise.
- Gli sconti sulla fascia di prezzo si applicano solo agli acquisti effettuati da AWS. Non si applicano agli acquisti di elementi di Istanze riservate di terze parti.
- I livelli di prezzi di sconto non sono attualmente applicabili agli acquisti di Istanza riservata modificabile.

Argomenti

Calcolare gli sconti sui prezzi della Istanza riservata

Puoi determinare il livello di prezzi per il tuo account calcolando il valore di listino per tutti i tuoi elementi di Istanze riservate in una regione. Moltiplica il prezzo orario ricorrente di ciascuna prenotazione per il numero totale di ore del termine e aggiungi il prezzo iniziale senza sconti (noto anche come prezzo fisso) al momento dell'acquisto. Dal momento che il valore di listino è basato su prezzi (pubblici) non scontati, non subisce variazioni qualora risultassi idoneo per uno sconto sui volumi o se il prezzo scendesse dopo l'acquisto degli elementi di Istanze riservate.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Ad esempio, in caso di un'Istanza riservata con pagamento anticipato parziale di un anno, `t2.small` suppone che il prezzo iniziale sia 60 USD e che la tariffa oraria sia 0,007 USD, per un valore di listino di 121,32 USD.

```
121.32 = 60.00 + (0.007 * 8760)
```

New console

Per visualizzare i valori del prezzo fisso per le Istanze riservate tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Per visualizzare la colonna Prezzo anticipato, scegli impostazioni () nell'angolo in alto a destra, attiva Prezzo anticipato e scegli Conferma.

Old console

Per visualizzare i valori del prezzo fisso per le Istanze riservate tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Per visualizzare la colonna Prezzo anticipato, scegli impostazioni () nell'angolo in alto a destra, seleziona Prezzo anticipato e scegli Chiudi.

Per visualizzare i valori del prezzo fisso per le Istanze riservate tramite la riga di comando

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)
- DescribeReservedInstances(API Amazon EC2)

Acquistare con un livello di sconto

Quando si acquistano Istanze riservate, Amazon EC2 applica automaticamente qualsiasi sconto alla parte dell'acquisto che rientra in un livello di prezzi di sconto. Non è richiesto alcun intervento diverso

ed è possibile acquistare Istanze riservate utilizzando qualsiasi strumento Amazon EC2. Per ulteriori informazioni, consulta Acquisto di istanze riservate.

Dopo che il valore di listino delle Istanze riservate attive in una regione passa in un livello di prezzi di sconto, qualsiasi acquisto futuro di Istanze riservate in tale regione viene addebitato a una tariffa scontata. Se un singolo acquisto di elementi di Istanze riservate in una regione ti permette di superare la soglia di un livello di sconto, la porzione dell'acquisto che va oltre tale soglia sarà addebitata alla tariffa scontata. Per ulteriori informazioni sugli ID temporanei dell'Istanza riservata creati durante il processo di acquisto, consulta Passaggio di livello di prezzi.

Se il valore di listino scende al di sotto del prezzo di vendita per tale livello di prezzi di sconto, ad esempio in caso di scadenza di — alcune Istanze riservate, gli acquisti — futuri di Istanze riservate nella regione non saranno scontati. Tuttavia, lo sconto continua a essere applicato agli elementi di Istanze riservate originariamente acquistati nel livello di prezzi di sconto.

Quando compri elementi di Istanze riservate, si verifica uno tra quattro possibili scenari:

- Nessuno sconto: l'acquisto all'interno di una regione è ancora al di sotto della soglia di sconto.
- Sconto parziale: l'acquisto all'interno di una regione supera la soglia del primo livello di sconto. Non si applica alcuno sconto a una o più prenotazioni e la tariffa scontata viene applicata alle restanti prenotazioni.
- Sconto completo: l'intero acquisto all'interno di una regione rientra in un livello di sconto e quest'ultimo viene applicato in modo corretto.
- Due tassi di sconto: l'acquisto all'interno di una regione passa da un livello di sconto inferiore a un livello di sconto superiore. Vengono applicati due tassi diversi: una o più prenotazioni alla tariffa scontata inferiore e le restanti prenotazioni alla tariffa scontata superiore.

Passaggio di livello di prezzi

Se il tuo acquisto ti permette di passare a un livello di prezzi scontati, vedrai più voci per tale acquisto: una per la parte dell'acquisto fatturata al prezzo normale e un'altra per la parte dell'acquisto addebitata alla tariffa scontata applicabile.

Il servizio dell'Istanza riservata genera vari ID dell'Istanza riservata perché l'acquisto è passato da un livello non scontato a un livello scontato o da un livello scontato a un altro. È disponibile un ID per ogni insieme di prenotazioni in un livello. Di conseguenza, l'ID restituito dal comando della CLI o dall'operazione API dell'acquisto è differente dall'ID effettivo dei nuovi elementi di Istanze riservate.

Fatturazione consolidata per i livelli di prezzi

Un account di fatturazione consolidata aggrega il valore di listino degli account membri all'interno di una regione. Quando il valore di listino di tutte le Istanze riservate attive per l'account di fatturazione consolidata raggiunge un livello di prezzi di sconto, tutte le Istanze riservate acquistate a partire da questo punto da qualsiasi membro di tale account vengono fatturate a una tariffa scontata (purché il valore di listino per tale account consolidato si mantenga al di sopra della soglia del livello dei prezzi di sconto). Per ulteriori informazioni, consulta Istanze riservate e fatturazione consolidata.

Acquisto di istanze riservate

Per acquistare un'istanza riservata, cerca le offerte di istanze riservate di venditori terzi o di terze parti, modificando i parametri di ricerca fino a trovare la corrispondenza esatta che stai cercando. AWS

Durante la ricerca di elementi di Istanze riservate da acquistare, ricevi un preventivo del costo delle offerte restituite. Quando procedi con l'acquisto, inserisce AWS automaticamente un prezzo limite sul prezzo di acquisto. Il costo totale dei tuoi elementi di Istanze riservate non supererà l'importo riportato nel preventivo.

Se il prezzo aumenta o varia per qualsiasi motivo, l'acquisto non viene completato. Quando acquisti un'istanza riservata di un venditore terzo dall'EC2 Reserved Instance Marketplace, se ci sono offerte simili alla tua scelta ma a un prezzo iniziale inferiore, ti AWS vende le offerte al prezzo iniziale più basso.

Prima di confermare l'acquisto, verifica i dettagli della Istanza riservata che intendi comprare e assicurati che tutti i parametri siano accurati. Dopo aver acquistato un'istanza riservata (da un venditore terzo nel Marketplace di istanze riservate o da AWS), non puoi annullare l'acquisto.

Per acquistare e modificare le istanze riservate, assicurarsi che l'utente disponga delle autorizzazioni appropriate, ad esempio la possibilità di descrivere le zone di disponibilità. Per informazioni, consulta the section called “Utilizzo delle Istanze riservate” (API) o the section called “Utilizzo delle Istanze riservate” (console).

Argomenti

- Scelta di una piattaforma
- Metti in coda il tuo acquisto
- Acquisto di Istanze riservate Standard

- Acquista Istanze riservate modificabili.
- Acquistare dal Marketplace di Istanza riservata
- Visualizzare le Istanze riservate
- Annulla un acquisto in coda
- Rinnovare una Istanza riservata

Scelta di una piattaforma

Amazon EC2 supporta le seguenti piattaforme per le istanze riservate:

- Linux/Unix
- Linux con SQL Server Standard
- Linux con SQL Server Web
- Linux con SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux con HA
- Windows
- Windows con SQL Server Standard
- Windows con SQL Server Web
- Windows con SQL Server Enterprise

Quando si acquista un'Istanza riservata, è necessario scegliere un'offerta per una piattaforma corrispondente al sistema operativo dell'istanza.

Istanze Linux

- Per le distribuzioni SUSE Linux e RHEL, è necessario scegliere offerte per quelle piattaforme specifiche, ad esempio per le piattaforme SUSE Linux o Red Hat Enterprise Linux.
- Per tutte le distribuzioni Linux (tra cui Ubuntu), scegliere un'offerta per la piattaforma Linux/UNIX.
- Se si dispone di una sottoscrizione RHEL esistente, occorre scegliere un'offerta per la piattaforma Linux/UNIX e non un'offerta per la piattaforma Red Hat Enterprise Linux.

Istanze Windows

- Per Windows con SQL Standard, Windows con SQL Server Enterprise e Windows con SQL Server Web, è necessario scegliere le offerte specifiche per tali piattaforme.
- Per tutte le altre versioni Windows, scegliere un'offerta per la piattaforma Windows.

> **Note**
>
> Ubuntu Pro non è disponibile come istanza riservata. Per risparmi significativi rispetto ai prezzi delle istanze on demand, ti consigliamo di utilizzare Ubuntu Pro con Savings Plans. Per ulteriori informazioni, consulta la Guida per l'utente dei Savings Plans.

> **Important**
>
> Se si prevede di acquistare un'istanza riservata da applicare a un'istanza on demand che è stata avviata da un'AMI di Marketplace AWS , controllare prima il campo `PlatformDetails` dell'AMI. Il campo `PlatformDetails` indica quale Istanza riservata acquistare. I dettagli della piattaforma dell'AMI devono corrispondere alla piattaforma dell'Istanza riservata, in caso contrario l'Istanza riservata non verrà applicata all'Istanza on demand. Per informazioni su come visualizzare i dettagli della piattaforma dell'AMI, consulta Comprendere le informazioni di fatturazione AMI.

Metti in coda il tuo acquisto

Per impostazione predefinita, quando si acquista una Istanza riservata, l'acquisto viene effettuato immediatamente. In alternativa, puoi accodare gli acquisti per una data e ora nel futuro. Ad esempio, puoi accodare un acquisto per l'ora approssimativa in cui un Istanza riservata esistente scade. Questo garantisce copertura continua.

Puoi accodare acquisti per Istanze riservate regionale, ma non per Istanze riservate o Istanze riservate zonale da altri venditori. Puoi mettere in coda un acquisto con fino a tre anni di anticipo. Alla data e ora pianificati, l'acquisto viene eseguito utilizzando il metodo di pagamento predefinito. Al termine del pagamento, viene applicato il vantaggio di fatturazione.

Nella console Amazon EC2 puoi visualizzare gli acquisti messi in coda. Lo stato degli acquisti accodati è queued (in coda). Puoi annullare un acquisto messo in coda in qualsiasi momento prima dell'ora pianificata. Per informazioni dettagliate, vedi Annulla un acquisto in coda.

Acquisto di Istanze riservate Standard

Puoi acquistare elementi di Istanze riservate standard in una zona di disponibilità specifica e ottenere una prenotazione di capacità. In alternativa, puoi fare a meno della prenotazione di capacità e acquistare una Istanza riservata standard regionale.

New console

Per acquistare Istanze riservate standard tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate), e quindi selezionare Purchase Istanze riservate (Acquista elementi di &ris;).
3. Per Offering Class (Classe di offerta), scegliere Standard per visualizzare le Istanze riservate standard.
4. Per acquistare una prenotazione di capacità, attivare Only show offerings that reserve capacity (Mostra solo le offerte che prenotano capacità) nell'angolo in alto a destra della schermata di acquisto. Quando si attiva questa impostazione, viene visualizzato il campo Availability Zone (Zona di disponibilità).

   Per acquistare una Istanza riservata regionale, disattivare questa impostazione. Quando si disattiva questa impostazione, il campo Availability Zone (Zona di disponibilità) scompare.
5. Selezionare altre configurazioni secondo necessità e poi scegliere Search (Cerca).
6. Per ciascuna Istanza riservata che si desidera acquistare, immettere la quantità desiderata e scegliere Add to Cart (Aggiungi al carrello).

   Per acquistare un'istanza riservata standard dal Marketplace delle istanze riservate, cercare 3rd Party (Terza parte) nella colonna Seller (Venditore) nei risultati della ricerca. La colonna Term (Termine) mostra termini non standard. Per ulteriori informazioni, consulta Acquistare dal Marketplace di Istanza riservata.
7. Per visualizzare un riepilogo delle Istanze riservate selezionate, scegliere View Cart (Visualizza carrello).
8. Se Order on (Ordina il) è Now (Ora), l'acquisto viene completato immediatamente dopo aver scelto Order all (Ordina tutto). Per mettere in corda un acquisto, scegli Now (Ora) e seleziona

una data. Puoi selezionate una data diversa per ogni offerta idonea nel carrello. L'acquisto viene messo in coda fino alle 00:00 UTC della data selezionata.

9. Per completare l'ordine, scegliere Order all (Ordina tutto).

   Se, al momento dell'ordine, ci sono offerte simili alla tua scelta ma con un prezzo inferiore, ti AWS vende le offerte al prezzo inferiore.

10. Scegliere Close (Chiudi).

    Nella colonna State (Stato) viene mostrato lo stato dell'ordine. Una volta completato l'ordine, il valore State (Stato) cambia da `Payment-pending` a `Active`. Quando l'Istanza riservata è `Active`, è pronta per l'uso.

> **Note**
>
> Se lo stato è impostato su`Retired`, è possibile che il AWS pagamento non sia stato ricevuto.

Old console

Per acquistare Istanze riservate standard tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate), e quindi selezionare Purchase Istanze riservate (Acquista elementi di &ris;).
3. Per Offering Class (Classe di offerta), scegliere Standard per visualizzare le Istanze riservate standard.
4. Per acquistare una prenotazione di capacità, scegliere Only show offerings that reserve capacity (Mostra solo le offerte che prenotano capacità) nell'angolo in alto a destra della schermata di acquisto. Per acquistare un'Istanza riservata regionale, lasciare la casella di controllo deselezionata.
5. Selezionare altre configurazioni secondo necessità e scegliere Search (Cerca).

   Per acquistare un'istanza riservata standard dal Marketplace delle istanze riservate, cercare 3rd Party (Terza parte) nella colonna Seller (Venditore) nei risultati della ricerca. La colonna Term (Termine) mostra termini non standard.

6. Per ciascuna Istanza riservata che si desidera acquistare, immettere la quantità e scegliere Add to Cart (Aggiungi al carrello).
7. Per visualizzare un riepilogo delle Istanze riservate selezionate, scegliere View Cart (Visualizza carrello).
8. Se Order On (Ordina il) è impostata su Now (Ora), l'acquisto viene completato immediatamente. Per mettere in corda un acquisto, scegli Now (Ora) e seleziona una data. Puoi selezionate una data diversa per ogni offerta idonea nel carrello. L'acquisto viene messo in coda fino alle 00:00 UTC della data selezionata.
9. Per completare l'ordine, scegliere Order (Ordina).

   Se, al momento dell'ordine, ci sono offerte simili alla tua scelta ma con un prezzo inferiore, ti AWS vende le offerte al prezzo inferiore.
10. Scegliere Close (Chiudi).

    Nella colonna State (Stato) viene mostrato lo stato dell'ordine. Una volta completato l'ordine, il valore State (Stato) cambia da `payment-pending` a `active`. Quando l'Istanza riservata è `active`, è pronta per l'uso.

> **Note**
>
> Se lo stato è impostato su`retired`, è possibile che il AWS pagamento non sia stato ricevuto.

Per acquistare un'istanza riservata standard utilizzando il AWS CLI

1. Trova le istanze riservate disponibili utilizzando il describe-reserved-instances-offeringscomando. Specificare `standard` per far sì che il parametro `--offering-class` restituisca solo Istanze riservate standard. È possibile applicare parametri aggiuntivi per restringere i risultati. Ad esempio, se si desidera acquistare un'Istanza riservata `t2.large` regionale con tenancy predefinita per `Linux/UNIX` per un periodo di un solo anno:

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
```

```
    --filters Name=duration,Values=31536000 Name=scope,Values=Region
```

Per trovare istanze riservate solo sul Marketplace delle istanze riservate, utilizza il filtro `marketplace` e non specificare una durata nella richiesta, dal momento che il termine potrebbe essere inferiore a 1 o 3 anni.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=marketplace,Values=true
```

Una volta individuata un'Istanza riservata che soddisfi le proprie esigenze, prendere nota dell'ID dell'offerta. Per esempio:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Usa il purchase-reserved-instances-offeringcomando per acquistare la tua istanza riservata. È necessario specificare l'ID dell'offerta dell'Istanza riservata ottenuto nella fase precedente nonché il numero di istanze per la prenotazione.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Per impostazione predefinita, l'acquisto viene completato immediatamente. In alternativa, per mettere in coda l'acquisto, aggiungere il seguente parametro alla chiamata precedente.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Usa il describe-reserved-instancescomando per ottenere lo stato della tua istanza riservata.

```
aws ec2 describe-reserved-instances
```

In alternativa, usa i seguenti AWS Tools for Windows PowerShell comandi:

- Get-EC2ReservedInstancesOffering

- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Al termine dell'acquisto, se disponi già di un'istanza in esecuzione che coincide con le specifiche dell'Istanza riservata, il vantaggio di fatturazione viene applicato immediatamente. Non è necessario riavviare le tue istanze. Se non hai un'istanza in esecuzione idonea, avvia un'istanza e assicurati di soddisfare le stesse policy specificate per l'Istanza riservata. Per ulteriori informazioni, consulta Usa le tue Istanze riservate.

Per esempi della modalità di applicazione delle Istanze riservate alle istanze in esecuzione, consulta Applicazione degli elementi di Istanze riservate.

Acquista Istanze riservate modificabili.

Puoi acquistare elementi di Istanze riservate modificabili in una zona di disponibilità specifica e ottenere una prenotazione di capacità. In alternativa, puoi fare a meno della prenotazione di capacità e acquistare una Istanza riservata modificabile regionale.

New console

Per acquistare Istanze riservate modificabili tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate), e quindi selezionare Purchase Istanze riservate (Acquista elementi di &ris;).
3. Per Offering Class (Classe di offerta), scegliere Convertible (Convertibile) per visualizzare le Istanze riservate modificabili.
4. Per acquistare una prenotazione di capacità, attivare Only show offerings that reserve capacity (Mostra solo le offerte che prenotano capacità) nell'angolo in alto a destra della schermata di acquisto. Quando si attiva questa impostazione, viene visualizzato il campo Availability Zone (Zona di disponibilità).

   Per acquistare una Istanza riservata regionale, disattivare questa impostazione. Quando si disattiva questa impostazione, il campo Availability Zone (Zona di disponibilità) scompare.
5. Selezionare altre configurazioni secondo necessità e scegliere Search (Cerca).
6. Per ciascuna Istanza riservata modificabile che si desidera acquistare, immettere la quantità e scegliere Add to Cart (Aggiungi al carrello).

7. Per visualizzare un riepilogo della selezione, scegliere View Cart (Visualizza carrello).
8. Se Order on (Ordina il) è Now (Ora), l'acquisto viene completato immediatamente dopo aver scelto Order all (Ordina tutto). Per mettere in corda un acquisto, scegli Now (Ora) e seleziona una data. Puoi selezionate una data diversa per ogni offerta idonea nel carrello. L'acquisto viene messo in coda fino alle 00:00 UTC della data selezionata.
9. Per completare l'ordine, scegliere Order all (Ordina tutto).

   Se, al momento dell'ordine, ci sono offerte simili alla tua scelta ma con un prezzo inferiore, ti AWS vende le offerte al prezzo inferiore.
10. Scegliere Close (Chiudi).

    Nella colonna State (Stato) viene mostrato lo stato dell'ordine. Una volta completato l'ordine, il valore State (Stato) cambia da `Payment-pending` a `Active`. Quando l'Istanza riservata è `Active`, è pronta per l'uso.

> **Note**
>
> Se lo stato è impostato su`Retired`, è possibile che il AWS pagamento non sia stato ricevuto.

Old console

Per acquistare Istanze riservate modificabili tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate), e quindi selezionare Purchase Istanze riservate (Acquista elementi di &ris;).
3. Per Offering Class (Classe di offerta), scegliere Convertible (Convertibile) per visualizzare le Istanze riservate modificabili.
4. Per acquistare una prenotazione di capacità, scegliere Only show offerings that reserve capacity (Mostra solo le offerte che prenotano capacità) nell'angolo in alto a destra della schermata di acquisto. Per acquistare un'Istanza riservata regionale, lasciare la casella di controllo deselezionata.
5. Selezionare altre configurazioni secondo necessità e scegliere Search (Cerca).

6. Per ciascuna Istanza riservata modificabile che si desidera acquistare, immettere la quantità e scegliere Add to Cart (Aggiungi al carrello).
7. Per visualizzare un riepilogo della selezione, scegliere View Cart (Visualizza carrello).
8. Se Order On (Ordina il) è impostata su Now (Ora), l'acquisto viene completato immediatamente. Per mettere in corda un acquisto, scegli Now (Ora) e seleziona una data. Puoi selezionate una data diversa per ogni offerta idonea nel carrello. L'acquisto viene messo in coda fino alle 00:00 UTC della data selezionata.
9. Per completare l'ordine, scegliere Order (Ordina).

   Se, al momento dell'ordine, ci sono offerte simili alla tua scelta ma con un prezzo inferiore, ti AWS vende le offerte al prezzo inferiore.
10. Scegliere Close (Chiudi).

    Nella colonna State (Stato) viene mostrato lo stato dell'ordine. Una volta completato l'ordine, il valore State (Stato) cambia da `payment-pending` a `active`. Quando l'Istanza riservata è `active`, è pronta per l'uso.

> **Note**
>
> Se lo stato è impostato su`retired`, è possibile che il AWS pagamento non sia stato ricevuto.

Per acquistare un'istanza riservata convertibile utilizzando il AWS CLI

1. Trova le istanze riservate disponibili utilizzando il describe-reserved-instances-offeringscomando. Specificare `convertible` per far sì che il parametro `--offering-class` restituisca solo Istanze riservate modificabili. È possibile applicare parametri aggiuntivi per restringere i risultati, ad esempio se si desidera acquistare un'Istanza riservata`t2.large` regionale con una tenancy predefinita per `Linux/UNIX`:

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class convertible \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=scope,Values=Region
```

Una volta individuata un'Istanza riservata che soddisfi le proprie esigenze, prendere nota dell'ID dell'offerta. Per esempio:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Usa il purchase-reserved-instances-offeringcomando per acquistare la tua istanza riservata. È necessario specificare l'ID dell'offerta dell'Istanza riservata ottenuto nella fase precedente nonché il numero di istanze per la prenotazione.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Per impostazione predefinita, l'acquisto viene completato immediatamente. In alternativa, per mettere in coda l'acquisto, aggiungere il seguente parametro alla chiamata precedente.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Usa il describe-reserved-instancescomando per ottenere lo stato della tua istanza riservata.

```
aws ec2 describe-reserved-instances
```

In alternativa, usa i seguenti AWS Tools for Windows PowerShell comandi:

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Se disponi di un'istanza in esecuzione che coincide con le specifiche dell'Istanza riservata, il vantaggio di fatturazione viene immediatamente applicato. Non è necessario riavviare le tue istanze. Se non hai un'istanza in esecuzione idonea, avvia un'istanza e assicurati di soddisfare le stesse policy specificate per l'Istanza riservata. Per ulteriori informazioni, consulta Usa le tue Istanze riservate.

Per esempi della modalità di applicazione delle Istanze riservate alle istanze in esecuzione, consulta Applicazione degli elementi di Istanze riservate.

Acquistare dal Marketplace di Istanza riservata

Puoi acquistare le istanze riservate da venditori di terza parte che non ne hanno più bisogno nel Marketplace delle istanze riservate. È possibile farlo utilizzando la console Amazon EC2 o uno strumento a riga di comando. Il processo è simile all'acquisto di istanze riservate da AWS. Per ulteriori informazioni, consulta Acquisto di Istanze riservate Standard.

Esistono alcune differenze tra le istanze riservate acquistate nel Reserved Instance Marketplace e le istanze riservate acquistate direttamente da: AWS

- Scadenza - Le istanze riservate acquistate da venditori di terza parte hanno una validità residua inferiore a quella standard. Termini standard completi a partire AWS dalla validità di uno o tre anni.
- Prezzo iniziale - Le istanze riservate di terza parte possono essere vendute a prezzi iniziali diversi. Le tariffe di utilizzo o ricorrenti sono del tutto identiche a quelle stabilite al momento dell'acquisto originale delle istanze riservate da AWS.
- Tipi di istanze riservate - Dal Marketplace delle istanze riservate è possibile acquistare solo le istanze riservate Standard di Amazon EC2. Le istanze riservate convertibili, Amazon RDS e le istanze ElastiCache riservate Amazon non sono disponibili per l'acquisto sul Reserved Instance Marketplace.

Le tue informazioni di base vengono condivise con il venditore, ad esempio il codice postale e le informazioni relative al paese.

Tali informazioni consentono al venditore di calcolare tutte le imposte destinate al governo applicabili alle transazioni (come l'imposta sulle vendite o l'imposta sul valore aggiunto). Vengono comunicate come report di pagamento. In rari casi, AWS potresti dover fornire al venditore il tuo indirizzo e-mail, in modo che possa contattarti in merito a domande relative alla vendita (ad esempio, domande fiscali).

Per ragioni simili, AWS condivide il nome della persona giuridica del venditore sulla fattura di acquisto dell'acquirente. Se hai bisogno di informazioni aggiuntive sul venditore, per motivi fiscali o ragioni correlate, contatta AWS Support.

Visualizzare le Istanze riservate

È possibile visualizzare le Istanze riservate acquistate utilizzando la console Amazon EC2 o uno strumento a riga di comando.

Per visualizzare elementi di Istanze riservate nella console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Sono elencate le tue Istanze riservate in coda, attive e ritirate. Nella colonna State (Stato) viene visualizzato lo stato.
4. Per i venditori nel Marketplace delle istanze riservate, nella scheda My Listings (I miei elenchi) viene visualizzato lo stato di una prenotazione elencata nel Marketplace delle istanze riservate. Per ulteriori informazioni, consulta Stato dell'elenco d'Istanza riservata.

Per visualizzare gli elementi di Istanze riservate utilizzando la riga di comando

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance(Strumenti per Windows PowerShell)

Annulla un acquisto in coda

Puoi mettere in coda un acquisto con fino a tre anni di anticipo. Puoi annullare un acquisto messo in coda in qualsiasi momento prima dell'ora pianificata.

New console

Per annullare un acquisto in coda

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Selezionare una o più Istanze riservate.
4. Scegliere Actions (Operazioni), Delete Queued Reserved Instances (Elimina istanze riservate in coda).
5. Quando viene richiesta la conferma, scegliere Delete (Elimina) e quindi Close (Chiudi).

Old console

Per annullare un acquisto in coda

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Selezionare una o più Istanze riservate.
4. Scegliere Actions (Operazioni), Delete Queued Reserved Instances (Elimina istanze riservate in coda).
5. Quando viene richiesta la conferma, selezionare Yes, Delete (Sì, elimina).

Per annullare un acquisto in coda utilizzando la riga di comando

- delete-queued-reserved-instances (AWS CLI)
- Remove-EC2QueuedReservedInstance(Strumenti per Windows PowerShell)

Rinnovare una Istanza riservata

È possibile rinnovare una Istanza riservata prima che sia programmata per la scadenza. Rinnovando una Istanza riservata viene messo in coda l'acquisto di una Istanza riservata con la stessa configurazione fino alla scadenza della Istanza riservata corrente.

New console

Come rinnovare una Istanza riservata utilizzando un acquisto in coda

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Selezionare l'Istanza riservata da rinnovare.
4. Selezionare Actions (Operazioni), Renew Reserved Instances (Rinnova istanze riservate).
5. Per completare l'ordine, scegliere Order all (Ordina tutto), quindi Close (Chiudi).

Old console

Come rinnovare una Istanza riservata utilizzando un acquisto in coda

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Selezionare l'Istanza riservata da rinnovare.
4. Selezionare Actions (Operazioni), Renew Reserved Instances (Rinnova istanze riservate).
5. Per completare l'ordine, scegliere Order (Ordina).

Vendita nel Marketplace delle istanze riservate

Il Marketplace delle istanze riservate è una piattaforma che supporta la vendita di istanze riservate standard inutilizzate di clienti AWS e di terza parte, con durata e opzioni di prezzi diverse. Ad esempio, potresti voler vendere istanze riservate dopo aver spostato le istanze in una nuova AWS regione, essere passato a un nuovo tipo di istanza, aver terminato i progetti prima della scadenza del termine, quando le esigenze aziendali cambiano o se disponi di capacità non necessaria.

Fino a quando le istanze riservate saranno elencate nel Marketplace delle istanze riservate, saranno disponibili per potenziali acquirenti. Tutti gli elementi di Istanze riservate sono raggruppati in base alla durata del periodo residuo e del prezzo orario.

Per soddisfare la richiesta di un acquirente di acquistare un'istanza riservata di un venditore terzo tramite l'EC2 Reserved Instance Marketplace, vende AWS innanzitutto l'istanza riservata con il prezzo iniziale più basso nel raggruppamento specificato. Quindi, AWS vende l'istanza riservata al prezzo successivo più basso, fino a quando l'intero ordine dell'acquirente non viene evaso. AWS quindi elabora le transazioni e trasferisce la proprietà delle istanze riservate all'acquirente.

Rimani proprietario della Istanza riservata finché non viene venduta. Una volta conclusa la vendita, non disporrai più della prenotazione di capacità e delle tariffe ricorrenti scontate. Se continui a utilizzare l'istanza, AWS addebita il prezzo on demand a partire dal momento in cui l'istanza riservata è stata venduta.

Per vendere istanze riservate inutilizzate sul Marketplace delle istanze riservate, è necessario soddisfare determinati criteri di idoneità.

Per informazioni sull'acquisto di istanze riservate nel Marketplace delle istanze riservate, consulta Acquistare dal Marketplace di Istanza riservata.

Indice

- Ciclo di vita di un elenco
- Dopo la vendita della Istanza riservata
- Ricezione dei pagamenti
- Informazioni condivise con l'acquirente

Restrizioni e limitazioni

Prima di poter vendere le prenotazioni inutilizzate, è necessario registrarsi come venditore nel Marketplace delle istanze riservate. Per informazioni, consulta Registrati come venditore.

Le seguenti limitazioni e restrizioni si applicano alla vendita di elementi di Istanze riservate:

- Sul Marketplace delle istanze riservate è possibile vendere solo le istanze riservate regionali e zonali standard di Amazon EC2.
- Sul Marketplace delle istanze riservate non è possibile vendere le istanze riservate modificabili di Amazon EC2.
- Le istanze riservate per altri AWS servizi, come Amazon RDS e Amazon ElastiCache, non possono essere vendute nel Reserved Instance Marketplace.
- L'Istanza riservata standard deve avere almeno un mese di validità residua.
- Non è possibile vendere una Istanza riservata standard in una regione disabilitata per impostazione predefinita.
- Il prezzo minimo consentito nel Marketplace delle istanze riservate è 0 USD.
- Nel Marketplace delle istanze riservate puoi vendere istanze riservate senza pagamento anticipato, con pagamento anticipato parziale o con pagamento anticipato completo, a condizione che siano attive nel tuo account per almeno 30 giorni. Inoltre, se è previsto un pagamento anticipato su un'istanza riservata, questa può essere venduta solo dopo aver ricevuto il pagamento AWS anticipato.
- Non è possibile modificare l'inserzione direttamente nel Marketplace delle istanze riservate. Tuttavia, puoi farlo annullandolo e successivamente creandone un altro con nuovi parametri. Per informazioni, consulta Dare un prezzo alla Istanze riservate. Puoi anche modificare gli elementi di Istanze riservate prima di includerli nell'elenco. Per informazioni, consulta Modificare le Istanze riservate.
- AWS addebita una commissione di servizio pari al 12% del prezzo iniziale totale di ogni istanza riservata standard venduta nel Reserved Instance Marketplace. Il prezzo iniziale è il prezzo che il venditore addebita per la Istanza riservata standard.

- Quando ti registri come venditore, la banca specificata deve avere un indirizzo negli Stati Uniti. Per maggiori informazioni, consulta Requisiti aggiuntivi del venditore per i prodotti a pagamento in Guida per i venditori di Marketplace AWS .
- I clienti di Amazon Web Services India Private Limited (AWS India) non possono vendere istanze riservate nel Reserved Instance Marketplace anche se dispongono di un conto bancario negli Stati Uniti. Per ulteriori informazioni, consulta Quali sono le differenze tra gli account Account AWS e gli account AWS indiani?

Registrati come venditore

> **Note**
>
> Solo loro Utente root dell'account AWS possono registrare un account come venditore.

Per vendere nel Marketplace delle istanze riservate, devi prima registrarti come venditore. Durante la registrazione, è necessario fornire le informazioni riportate di seguito:

- Informazioni bancarie: èAWS necessario disporre delle tue informazioni bancarie per poter erogare i fondi raccolti quando vendi le tue prenotazioni. La banca specificata deve avere un indirizzo negli Stati Uniti. Per ulteriori informazioni, consulta Conto bancario per il pagamento.
- Informazioni fiscali — Tutti i venditori devono completare un questionario fiscale per determinare gli eventuali obblighi fiscali. Per ulteriori informazioni, consulta Informazioni fiscali.

Dopo aver AWS ricevuto la registrazione come venditore completata, riceverai un'email di conferma della registrazione e ti informa che puoi iniziare a vendere nel Reserved Instance Marketplace.

Conto bancario per il pagamento

AWS devi avere i tuoi dati bancari per poter erogare i fondi raccolti quando vendi l'istanza riservata. La banca specificata deve avere un indirizzo negli Stati Uniti. Per maggiori informazioni, consulta Requisiti aggiuntivi del venditore per i prodotti a pagamento in Guida per i venditori di Marketplace AWS .

Per registrare un conto bancario predefinito per pagamenti

1. Aprire la pagina per la Registrazione dei venditori nel Marketplace delle istanze riservate e accedere utilizzando le credenziali AWS .

2. Nella pagina Manage Bank Account (Gestisci conto bancario), fornire le informazioni seguenti sulla banca tramite cui ricevere il pagamento:

   - Nome del titolare del conto bancario
   - Numero di routing
   - Numero conto
   - Tipo di conto bancario

   > **Note**
   >
   > Se si sta utilizzando un conto bancario aziendale, viene richiesto l'invio delle informazioni sul conto bancario tramite fax (1-206-765-3424).

Dopo la registrazione, il conto bancario fornito viene impostato come predefinito, in attesa di verifica con la banca. La verifica di un nuovo conto bancario può richiedere fino a due settimane, durante le quali non è possibile ricevere alcun pagamento. In caso di conto costituito, i pagamenti richiedono in genere circa due giorni.

Per modificare il conto bancario predefinito per il pagamento

1. Nella pagina per la Registrazione dei venditori nel Marketplace delle istanze riservate, accedere con l'account utilizzato per la registrazione.
2. Nella pagina Manage Bank Account (Gestisci conto bancario), aggiungere un nuovo conto bancario o modificare il conto predefinito secondo necessità.

Informazioni fiscali

La vendita di elementi di Istanze riservate potrebbe essere soggetta a un'imposta basata sulle transazioni, come un'imposta sulle vendite o un'imposta sul valore aggiunto. È necessario consultare il reparto fiscale, legale, finanziario o contabile dell'azienda per stabilire se vi sono imposte basate sulle transazioni applicabili. Sei tenuto a riscuotere e inviare tali imposte sulle transazioni alla opportuna autorità fiscale.

Come parte del processo di registrazione dei venditori, è necessario completare un questionario fiscale nel portale di registrazione dei venditori. Il questionario raccoglie le tue informazioni fiscali

e popola il modulo IRS W-9, W-8BEN o W-8BEN-E utilizzato per determinare gli eventuali obblighi fiscali.

Le informazioni di natura fiscale indicate come parte del questionario fiscale possono differire a seconda che operi in forma individuale o come impresa e che l'azienda sia una persona fisica o giuridica statunitense o meno. Quando si compila il questionario fiscale, è necessario tenere presente quanto segue:

- Le informazioni fornite da AWS, incluse le informazioni in questo argomento, non costituiscono consulenza fiscale, legale o professionale di altro tipo. Per scoprire in che modo i requisiti di dichiarazione IRS possono influire sull'azienda, o in caso di altre domande, contattare il proprio consulente fiscale, legale o di altra natura professionale.
- Per soddisfare tali requisiti nella massima misura possibile, rispondere a tutte le domande e inserire tutte le informazioni richieste durante il questionario.
- Controllare le risposte. Evitare errori ortografici o di inserire numeri di identificazione fiscale errati. Ciò potrebbe comportare l'invalidazione del modulo fiscale.

In base alle risposte del questionario fiscale e alle soglie di dichiarazione dell'IRS, Amazon può presentare il modulo 1099-K, che invia per posta entro il 31 gennaio dell'anno seguente a quello in cui il tuo conto fiscale ha raggiunto i livelli di soglia. Ad esempio, se il conto raggiunge la soglia nel 2018, il modulo 1099-K viene inviato entro il 31 gennaio 2019.

Per ulteriori informazioni sui requisiti IRS e sul modulo 1099-K, consulta il sito Web IRS.

Dare un prezzo alla Istanze riservate

Durante la definizione del prezzo per le istanze riservate, considera quanto segue:

- Costo anticipato - Il costo anticipato è l'unica tariffa che puoi specificare per l'Istanza riservata che stai vendendo. Il costo anticipato è l'unico singolo addebito che l'acquirente paga quando acquista un'Istanza riservata.

  Poiché il valore delle istanze riservate diminuisce nel tempo, per impostazione predefinita, è AWS possibile impostare prezzi in modo che diminuiscano con incrementi uguali mese dopo mese. Tuttavia, puoi stabilire diversi prezzi iniziali in base a quando viene venduta la prenotazione. Ad esempio se l'Istanza riservata ha una validità residua di nove mesi, puoi specificare l'importo che accetteresti se un cliente acquistasse tale Istanza riservata con una validità di nove mesi. Puoi stabilire un altro prezzo con una validità di cinque mesi e un altro ancora con un mese di validità.

Il prezzo minimo consentito nel Marketplace delle istanze riservate è 0 USD.

- Limiti - I seguenti limiti per la vendita di istanze riservate si applicano per tutta la durata della tua Account AWS. Non sono limiti annuali.
  - Puoi effettuare vendite fino a 50.000 USD in Istanze riservate.
  - Puoi effettuare vendite fino a 5.000 USD in Istanze riservate.

  Questi limiti in genere non possono essere aumentati, ma verranno valutati di volta in volta, se richiestocase-by-case . Per richiedere l'incremento di un limite, completa il modulo di incremento dei limiti di servizio. Per Tipo di limite, scegli EC2 Reserved Instance Sales.
- Impossibile modificare - Non puoi modificare l'elenco direttamente. Tuttavia, puoi farlo annullandolo e successivamente creandone un altro con nuovi parametri.
- Cancellazione - Puoi annullare il tuo elenco in qualsiasi momento purché il relativo stato sia `active`. Non puoi annullare l'elenco se già oggetto di corrispondenza o in corso di elaborazione per una vendita. In caso di annullamento di un elenco contenente alcune istanze oggetto di corrispondenza, saranno rimosse da tale elenco solo le istanze non oggetto di corrispondenza.

Elencare le Istanze riservate

In qualità di venditore registrato, puoi decidere di vendere uno o più elementi di Istanze riservate. Puoi decidere di venderli tutti in un elenco o in più parti. Inoltre, puoi elencare elementi di Istanze riservate con qualsiasi configurazione di tipo di istanza, piattaforma e ambito.

La console determina un prezzo consigliato. Verifica le offerte che corrispondono alle Istanza riservata e mette in corrispondenza quella con il prezzo più basso. Altrimenti, calcola un prezzo consigliato in base al costo delle Istanza riservata per il tempo restante. Se il valore calcolato è inferiore a $1,01, il prezzo consigliato è $1,01.

Se annulli l'elenco e una parte di esso è già stato venduto, l'annullamento non viene applicato alla parte già venduta. Solo la parte invenduta dell'inserzione non è più disponibile nel Marketplace delle istanze riservate.

Per elencare un'istanza riservata nel Reserved Instance Marketplace utilizzando il AWS Management Console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).

3. Seleziona le Istanze riservate da elencare e scegli Actions (Operazioni), Sell Reserved Instances (Vendi le Istanze riservate).
4. Nella pagina Configure Your Istanza riservata Listing (Configura l'elenco di) impostare il numero di istanze da vendere e il prezzo iniziale per la validità residua nelle colonne corrispondenti. Per vedere in che modo cambia il valore della prenotazione nel periodo di validità residua, selezionare la freccia accanto alla colonna Months Remaining (Mesi rimanenti).
5. Gli utenti avanzati che desiderano personalizzare i prezzi, possono immettere valori diversi per i mesi successivi. Per tornare al decremento dei prezzi lineare predefinito, scegliere Reset (Reimposta).
6. Al termine della configurazione dell'elenco, scegliere Continue (Continua).
7. Confermare i dettagli dell'elenco nella pagina Confirm Your Istanza riservata Listing (Conferma l'elenco di) e, se non è necessario apportare modifiche, scegliere List Reserved Instance (Elenca istanza riservata).

Per visualizzare gli elenchi nella console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Seleziona l'Istanza riservata elencata e scegli la scheda Le My Listings (I miei elenchi) nella parte inferiore della pagina.

Per gestire le istanze riservate nel Reserved Instance Marketplace utilizzando il AWS CLI

1. Ottieni un elenco delle tue istanze riservate utilizzando il describe-reserved-instancescomando.
2. Annota l'ID dell'istanza riservata che desideri elencare e chiamare create-reserved-instances-listing. È necessario specificare l'ID dell'Istanza riservata, il numero di istanze e il piano dei prezzi.
3. Per visualizzare la tua inserzione, usa il describe-reserved-instances-listingscomando.
4. Per cancellare la tua inserzione, usa il cancel-reserved-instances-listingscomando.

Stato dell'elenco d'Istanza riservata

L'opzione Listing State (Stato elenco) nella scheda My Listings (I miei elenchi) della pagina delle Istanze riservate mostra lo stato corrente degli elenchi:

Le informazioni visualizzate in Listing State (Stato inserzione) riguardano lo stato dell'inserzione nel Marketplace delle istanze riservate. Sono diverse dalle informazioni di stato mostrate nella colonna State (Stato) nella pagina Reserved Instances (Istanze riservate). Le informazioni in State (Stato) riguardano la prenotazione.

- active (attivo) — L'elenco è disponibile per l'acquisto.
- canceled (annullata) - L'inserzione è stata annullata e non è disponibile per l'acquisto nel Marketplace delle istanze riservate.
- closed (chiuso) — L'Istanza riservata non è inclusa nell'elenco. Un'Istanza riservata potrebbe essere `closed` perché la vendita dell'elenco è stata completata.

Ciclo di vita di un elenco

Quando tutte le istanze in elenco corrispondono e risultano vendute, la scheda My Listings (I miei elenchi) mostra una corrispondenza tra Total instance count (Conteggio totale delle istanze) e il conteggio elencato in Sold (Venduto). Inoltre, non c'è alcuna istanza Available (Disponibile) per l'elenco e il suo Status (Stato) è `closed`.

Quando viene venduta solo una parte della tua inserzione, AWS elimina le istanze riservate dall'inserzione e crea un numero di istanze riservate pari alle istanze riservate rimanenti nel conteggio. Pertanto, l'ID elenco e l'elenco che rappresenta, che ora include meno prenotazioni per la vendita, è ancora attivo.

Eventuali vendite future di elementi di Istanze riservate in questo elenco sono elaborate in questo modo. Quando tutte le istanze riservate dell'inserzione vengono vendute, AWS contrassegna l'inserzione come. `closed`

Ad esempio, puoi creare un elenco ID di elenco di Istanze riservate 5ec28771-05ff-4b9b-aa31-9e57dexample con un conteggio pari a 5.

La scheda My Listings (I miei elenchi) nella pagina della console Reserved Instance (Istanza riservata) visualizza l'elenco in questo modo:

ID di elenco di Istanza riservata 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count (Conteggio totale delle prenotazioni) = 5
- Sold (Venduto) = 0
- Available (Disponibile) = 5

- Status (Stato) = active (attivo)

Un acquirente compra due delle prenotazioni, lasciando un conteggio di tre prenotazioni ancora disponibili per la vendita. A causa di questa vendita parziale, AWS crea una nuova prenotazione contando fino a tre per rappresentare le prenotazioni rimanenti ancora in vendita.

Questo è l'aspetto che avrebbe l'elenco nella scheda My Listings (I miei elenchi):

ID di elenco di Istanza riservata 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count (Conteggio totale delle prenotazioni) = 5
- Sold (Venduto) = 2
- Available (Disponibile) = 3
- Status (Stato) = active (attivo)

Se annulli l'elenco e una parte di esso è già stato venduto, l'annullamento non viene applicato alla parte già venduta. Solo la parte invenduta dell'inserzione non è più disponibile nel Marketplace delle istanze riservate.

Dopo la vendita della Istanza riservata

Quando la tua istanza riservata viene venduta, ti AWS invia una notifica via e-mail. Vieni avvisato tramite notifica via e-mail di tutte le attività che si verificano in una giornata. Le attività possono includere la creazione o la vendita di un'inserzione o l' AWS invio di fondi al proprio account.

Per tenere traccia dello stato di un elenco di Istanza riservata nella console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella pagina di navigazione scegli Reserved Instances (Istanze riservate).
3. Scegli la scheda My Listings (I miei elenchi).

   La scheda My Listings (I miei elenchi) contiene il valore Listing State (Stato elenco). Contiene inoltre informazioni su termine, prezzo di listino e suddivisione del numero di istanze disponibili, in attesa, vendute e annullate nell'elenco.

Puoi anche utilizzare il describe-reserved-instances-listingscomando con il filtro appropriato per ottenere informazioni sulle tue inserzioni.

Ricezione dei pagamenti

Non appena AWS riceve fondi dall'acquirente, viene inviato un messaggio all'indirizzo e-mail dell'account del proprietario registrato per l'istanza riservata venduta.

AWS invia un bonifico bancario Automated Clearing House (ACH) sul conto bancario specificato. In genere, questo bonifico viene effettuato in da uno a tre giorni dopo la vendita della Istanza riservata. I pagamenti hanno cadenza giornaliera. Riceverai un'e-mail con le informazioni di pagamento una volta erogati i fondi. Tieni presente che non puoi ricevere pagamenti finché non ricevi una verifica dalla tua AWS banca. Ciò può richiedere fino a due settimane.

L'Istanza riservata venduta continua a comparire quando descrivi le tue Istanze riservate.

Riceverai un rimborso in contanti per le tue istanze riservate tramite bonifico bancario direttamente sul tuo conto bancario. AWS addebita una commissione di servizio pari al 12% del prezzo iniziale totale di ogni istanza riservata venduta nel Reserved Instance Marketplace.

Informazioni condivise con l'acquirente

Quando vendi nel Reserved Instance Marketplace AWS , riporta la ragione sociale della tua azienda sull'estratto conto dell'acquirente in conformità con le normative statunitensi. Inoltre se l'acquirente chiama il AWS Support perché ha la necessità di contattarti per una fattura o per questioni fiscali, AWS potrebbe dover fornire all'acquirente il tuo indirizzo e-mail in modo da contattarti direttamente.

Per motivi simili, il codice fiscale dell'acquirente e le informazioni sul paese vengono fornite al venditore nel report di pagamento. In qualità di venditore, potresti aver bisogno di queste informazioni a corredo di qualsiasi imposta sulle transazioni corrisposta al governo (come l'imposta sulle vendite e l'imposta sul valore aggiunto).

AWS non può offrire consulenza fiscale, ma se il tuo specialista fiscale ritiene che tu abbia bisogno di informazioni aggiuntive specifiche, contatta AWS Support.

Modificare le Istanze riservate

Quando le tue esigenze cambiano, puoi modificare i tuoi elementi di Istanze riservate modificabili o standard e continuare a beneficiare del vantaggio di fatturazione. Puoi modificare gli attributi quali la zona di disponibilità, le dimensioni dell'istanza (nella stessa famiglia di istanze) e l'ambito dell'istanza riservata.

> **Note**
>
> Puoi inoltre scambiare una Istanza riservata modificabile con un'altra Istanza riservata modificabile con una configurazione diversa. Per ulteriori informazioni, consulta Scambiare le Istanze riservate modificabili.

Puoi modificare tutti gli elementi di Istanze riservate o un sottoinsieme di essi. Puoi separare le Istanze riservate originali in due o più Istanze riservate nuove. Ad esempio, se hai una prenotazione per 10 istanze in `us-east-1a` e decidi di spostarne 5 in `us-east-1b`, la richiesta di modifica determina due nuove prenotazioni: una per 5 istanze in `us-east-1a` e un'altra per 5 istanze in `us-east-1b`.

Puoi inoltre unire due o più Istanze riservate in una singola Istanza riservata. Ad esempio, se hai quattro Istanze riservate `t2.small` di un'istanza ciascuna, puoi unirli per creare un'unica Istanza riservata `t2.large`. Per ulteriori informazioni, consulta Supporto per la modifica delle dimensioni dell'istanza.

Dopo la modifica, il vantaggio degli elementi di Istanze riservate viene applicato solo alle istanze corrispondenti ai nuovi parametri. Ad esempio, se cambi la zona di disponibilità di una prenotazione, la prenotazione di capacità e i vantaggi in termini di prezzi vengono automaticamente applicati all'utilizzo dell'istanza nella nuova zona di disponibilità. Le istanze che non coincidono più con i nuovi parametri vengono addebitata alla tariffa on demand a meno che l'account non abbia altre prenotazioni applicabili.

Se la tua richiesta di modifica viene applicata

- La prenotazione modificata diventa effettiva immediatamente e il vantaggio di prezzo viene applicato alle nuove istanze a partire dall'ora della richiesta di modifica. Ad esempio, se modifichi correttamente le prenotazioni alle 21:15, il vantaggio di prezzo si trasferisce alla nuova istanza alle 21:00. È possibile ottenere la data di validità delle istanze riservate modificate utilizzando il describe-reserved-instancescomando.
- La prenotazione originale viene ritirata. La sue data di fine coincide con la data di inizio della nuova prenotazione e la data di fine della nuova prenotazione è la stessa della data di fine della Istanza riservata originale. Se modifichi una prenotazione di tre anni con una validità residua di 16 mesi, la prenotazione modificata risultante è una prenotazione di 16 mesi con la stessa data di fine dell'originale.

- La prenotazione modificata indica un prezzo fisso di 0 USD e non quello della prenotazione originale.
- Il prezzo fisso della prenotazione modificata non influisce sui calcoli del livello di prezzi di sconto applicati al tuo account, che si basano sul prezzo fisso della prenotazione originale.

Se la richiesta di modifica genera un errore, gli elementi di Istanze riservate mantengono la configurazione originale e sono immediatamente disponibili per un'altra richiesta di modifica.

Non è previsto alcun costo per la modifica e non ricevi alcuna fattura nuova.

Puoi modificare le prenotazione alla frequenza che desideri, ma non puoi cambiare o annullare una richiesta di modifica in attesa dopo averla inviata. Dopo che la modifica è stata completata correttamente, puoi inviare un'altra richiesta di modifica per eseguire il rollback di qualsiasi modifica eseguita, se necessario.

Indice

Requisiti e restrizioni per la modifica

Puoi modificare tali attributi nel modo seguente.

Attributo modificabile	Piattaforme supportate	Considerazioni e limitazioni
Cambiare le zone di disponibilità all'interno della stessa regione	Linux e Windows	-
Cambiare l'ambito di applicazione dalla zona di disponibilità alla regione e viceversa	Linux e Windows	Un'istanza riservata zonale viene assegnata a una zona di disponibilità e riserva la capacità in quella zona di

Attributo modificabile	Piattaforme supportate	Considerazioni e limitazioni
		disponibilità. Se cambi l'ambito di applicazione da zona di disponibilità a regione (in altre parole, da zonale a regionale), perdi il vantaggio della prenotazione della capacità. Un'istanza riservata regionale viene assegnata a una regione. Lo sconto dell'Istanza riservata si applica alle istanze in esecuzione in qualsiasi zona di disponibilità di quella regione. Inoltre, lo discount dell'istanza riservata si applica all'utilizzo dell'istanza su tutte le dimensioni della stessa famiglia di istanze selezionata. Se cambi l'ambito di applicazione da regione a zona di disponibilità (in altre parole, da regionale a zonale), perdi la flessibilità della zona di disponibilità e della dimensione dell'istanza (se applicabile). Per ulteriori informazioni, consulta Applicazione degli elementi di Istanze riservate.

Attributo modificabile	Piattaforme supportate	Considerazioni e limitazioni
Cambia la dimensione dell'istanza all'interno della stessa famiglia e generazione di istanze.	Solo Linux/UNIX La flessibilità delle dimensioni delle istanze non è disponibile per Istanze riservate su altre piattaforme, tra le quali Linux con SQL Server Standard, Linux con SQL Server Web, Linux con SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows con SQL Standard, Windows con SQL Server Enterprise e Windows con SQL Server Web.	La prenotazione deve utilizzare la tenancy predefinita. Alcune famiglie di istanze non sono supportate perché non sono disponibili altre dimensioni. Per ulteriori informazioni, consulta Supporto per la modifica delle dimensioni dell'istanza

Requisiti

Amazon EC2 elabora la richiesta di modifica se è disponibile una capacità sufficiente per la nuova configurazione (se applicabile) e se sono soddisfatte le condizioni seguenti:

- Le Istanza riservata non possono essere modificate prima o al momento del relativo acquisto
- La Istanza riservata deve essere attiva
- Non possono esserci richieste di modifica in sospeso
- L'istanza riservata non è più elencata nel Marketplace delle istanze riservate.
- Deve esserci corrispondenza tra il footprint associato alla dimensione dell'istanza della prenotazione originale e la nuova configurazione. Per ulteriori informazioni, consulta Supporto per la modifica delle dimensioni dell'istanza.
- Le Istanze riservate originali sonno tutte Istanze riservate Standard o tutte Istanze riservate modificabili, non alcune di ogni tipo
- Le Istanze riservate originali devono scadere entro lo stesso orario, se sono Istanze riservate Standard
- L'istanza riservata non è un'istanza G4, G4ad, G4dn, G5, G5g, Inf1 o Inf2.

Supporto per la modifica delle dimensioni dell'istanza

È possibile modificare la dimensione dell'istanza di una Istanza riservata se sono soddisfatti i seguenti requisiti.

Requisiti

- La piattaforma è Linux/UNIX.
- Devi selezionare un'altra dimensione di istanza nella stessa famiglia di istanze (indicata da una lettera, ad esempio T) e generazione (indicata da un numero, ad esempio 2).

  Ad esempio, puoi modificare un'istanza riservata da `t2.small` a `t2.large` perché appartengono entrambe alla stessa famiglia e generazione T2. Tuttavia, non è possibile modificare un'istanza riservata da T2 a M2 o da T2 a T3, poiché in entrambi i casi, la famiglia e la generazione dell'istanza di destinazione non sono le stesse di quelle dell'istanza riservata originale.
- Non puoi modificare la dimensione dell'istanza di istanze riservate per le istanze seguenti, poiché ciascuna di queste famiglie di istanze ha una sola dimensione:
  - `t1.micro`
- Non è possibile modificare la dimensione dell'istanza delle istanze riservate per le seguenti combinazioni di famiglia di istanze, generazione e attributo:
  - G4ad
  - G4dn
  - G5
  - G5g
  - Inf1
  - Inf2
- La Istanza riservata originale e quella nuova devono avere la stessa impronta dell'istanza.

Indice

Impronta dimensione istanza

Ciascuna Istanza riservata ha un'impronta associata alla dimensione dell'istanza, determinato dal fattore di normalizzazione della dimensione di istanza e dal numero di istanze nella prenotazione. Quando modifichi le dimensioni di istanza in una Istanza riservata, l'impronta della nuova configurazione deve corrispondere a quella della configurazione originale, altrimenti la richiesta di modifica non viene elaborata.

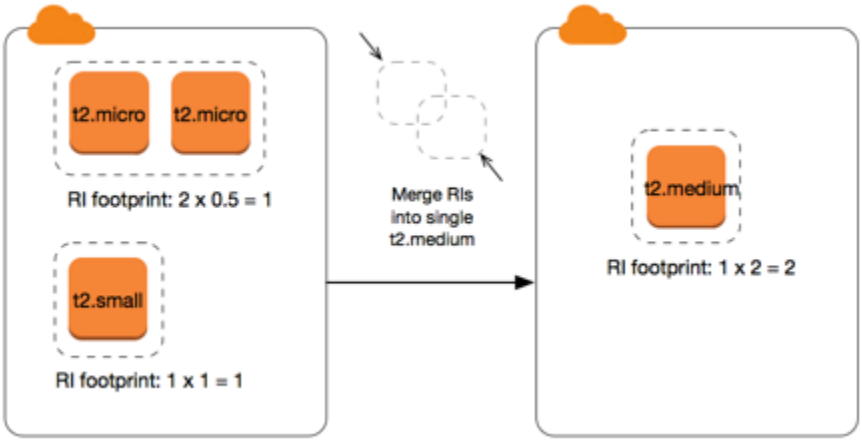
Per calcolare il footprint della dimensione dell'istanza di una Istanza riservata, moltiplica il numero di istanza per il fattore di normalizzazione. Nella console Amazon EC2, il fattore di normalizzazione si misura in unità. Nella tabella seguente viene descritto il fattore di normalizzazione per le dimensioni delle istanze in una famiglia di istanze. Ad esempio, `t2.medium` ha un fattore di normalizzazione 2, quindi una prenotazione per quattro istanze `t2.medium` ha un'impronta di 8 unità.

Dimensioni istanza	Fattore di normalizzazione
nano	0.25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80

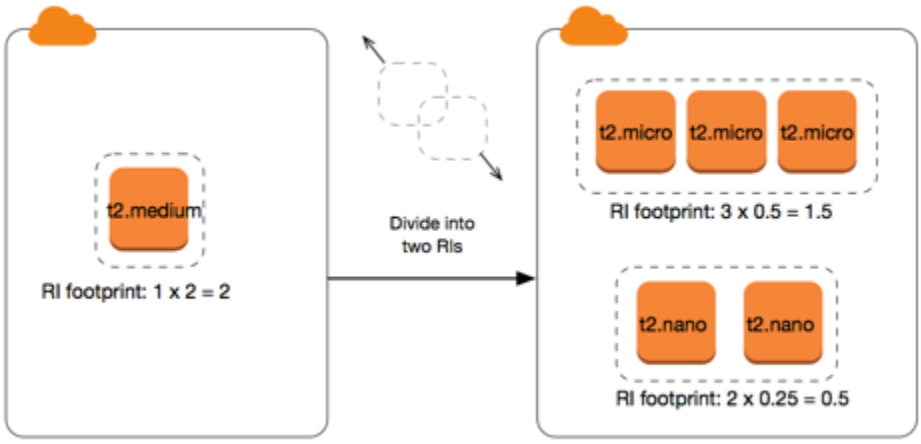
Dimensioni istanza	Fattore di normalizzazione
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Puoi allocare le prenotazioni in diverse dimensioni di istanza nella stessa famiglia di istanze purché l'impronta della dimensione dell'istanza della prenotazione rimanga invariata. Ad esempio, è possibile dividere una prenotazione per un'istanza `t2.large` (1 @ 4 unità) in quattro istanze `t2.small` (4 @ 1 unità). Analogamente, è possibile combinare una prenotazione per quattro istanze `t2.small` in un'unica istanza `t2.large`. Tuttavia, non è possibile modificare la prenotazione per due istanze `t2.small` in un'istanza `t2.large` perché l'impronta della nuova prenotazione (4 unità) è maggiore dell'impronta della prenotazione originale (2 unità).

Nell'esempio seguente si dispone di una prenotazione con due istanze `t2.micro` (1 unità) e una prenotazione con un'istanza `t2.small` (1 unità). Se si uniscono entrambe le prenotazioni a una singola prenotazione con un'istanza `t2.medium` (2 unità), l'impronta della nuova prenotazione equivale all'impronta delle prenotazioni combinate.



Puoi inoltre modificare una prenotazione per dividerla in due o più prenotazioni. Nell'esempio seguente, hai una prenotazione con un'istanza `t2.medium` (2 unità). È possibile dividere la prenotazione in due, una con due istanze `t2.nano` (.5 unità) e l'altra con tre istanze `t2.micro` (1,5 unità).



Fattori di normalizzazione per le istanze bare metal

È possibile modificare una prenotazione con istanze `metal` che utilizzano altre dimensioni all'interno della stessa famiglia di istanze. Analogamente, puoi modificare una prenotazione con varianti diverse da quelle bare metal utilizzando le dimensioni `metal` all'interno della stessa famiglia di istanze. Generalmente, un'istanza bare metal ha la stessa dimensione della più grande dimensione disponibile all'interno della stessa famiglia di istanze. Ad esempio, un'istanza `i3.metal` ha le stesse dimensioni di un'istanza `i3.16xlarge`, quindi hanno lo stesso fattore di normalizzazione.

Nella tabella seguente viene descritto il fattore di normalizzazione per le dimensioni delle istanze bare metal nelle famiglie di istanze con istanze bare metal. Il fattore di normalizzazione per `metal` le istanze dipende dalla famiglia di istanze, a differenza delle altre dimensioni di istanza.

Dimensioni istanza	Fattore di normalizzazione
a1.metal	32
m5zn.metal | x2iezn.metal z1d.metal	96
c6g.metal | c6gd.metal | i3.metal | m6g.metal | m6gd.metal | r6g.metal | r6gd.metal | x2gd.metal	128
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-*.metal	896

Ad esempio, il fattore di normalizzazione di un'istanza `i3.metal` è 128. Se acquisti una Istanza riservata Amazon Linux/Unix con tenancy di default `i3.metal` puoi dividere la prenotazione come segue:

- Una istanza `i3.16xlarge` ha la stessa dimensione di `i3.metal`, quindi il suo fattore di normalizzazione è 128 (128/1). La prenotazione per una istanza `i3.metal` non può essere modificata in una istanza `i3.16xlarge`.
- Una istanza `i3.8xlarge` ha dimensione pari alla metà di `i3.metal`, quindi il suo fattore di normalizzazione è 64 (128/2). La prenotazione per una istanza `i3.metal` non può essere divisa in due istanze `i3.8xlarge`.
- Una istanza `i3.4xlarge` ha dimensione pari ad un quarto di `i3.metal`, quindi il suo fattore di normalizzazione è 32 (128/4). La prenotazione per una istanza `i3.metal` non può essere divisa in quattro istanze `i3.4xlarge`.

Inviare richieste di modifica

Prima di modificare le istanze riservate, assicurati di aver letto le restrizioni applicabili. Prima di modificare la dimensione dell'istanza, calcola l'ingombro totale delle dimensioni dell'istanza delle prenotazioni originali che desideri modificare e assicurati che corrisponda all'ingombro totale delle dimensioni dell'istanza delle nuove configurazioni.

New console

Per modificare le istanze riservate utilizzando il AWS Management Console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella pagina Reserved Instances (Istanze riservate), selezionare una o più Istanze riservate da modificare e scegliere Actions (Azioni), Modify Reserved Instances (Modifica istanze riservate).

   > **Note**
   >
   > Se le Istanze riservate non sono nello stato attivo o non possono essere modificate, l'opzione Modify Istanze riservate (Modifica Istanze riservate) è disabilitata.

3. La prima voce nella tabella di modifica indica gli attributi delle Istanze riservate selezionate e almeno una configurazione di destinazione al di sotto. La colonna Units (unità) mostra il footprint della dimensione dell'istanza totale. Selezionare Add (Aggiungi) per ciascuna nuova configurazione da aggiungere. Modificare gli attributi in base alle esigenze per ogni configurazione.

   - Scope (Ambito di applicazione): scegliere se la configurazione si applica a una zona di disponibilità o all'intera regione.
   - Availability Zone (Zona di disponibilità): scegliere la zona di disponibilità richiesta. Non applicabile agli elementi di Istanze riservate regionali.
   - Tipo di istanza: seleziona il tipo di istanza richiesto. Le configurazioni combinate devono avere un footprint delle dimensioni di istanza pari alle configurazioni originali.
   - Count (Conteggio): specificare il numero di istanze. Per dividere le Istanze riservate in più configurazioni, ridurre il conteggio, scegliere Add (Aggiungi) e specificare un conteggio per la configurazione aggiuntiva. Ad esempio, se si ha una singola configurazione con un conteggio di 10, è possibile impostare il relativo conteggio su 6 e aggiungere una

configurazione con un conteggio di 4. In questo modo, l'Istanza riservata originale viene ritirata dopo l'attivazione della nuova Istanze riservate.

4. Scegliere Continue (Continua).
5. Per confermare le scelte di modifica dopo aver terminato di specificare le configurazioni di destinazione, scegliere Submit Modifications (Invia modifiche).
6. Puoi determinare lo stato della richiesta di modifica osservando la colonna State (Stato) nella schermata delle Istanze riservate. Di seguito sono riportati gli stati possibili.

   - attiva (modifica in sospeso) – Stato della transizione per la Istanze riservate di origine
   - ritirata (modifica in sospeso) – Stato della transizione per la Istanze riservate di origine mentre vengono create le nuove Istanze riservate
   - ritirata – Istanze riservate modificata e sostituita con successo
   - attiva – Una delle seguenti opzioni:
     - Nuovi elementi di Istanze riservate creati da una richiesta di modifica corretta
     - Elementi di Istanze riservate originali dopo una richiesta di modifica errata

Old console

Per modificare le istanze riservate utilizzando il AWS Management Console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella pagina Reserved Instances (Istanze riservate), selezionare una o più Istanze riservate da modificare e scegliere Actions (Azioni), Modify Reserved Instances (Modifica istanze riservate).

   > **Note**
   >
   > Se le Istanze riservate non sono nello stato attivo o non possono essere modificate, l'opzione Modify Istanze riservate (Modifica Istanze riservate) è disabilitata.

3. La prima voce nella tabella di modifica indica gli attributi degli elementi di Istanze riservate selezionati e almeno una configurazione di destinazione al di sotto. La colonna Units (unità) mostra il footprint della dimensione dell'istanza totale. Selezionare Add (Aggiungi) per ciascuna nuova configurazione da aggiungere. Modifica gli attributi secondo necessità per ciascuna configurazione, quindi scegli Continue (Continua):

- Scope (Ambito di applicazione): scegliere se la configurazione si applica a una zona di disponibilità o all'intera regione.
- Availability Zone (Zona di disponibilità): scegliere la zona di disponibilità richiesta. Non applicabile agli elementi di Istanze riservate regionali.
- Tipo di istanza: seleziona il tipo di istanza richiesto. Le configurazioni combinate devono avere un footprint delle dimensioni di istanza pari alle configurazioni originali.
- Count (Conteggio): specificare il numero di istanze. Per dividere le Istanze riservate in più configurazioni, ridurre il conteggio, scegliere Add (Aggiungi) e specificare un conteggio per la configurazione aggiuntiva. Ad esempio, se si ha una singola configurazione con un conteggio di 10, è possibile impostare il relativo conteggio su 6 e aggiungere una configurazione con un conteggio di 4. In questo modo, l'Istanza riservata originale viene ritirata dopo l'attivazione della nuova Istanze riservate.

4. Per confermare le scelte di modifica dopo aver specificato le configurazioni di destinazione, scegli Submit Modifications (Invia modifiche).
5. Puoi determinare lo stato della richiesta di modifica osservando la colonna State (Stato) nella schermata delle Istanze riservate. Di seguito sono riportati gli stati possibili.

   - attiva (modifica in sospeso) – Stato della transizione per la Istanze riservate di origine
   - ritirata (modifica in sospeso) – Stato della transizione per la Istanze riservate di origine mentre vengono create le nuove Istanze riservate
   - ritirata – Istanze riservate modificata e sostituita con successo
   - attiva – Una delle seguenti opzioni:
     - Nuovi elementi di Istanze riservate creati da una richiesta di modifica corretta
     - Elementi di Istanze riservate originali dopo una richiesta di modifica errata

Per modificare Istanze riservate utilizzando la riga di comando

1. Per modificare Istanze riservate, puoi usare uno dei comandi seguenti:
   - modify-reserved-instances (AWS CLI)
   - Edit-EC2ReservedInstance (AWS Tools for Windows PowerShell)
2. Per ottenere lo stato della richiesta della modifica (`processing`, `fulfilled` o `failed`), utilizza uno dei comandi seguenti:
   - describe-reserved-instances-modifications (AWS CLI)

- Get-EC2ReservedInstancesModification (AWS Tools for Windows PowerShell)

Risoluzione dei problemi relativi alle richieste di modifica

Se le impostazioni della configurazione di destinazione richieste erano univoche, riceverai un messaggio indicante che si sta elaborando la richiesta. In questa fase, Amazon EC2 ha solo stabilito che i parametri della richiesta di modifica siano validi. La richiesta di modifica può sempre generare un errore durante l'elaborazione se non è disponibile la capacità necessaria.

In alcune situazioni, potresti ricevere un messaggio indicante richieste di modifica incomplete o errate invece di una conferma. Utilizza le informazioni incluse in tali messaggi come punto iniziale per inviare nuovamente un'altra richiesta di modifica. Assicurati di aver letto le restrizioni applicabili prima di inviare la richiesta.

Non tutti gli elementi di Istanze riservate selezionati possono essere elaborati per la modifica

Amazon EC2 identifica ed elenca le Istanze riservate che non possono essere modificate. Se ricevi un messaggio di questo tipo, vai alla pagina Reserved Instances (Istanze riservate) nella console di Amazon EC2 e controlla le informazioni per le Istanze riservate.

Errore durante l'elaborazione della richiesta di modifica

Hai richiesto la modifica di uno o più elementi di Istanze riservate ma nessuna delle richieste può essere elaborata. In base al numero di prenotazioni modificate, puoi ottenere versioni diverse del messaggio.

Amazon EC2 mostra le ragioni per cui la richiesta non può essere elaborata. Ad esempio, potresti aver specificato la stessa configurazione di destinazione (una combinazione di zona di disponibilità e piattaforma) per uno o più sottoinsiemi delle Istanze riservate che stai modificando. Prova a inviare nuovamente le richieste di modifica, ma assicurati che i dettagli dell'istanza delle prenotazioni coincidano e che le configurazioni di destinazione per tutti i sottoinsiemi modificati siano univoci.

Scambiare le Istanze riservate modificabili

Puoi scambiare una o più Istanze riservate modificabili con un'altra Istanza riservata modificabile caratterizzata da una diversa configurazione, inclusa la famiglia di istanze, il sistema operativo e la tenancy. Non ci sono limiti al numero di scambi che puoi effettuare, purché la nuova istanza riservata modificabile abbia un valore pari o superiore alle istanze riservate modificabili che stai scambiando.

Quando scambi l'Istanza riservata modificabile, il numero di istanze per la prenotazione corrente viene scambiato con un numero di istanze che copre un valore pari o superiore alla configurazione della nuova istanza riservata modificabile. Amazon EC2 calcola il numero di istanze riservate che puoi ricevere a seguito dello scambio.

Non è possibile scambiare Istanze riservate Standard, ma è possibile modificarle. Per ulteriori informazioni, consulta Modificare le Istanze riservate.

Indice

Requisiti per lo scambio di elementi di Istanze riservate modificabili

Se sono soddisfatte le condizioni seguenti, Amazon EC2 elabora la tua richiesta di scambio. La Istanza riservata modificabile deve essere:

- Attivo
- Priva di una richiesta di scambio precedente
- Con tempo residuo di almeno 24 ore prima della scadenza

Si applicano le regole seguenti:

- Le istanze riservate modificabili possono essere scambiate con altre istanze riservate modificabili attualmente offerte da AWS.
- Gli elementi di Istanze riservate modificabili sono associati a una regione specifica, che resta invariata per la durata del periodo della prenotazione. Non puoi scambiare un'Istanza riservata modificabile con un'altra Istanza riservata modificabile in una regione diversa.
- Puoi scambiare una o più Istanze riservate modificabili alla volta con una sola Istanza riservata modificabile.
- Puoi scambiare una parte di un'Istanza riservata modificabile, modificarle in due o più prenotazioni e quindi scambiare una o più prenotazioni con una nuova Istanza riservata modificabile. Per

ulteriori informazioni, consulta Scambiare una parte di una Istanza riservata modificabile. Per ulteriori informazioni sulla modifica delle Istanze riservate, consulta Modificare le Istanze riservate.

- Tutte le Istanze riservate modificabili con pagamento anticipato possono essere scambiate con Istanze riservate modificabili con pagamento anticipato parziale e viceversa.

> **Note**
>
> Se il pagamento anticipato totale richiesto per lo scambio (costo effettivo) è inferiore a 0,00 USD, nell'istanza riservata convertibile AWS viene assegnata automaticamente una quantità di istanze tale da garantire che il costo effettivo sia pari o superiore a 0,00 USD.

> **Note**
>
> Se il valore totale (prezzo iniziale + prezzo orario * numero di ore rimanenti) della nuova istanza riservata convertibile è inferiore al valore totale dell'istanza riservata convertibile scambiata, ti fornisce AWS automaticamente una quantità di istanze nell'istanza riservata convertibile che garantisce che il valore totale sia uguale o superiore a quello dell'istanza riservata convertibile scambiata.

- Per beneficiare di un prezzo migliore, puoi scambiare un'Istanza riservata modificabile senza pagamento anticipato con un'Istanza riservata modificabile con pagamento anticipato totale o parziale.
- Non puoi scambiare tutte le Istanze riservate modificabili con pagamento anticipato totale e parziale con Istanze riservate modificabili senza pagamento anticipato.
- Puoi scambiare un'Istanza riservata modificabile senza pagamento anticipato con un'altra Istanza riservata modificabile senza pagamento anticipato solo se il prezzo orario della nuova Istanza riservata modificabile è identico o superiore a quello della Istanza riservata modificabile scambiata.

> **Note**
>
> Se il valore totale (tariffa oraria * numero di ore residue) della nuova istanza riservata modificabile è inferiore al valore totale dell'istanza riservata modificabile scambiata, AWS ti fornisce automaticamente una quantità di istanze nell'istanza riservata modificabile che assicura che il valore totale sia lo stesso o superiore a quello dell'istanza riservata modificabile.

- Se scambi più Istanze riservate modificabili con date di scadenza differenti, la data di scadenza della nuova Istanza riservata modificabile sarà la più lontana nel futuro.
- Se scambi una singola Istanza riservata modificabile, questa deve avere la stessa durata (1 o 3 anni) della nuova Istanza riservata modificabile. Se unisci più Istanze riservate modificabili di diversa durata, la nuova Istanza riservata modificabile ha una durata di 3 anni. Per ulteriori informazioni, consulta Unire le Istanze riservate modificabili.
- Quando Amazon EC2 scambia un'istanza riservata modificabile, ritira la prenotazione associata e trasferisce la data di fine alla nuova prenotazione. Dopo lo scambio, Amazon EC2 imposta sia la data di fine per la vecchia prenotazione sia la data di inizio per la nuova prenotazione sulla data dello scambio. Ad esempio, se sostituisci una prenotazione di 3 anni con una validità residua di 16 mesi, la nuova prenotazione sarà di 16 mesi e avrà la stessa data di fine della prenotazione dell'istanza riservata modificabile che hai scambiato.

Calcolare gli scambi di Istanze riservate modificabili

Lo scambio di elementi di Istanze riservate modificabili è gratuito. Tuttavia, potresti dover pagare un costo di allineamento, che è un costo anticipato ripartito proporzionalmente della differenza tra le Istanze riservate modificabili di cui eri in possesso e le nuove Istanze riservate modificabili ricevute nello scambio.

Ciascuna Istanza riservata modificabile ha un valore di listino. Questo valore viene confrontato con quello degli elementi di Istanze riservate modificabili richieste al fine di determinare quante prenotazioni di istanze puoi ricevere dallo scambio.

Ad esempio, hai una Istanza riservata modificabile con un valore di listino di 35 USD che intendi scambiare per un tipo di istanza nuovo con un valore di listino di 10 USD.

```
$35/$10 = 3.5
```

Puoi scambiare la Istanza riservata modificabile con tre Istanze riservate modificabili da 10 USD. Non è possibile acquistare metà delle prenotazioni, pertanto è necessario acquistare un'ulteriore Istanza riservata modificabile che copra il resto:

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved
 Instance
```

La quarta Istanza riservata modificabile ha la stessa data di fine delle altre tre. Se stai scambiando elementi di Istanze riservate modificabili con costo anticipato parziale o totale, sarà necessario

pagare il costo di allineamento per la quarta prenotazione. Se il costo anticipato restante degli elementi di Istanze riservate modificabili è 500 USD, e la nuova prenotazione è di norma 600 USD su base ripartita proporzionalmente, ti verranno addebitati 100 USD.

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of old
 reservations = $100 difference
```

Unire le Istanze riservate modificabili

Se unisci due o più Istanze riservate modificabili, il termine della nuova Istanza riservata modificabile deve essere lo stesso o più grande delle Istanze riservate modificabili originali. La data di scadenza della nuova Istanza riservata modificabile sarà la più lontana nel futuro.

Supponiamo, ad esempio, tu abbia i seguenti elementi di Istanze riservate modificabili nell'account:

ID Istanza riservata	Termine	Data di scadenza
aaaa1111	1 anno	31/12/2018
bbbb2222	1 anno	31/07/2018
cccc3333	3 anni	30/06/2018
dddd4444	3 anni	31/12/2019

- Puoi unire `aaaa1111` e `bbbb2222` e scambiarli con un'Istanza riservata modificabile di 1 anno. Non puoi scambiarli con un'Istanza riservata modificabile di 3 anni. La data di scadenza della nuova Istanza riservata modificabile è 31/12/2018.
- Puoi unire `bbbb2222` e `cccc3333` e scambiarli con un'Istanza riservata modificabile di 3 anni. Non puoi scambiarli con un'Istanza riservata modificabile di 1 anno. La data di scadenza della nuova Istanza riservata modificabile è 31/07/2018.
- Puoi unire `cccc3333` e `dddd4444` e scambiarli con un'Istanza riservata modificabile di 3 anni. Non puoi scambiarli con un'Istanza riservata modificabile di 1 anno. La data di scadenza della nuova Istanza riservata modificabile è 31/12/2019.

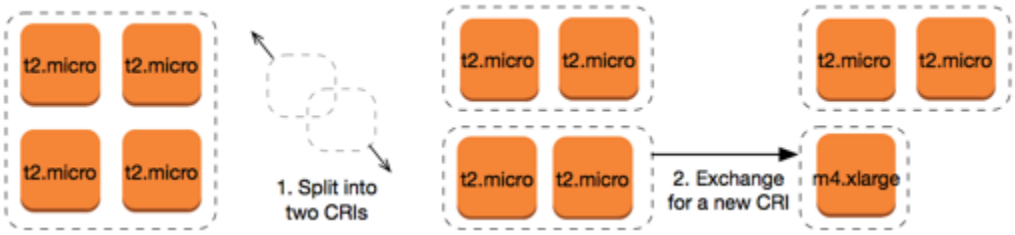
Scambiare una parte di una Istanza riservata modificabile

Puoi usare il processo di modifica per suddividere l'Istanza riservata modificabile in prenotazioni più piccole, quindi scambiare una o più delle nuove prenotazioni con una nuova Istanza riservata modificabile. Gli esempi seguenti mostrano come procedere.

Example Esempio: Istanza riservata modificabile con più istanze

In questo esempio hai un'`t2.micro` Istanza riservata modificabile con quattro istanze nella prenotazione. Per scambiare due istanze `t2.micro` con un'istanza `m4.xlarge`:

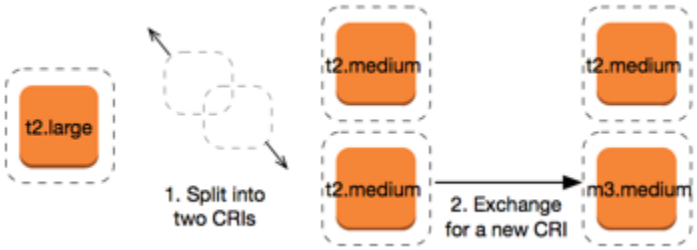
1. Modifica l'Istanza riservata modificabile `t2.micro` suddividendola in due Istanze riservate modificabili `t2.micro` con due istanze ciascuna.
2. Scambia una delle nuove Istanze riservate modificabili `t2.micro` con un'Istanza riservata modificabile `m4.xlarge`.



Example Esempio: Istanza riservata modificabile con una singola istanza

In questo esempio hai un'Istanza riservata modificabile `t2.large`. Per modificarla in una istanza `t2.medium` più piccola e un'istanza `m3.medium`:

1. Modifica l'Istanza riservata modificabile `t2.large` suddividendola in due Istanze riservate modificabili `t2.medium`. Una sola istanza `t2.large` ha lo stesso footprint della dimensione di istanza di due istanze `t2.medium`.
2. Scambia una delle nuove Istanze riservate modificabili `t2.medium` con un'Istanza riservata modificabile `m3.medium`.



Per ulteriori informazioni, consulta Supporto per la modifica delle dimensioni dell'istanza e Inviare richieste di scambio.

Inviare richieste di scambio

Puoi scambiare le Istanze riservate modificabili utilizzando la console Amazon EC2 o uno strumento a riga di comando.

Scambiare una Istanza riservata modificabile utilizzando la console

Puoi ricercare offerte di elementi di Istanze riservate modificabili e selezionare la nuova configurazione dalle scelte fornite.

New console

Per scambiare le Istanze riservate modificabili tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Reserved Instances (Istanze riservate), selezionare le Istanze riservate modificabili da scambiare e scegliere Actions (Azioni), Exchange Istanza riservata (Scambia Istanza riservata).
3. Selezionare gli attributi della configurazione desiderata e scegliere Find offering (Trova offerta).
4. Selezionare una nuova Istanza riservata modificabile. Nella parte inferiore dello schermo, è possibile visualizzare il numero di Istanze riservate che si riceve per lo scambio e gli eventuali costi aggiuntivi.
5. Una volta selezionata una Istanza riservata modificabile che soddisfi le proprie esigenze, scegliere Review (Verifica).
6. Scegliere Exchange (Scambia), quindi Close (Chiudi).

Old console

Per scambiare le Istanze riservate modificabili tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Reserved Instances (Istanze riservate), selezionare le Istanze riservate modificabili da scambiare e scegliere Actions (Azioni), Exchange Istanza riservata (Scambia Istanza riservata).
3. Selezionare gli attributi della configurazione desiderata e scegliere Find Offering (Trova offerta).
4. Selezionare una nuova Istanza riservata modificabile. Nella colonna Instance Count (Conteggio istanze) viene visualizzato il numero di Istanze riservate ricevute per lo scambio. Una volta selezionata un'Istanza riservata modificabile che soddisfi le proprie esigenze, scegliere Exchange (Scambia).

Le Istanze riservate scambiate vengono ritirate e le nuove Istanze riservate vengono visualizzate nella console Amazon EC2. La propagazione di questo processo può richiedere alcuni minuti.

Scambiare una Istanza riservata modificabile tramite la CLI

Per scambiare un'Istanza riservata modificabile, individua innanzitutto una nuova Istanza riservata modificabile che soddisfi le tue esigenze:

- describe-reserved-instances-offerings (AWS CLI)
- Get-EC2ReservedInstancesOffering PowerShell(Strumenti per Windows)

Ottieni un preventivo per lo scambio, che includa il numero di elementi di Istanze riservate che otterrai dallo scambio e il costo di allineamento effettivo per lo scambio:

- get-reserved-instances-exchange-citazione ()AWS CLI
- getEC2- ReservedInstancesExchangeQuote (Strumenti per Windows) PowerShell

Infine, esegui lo scambio:

- accept-reserved-instances-exchange-citazione ()AWS CLI
- Confirm-EC2ReservedInstancesExchangeQuote(Strumenti per Windows PowerShell)

Quote di istanze riservate

Puoi acquistare nuove istanze riservate ogni mese. Il numero di nuove istanze riservate che puoi acquistare ogni mese è determinato dalla quota mensile, come segue:

Descrizione della quota	Quota predefinita
Nuove istanze regionali riservate	20 per regione al mese
Nuove istanze riservate zonali	20 per zona di disponibilità al mese

Ad esempio, in una regione con tre zone di disponibilità, la quota predefinita è di 80 nuove istanze riservate al mese, calcolata come segue:

- 20 istanze riservate regionali per la regione
- Più 60 istanze riservate zonali (20 per ciascuna delle tre zone di disponibilità)

Le istanze nello `running` stato vengono conteggiate ai fini della quota. Le istanze che si trovano negli `hibernated` statipending, `stoppingstopped`, e non vengono conteggiate ai fini della quota.

Visualizza il numero di istanze riservate acquistate

Il numero di istanze riservate acquistate è indicato dal campo Instance count (Conteggio istanze) (console) o dal parametro `InstanceCount` (AWS CLI). Quando acquisti nuove istanze riservate, la quota viene misurata rispetto al numero totale di istanze. Ad esempio, se acquisti una singola configurazione di istanza riservata con un numero di istanze pari a 10, l'acquisto viene conteggiato ai fini della tua quota come 10, e non come 1.

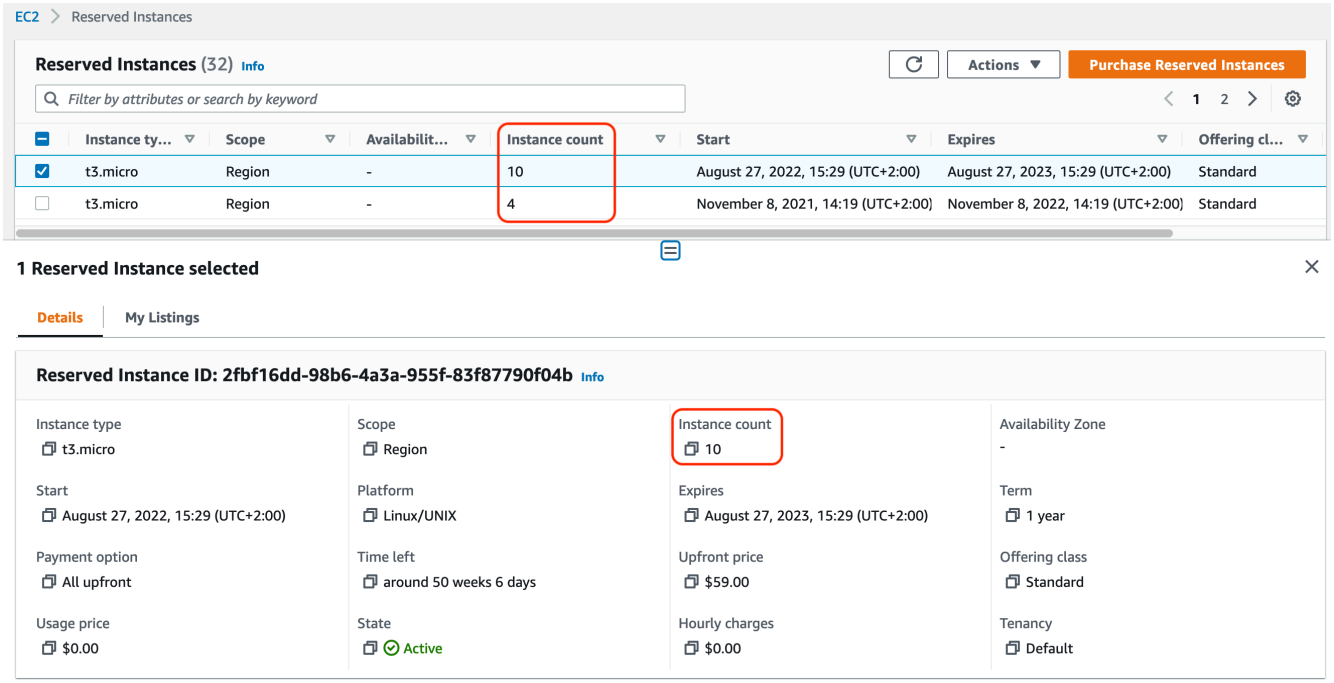
Puoi visualizzare quante istanze riservate hai acquistato utilizzando Amazon EC2 o l' AWS CLI.

Console

Per visualizzare il numero di istanze riservate acquistate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Seleziona una configurazione di istanza riservata dalla tabella e controlla il campo Instance count (Conteggio istanze).

Nella schermata seguente, la riga selezionata rappresenta una singola configurazione dell'istanza riservata per un tipo di istanza `t3.micro`. La colonna Instance count (Conteggio istanze) nella vista della tabella e il campo Instance count (Conteggio istanze) nella vista dettagliata (evidenziata nella schermata) indicano che ci sono 10 istanze riservate per questa configurazione.



AWS CLI

Per visualizzare il numero di istanze riservate acquistate

Utilizza il comando describe-reserved-instancesCLI e specifica l'ID della configurazione dell'istanza riservata.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids 2fbf16dd-98b6-4a3a-955f-83f87790f04b \
    --output table
```

Output di esempio: il campo `InstanceCount` indica che ci sono 10 istanze riservate per questa configurazione.

```
-------------------------------------------------------------------
|                   DescribeReservedInstances                     |
+-----------------------------------------------------------------+
```

```
||                      ReservedInstances                          ||
|+----------------------+-----------------------------------------+|
||  CurrencyCode        |  USD                                    ||
||  Duration            |  31536000                               ||
||  End                 |  2023-08-27T13:29:44+00:00              ||
||  FixedPrice          |  59.0                                   ||
||  InstanceCount       |  10                                     ||
||  InstanceTenancy     |  default                                ||
||  InstanceType        |  t3.micro                               ||
||  OfferingClass       |  standard                               ||
||  OfferingType        |  All Upfront                            ||
||  ProductDescription  |  Linux/UNIX                             ||
||  ReservedInstancesId |  2fbf16dd-98b6-4a3a-955f-83f87790f04b   ||
||  Scope               |  Region                                 ||
||  Start               |  2022-08-27T13:29:45.938000+00:00       ||
||  State               |  active                                 ||
||  UsagePrice          |  0.0                                    ||
|+----------------------+-----------------------------------------+|
|||                      RecurringCharges                         |||
||+---------------------------------+--------------------------+||
|||  Amount                         |  0.0                     |||
|||  Frequency                      |  Hourly                  |||
||+---------------------------------+--------------------------+||
```

Considerazioni

Un'Istanza riservata regionale applica uno sconto a un'Istanza on demand in esecuzione. Il limite predefinito per le Istanza on demand è 20. Non è possibile superare il limite di Istanza on demand acquistando Istanze riservate regionali. Se ad esempio sono in esecuzione già 20 Istanze on demand e si acquistano 20 Istanze riservate regionali, i 20 Istanze riservate regionali vengono utilizzati per applicare uno sconto ai 20 Istanze on demand in esecuzione. Se si acquistano altre Istanze riservate regionali, non sarà possibile avviare altre istanze, in quanto viene raggiunto il limite di Istanza on demand.

Prima di acquistare Istanze riservateregionali, verificare il limite Istanza on demand corrisponda o superi il numero di Istanze riservate regionali che vuoi. Se necessario, richiedere un aumento del limite Istanza on demand prima di acquistare più Istanze riservate regionali.

Istanza riservata zonale: un'Istanza riservata acquistata per una zona di disponibilità specifica, che offre la prenotazione della capacità e uno sconto. È possibile superare il limite di Istanza on demand in esecuzione acquistando Istanze riservate di zona. Se, ad esempio, sono in esecuzione già 20

Istanze on demand e si acquistano 20 Istanze riservate di zona, è possibile avviare altre 20 Istanze on demand che corrispondono alle specifiche delle Istanze riservate di zona, ottenendo un totale di 40 istanze in esecuzione.

Visualizza le quote della tua istanza riservata e richiedi un aumento della quota

La console Amazon EC2 fornisce informazioni sulle quote. Puoi anche richiedere un aumento delle quote. Per ulteriori informazioni, consultare Visualizzazione delle quote correnti e Richiesta di un aumento.

Spot Instances

Un'istanza spot è un'istanza EC2 che utilizza capacità EC2 inutilizzata disponibile a un prezzo inferiore a quello on demand. Poiché Istanze spot consente di richiedere istanze EC2 inutilizzate con forti sconti, è possibile ridurre i costi di Amazon EC2 in modo significativo. La tariffa oraria per un'istanza spot è denominata prezzo Spot. Il prezzo Spot per ogni tipo di istanza in ogni zona di disponibilità viene stabilito da Amazon EC2 e regolato gradualmente in base alla fornitura sul lungo periodo e alla richiesta per Istanze spot. L'istanza spot viene eseguita ogni qualvolta è disponibile capacità.

Le Istanze spot sono una scelta conveniente se si può essere flessibili su quando vengono eseguite le applicazioni e se queste possono essere interrotte. Per esempio, le Istanze spot sono adatte all'analisi dei dati, alle attività batch, alle elaborazioni in background e alle attività opzionali. Per ulteriori informazioni, consulta Istanze spot Amazon EC2.

Per un confronto tra le diverse opzioni di acquisto per le istanze EC2, consulta Opzioni di acquisto delle istanze.

Argomenti

Concetti

Prima di cominciare a utilizzare istanze spot, occorre acquisire familiarità con i concetti seguenti:

- Pool di capacità spot - Un insieme di istanze EC2 inutilizzate con lo stesso tipo di istanza (ad esempio, `m5.large`) e zona di disponibilità.
- Prezzo Spot - Il prezzo orario attuale di un'istanza spot.
- Richiesta di istanza spot - Richiede un'istanza spot. Quando la capacità è disponibile, Amazon EC2 soddisfa la richiesta. Una richiesta di istanza spot può essere una tantum o persistente. Amazon EC2 invia automaticamente una nuova richiesta di istanza spot persistente dopo che l'istanza spot associata alla richiesta viene interrotta.

- Suggerimento di ribilanciamento dell'istanza EC2: Amazon EC2 emette un segnale che suggerisce il ribilanciamento dell'istanza per segnalarti che un'istanza spot è ad alto rischio di interruzione. Questo segnale ti offre l'opportunità di ribilanciare preventivamente i carichi di lavoro tra quelli esistenti o tra nuove istanze spot senza dover attendere l'avviso di interruzione dell'istanza spot di due minuti.
- Interruzione istanza spot: Amazon EC2 termina, arresta o iberna l'istanza spot quando Amazon EC2 deve recuperare capacità. Amazon EC2 fornisce una notifica di interruzione dell'istanza spot, che dà all'istanza un preavviso di due minuti prima che venga interrotta.

Principali differenze tra Istanze spot e Istanze on demand

Nella tabella seguente sono elencate le principali differenze tra istanze spot e istanze on demand.

	Spot Instances	On-Demand Instances
Ora di avvio	Può essere avviata immediatamente solo se è attiva la richiesta dell'istanza spot e se la capacità è disponibile.	Può essere avviata immediatamente solo se si effettua una richiesta di avvio manuale e la capacità è disponibile.
Capacità disponibile	Se la capacità non è disponibile, la richiesta dell'istanza spot continuerà a effettuare automaticamente la richiesta di avvio fino a quando la capacità non diventa disponibile.	Se la capacità non è disponibile quando si effettua una richiesta di avvio, si ottiene un errore di capacità insufficiente (ICE).
Tariffa oraria	Il prezzo orario per istanze spot varia in base alla fornitura a lungo termine e alla domanda.	Il prezzo orario per le Istanze on demand è statico.
Raccomandazione di ribilanciamento	Il segnale che Amazon EC2 emette per un'istanza spot in esecuzione quando presenta un rischio elevato di interruzione.	L'utente determina quando un'Istanza on demand viene interrotta (arrestata, ibernata o terminata).

	Spot Instances	On-Demand Instances
Interruzione istanza	Un'istanza spot supportata da Amazon EBS può essere arrestata e avviata. Amazon EC2, inoltre, può interrompere una singola istanza spot se la capacità non è più disponibile.	L'utente determina quando un'Istanza on demand viene interrotta (arrestata, ibernata o terminata).

Come iniziare

Occorre innanzitutto la configurazione per l'uso di Amazon EC2. Può anche essere utile acquisire dimestichezza con il lancio delle Istanze on demand prima del lancio delle Istanze spot.

Nozioni Spot di base

- Come funzionano Istanze spot

Utilizzo di Istanze spot

- Creare una richiesta di istanza spot
- Ottenere informazioni sullo stato della richiesta
- Interruzioni dell'istanza spot

Servizi correlati

È possibile eseguire il provisioning delle Istanze spot direttamente utilizzando Amazon EC2. È possibile eseguire il provisioning delle istanze spot anche utilizzando altri servizi di AWS. Per ulteriori informazioni, consulta la seguente documentazione:

Amazon EC2 Auto Scaling e Istanze spot

> Puoi creare modelli o configurazioni di avvio in modo che il Dimensionamento automatico Amazon EC2 possa lanciare istanze spot. Per ulteriori informazioni, consulta Richiesta di Istanze spot per applicazioni e gruppi flessibili a tolleranza d'errore e Gruppi Auto Scaling con più tipi di istanza e opzioni di acquisto nella Guida per l'utente di Amazon EC2 Auto Scaling.

Amazon EMR e Istanze spot

Ci sono casi in cui può essere utile eseguire le Istanze spot in un cluster Amazon EMR. Per maggiori informazioni, consulta Istanze spot e When Should You Use Istanze spot (Quando utilizzare le Istanze spot) nella Amazon EMR Management Guide.

AWS CloudFormation modelli

AWS CloudFormation consente di creare e gestire una raccolta di AWS risorse utilizzando un modello in formato JSON. Per ulteriori informazioni, consulta EC2 Spot Instance Updates - Auto Scaling CloudFormation and Integration.

AWS SDK for Java

Puoi usare il linguaggio di programmazione Java per gestire le Istanze spot. Per ulteriori informazioni, consulta Tutorial: Amazon EC2 Istanze spot (Tutorial: Istanze spot Amazon EC2) e Tutorial: Advanced Amazon EC2 Spot Request Management (Tutorial: gestione avanzata delle richieste Spot di Amazon EC2).

AWS SDK for .NET

Puoi usare l'ambiente di programmazione .NET per gestire le Istanze spot. Per ulteriori informazioni, consulta Tutorial: Amazon EC2 Istanze spot (Tutorial: Istanze spot Amazon EC2).

Prezzi e risparmio

Paghi il prezzo Spot per le Istanze spot, che viene stabilito da Amazon EC2 e regolato gradualmente in base alla fornitura sul lungo periodo e alla richiesta di Istanze spot. Le istanze spot vengono eseguite fino a quando non vengono terminate, la capacità non è più disponibile o il gruppo Dimensionamento automatico di Amazon EC2 le termina durante il dimensionamento.

Se un'istanza spot in esecuzione viene interrotta da te o da Amazon EC2, ti vengono fatturati i secondi utilizzati o l'intera ora, oppure non viene fatturato nulla, a seconda del sistema operativo utilizzato e di chi ha interrotto l'istanza spot. Per ulteriori informazioni, consulta Fatturazione delle Istanze spot interrotte.

Le istanze Spot non sono coperte da Savings Plans. Se disponi di un Savings Plan, questo non offre risparmi aggiuntivi oltre ai risparmi che già ottieni utilizzando le istanze Spot. Inoltre, la spesa per le istanze Spot non applica gli impegni previsti dai tuoi Compute Savings Plans.

Visualizza prezzi

Per visualizzare il prezzo Spot attualmente più basso (aggiornato ogni cinque minuti) per Regione AWS tipo di istanza, consulta la pagina dei prezzi delle istanze Spot di Amazon EC2.

Per visualizzare la cronologia dei prezzi Spot degli ultimi tre mesi, usa la console Amazon EC2 o il describe-spot-price-historycomando ()AWS CLI. Per ulteriori informazioni, consulta Cronologia dei prezzi dell'istanza spot.

Associamo in modo indipendente le zone di disponibilità ai codici per ciascuna di esse Account AWS. Pertanto, è possibile ottenere risultati diversi per lo stesso codice di zona di disponibilità (per esempio, `us-west-2a`) tra account diversi.

Visualizzare il risparmio

Puoi visualizzare i risparmi ottenuti utilizzando istanze spot per una singola serie di istanze spot o per tutte le istanze spot. È possibile visualizzare il risparmio realizzato nell'ultima ora o negli ultimi tre giorni e il costo medio orario per la vCPU e per la memoria (GiB). Gli importi risparmiati sono solo delle stime e potrebbero essere diversi da quelli effettivi, in quanto non includono gli adeguamenti della fatturazione per l'utilizzo. Per ulteriori informazioni sulla visualizzazione delle informazioni sul risparmio, consulta Risparmio sull'acquisto di Istanze spot.

Visualizzare la fattura

La fattura fornisce dettagli sull'utilizzo del servizio. Per ulteriori informazioni, consulta Visualizzazione della fattura nella Guida per l'utente di AWS Billing .

Best practice per EC2 Spot

Le istanze Spot di Amazon EC2 sono capacità di elaborazione EC2 di riserva a tua disposizione con risparmi fino al 90% rispetto ai prezzi on demand. Cloud AWS L'unica differenza tra Istanze on demand e Istanze spot è che Istanze spot possono essere interrotte da Amazon EC2, con due minuti di notifica, quando Amazon EC2 necessita delle capacità in uso.

Istanze spot sono consigliate per applicazioni stateless, con tolleranza ai guasti, flessibili. Ad esempio, Istanze spot funzionano bene per Big Data, carichi di lavoro containerizzati, CI/CD, server Web stateless, High Performance Computing (HPC) e carichi di lavoro di rendering.

Durante l'esecuzione, Istanze spot sono esattamente identici a Istanze on demand. Tuttavia, Spot non garantisce la possibilità di continuare a eseguire le istanze abbastanza a lungo da completare i carichi di lavoro. Inoltre, Spot non garantisce di poter avere immediatamente a disposizione le istanze

che si stanno cercando o che sia sempre possibile ottenere la capacità aggregata richiesta. Inoltre, interruzioni e capacità delle istanze spot possono cambiare nel tempo perché la disponibilità delle istanze spot varia in base all'offerta e alla domanda e le prestazioni passate non sono una garanzia di risultati futuri.

Istanze spot non sono adatte per carichi di lavoro inflessibili, stateful, senza tolleranza ai guasti o strettamente accoppiati tra nodi di istanze. Non consigliamo le istanze Spot per carichi di lavoro intolleranti a periodi occasionali in cui l'intera capacità prevista non è completamente disponibile. Se da un lato seguire le best practice di Spot, che mirano alla flessibilità sui tipi di istanze e sulle zone di disponibilità, offre le migliori possibilità di elevata disponibilità, dall'altro non vi è alcuna garanzia che la capacità sarà disponibile, in quanto i picchi di domanda di istanze on demand possono interrompere i carichi di lavoro sulle istanze Spot.

Sconsigliamo vivamente di utilizzare le istanze Spot per questi carichi di lavoro o di effettuare il failover sulle istanze on demand per gestire interruzioni o periodi di indisponibilità. Il failover sulle istanze on demand può causare inavvertitamente interruzioni per le altre istanze Spot. Inoltre, se le istanze Spot per una combinazione di tipo di istanza e zona di disponibilità vengono interrotte, potrebbe diventare difficile ottenere istanze on demand con la stessa combinazione.

A prescindere che l'utente conosca già Spot o sia la prima volta che utilizza le istanze spot, se si verificano problemi di interruzioni o disponibilità delle istanze spot è consigliabile seguire queste best practice per ottenere la migliore esperienza di utilizzo del servizio Spot.

Best practice Spot

- Preparazione di singole istanze per le interruzioni
- Essere flessibili riguardo tipi di istanza e zone di disponibilità
- Utilizzo dei gruppi con dimensionamento automatico EC2 o del parco istanze EC2 per gestire la capacità aggregata
- Utilizzo della strategia di allocazione ottimizzata per prezzo e capacità
- Utilizza servizi integrati per gestire le tue istanze Spot AWS
- Qual è il metodo di richiesta Spot migliore da utilizzare?

Preparazione di singole istanze per le interruzioni

Il modo migliore per gestire nel modo appropriato le interruzioni delle istanze spot è progettare l'applicazione affinché sia tollerante ai guasti. A tale scopo, è possibile sfruttare i suggerimenti di ribilanciamento delle istanze EC2 e gli avvisi di interruzione delle istanze spot.

Un suggerimento di ribilanciamento dell'istanza EC2 è un segnale che avvisa che un'istanza spot è a rischio elevato di interruzione. Il segnale ti dà la possibilità di gestire l'istanza spot in modo proattivo rispetto all'avviso di interruzione dell'istanza spot con preavviso di due minuti. È possibile decidere di ribilanciare il carico di lavoro su Istanze spot nuove o esistenti che non presentano un rischio elevato di interruzione. Abbiamo semplificato l'utilizzo di questo segnale utilizzando la funzionalità di ribilanciamento della capacità nei gruppi con dimensionamento automatico e nel parco istanze EC2.

Una notifica di interruzione di istanza spot è un avviso che viene emesso due minuti prima che Amazon EC2 interrompa un'istanza spot. Se il carico di lavoro è "flessibile nel tempo", puoi anche configurare le istanze spot affinché vengano arrestate o ibernate, anziché terminate, quando vengono interrotte. Amazon EC2 arresta o iberna automaticamente le istanze spot in caso di interruzione e ripristina automaticamente le istanze quando la capacità è disponibile.

Ti consigliamo di creare una regola in Amazon EventBridge che acquisisca i consigli di ribilanciamento e le notifiche di interruzione, quindi attivi un checkpoint per l'avanzamento del carico di lavoro o gestisca correttamente l'interruzione. Per ulteriori informazioni, consulta Monitorare i segnali di raccomandazione di ribilanciamento. Per un esempio dettagliato che illustra come creare e utilizzare le regole degli eventi, consulta Taking Advantage of Amazon EC2 Spot Instance Interruption Notices.

Per ulteriori informazioni, consulta Raccomandazioni per il ribilanciamento delle istanze EC2 e Interruzioni dell'istanza spot.

Essere flessibili riguardo tipi di istanza e zone di disponibilità

Un pool di capacità spot è un insieme di istanze EC2 inutilizzate con lo stesso tipo di istanza (ad esempio `m5.large`) e zona di disponibilità (ad esempio, us-east-1a). È necessario essere flessibili sui tipi di istanza richiesti e sulle zone di disponibilità in cui è possibile distribuire il carico di lavoro. Questo offre a Spot una migliore possibilità di trovare e allocare la quantità di capacità di elaborazione richiesta. Ad esempio, non richiedere solo `c5.large` se sei disposto a usare grandi quantità delle famiglie c4, m5 e m4.

A seconda delle esigenze specifiche, puoi valutare su quali tipi di istanza puoi essere flessibile per soddisfare i requisiti di calcolo. Se un carico di lavoro può essere scalato verticalmente, occorre includere tipi di istanza più grandi (più vCPU e memoria) nelle richieste. Se puoi scalare solo orizzontalmente, devi includere tipi di istanza di vecchia generazione in quanto sono meno richiesti dai clienti on demand.

Una buona regola è quella di essere flessibili su almeno 10 tipi di istanza per ogni carico di lavoro. Assicurati inoltre che tutte le zone di disponibilità siano configurate per l'utilizzo nel VPC e selezionate per il carico di lavoro.

Utilizzo dei gruppi con dimensionamento automatico EC2 o del parco istanze EC2 per gestire la capacità aggregata

Spot consente di pensare in termini di capacità aggregata (in unità che includono vCPU, memoria, archiviazione o velocità effettiva di rete), piuttosto che in termini di singole istanze. I gruppi con dimensionamento automatico e il parco istanze EC2 consentono di avviare e gestire una capacità di destinazione e di sostituire automaticamente le risorse interrotte o terminate manualmente. Quando configuri un gruppo con dimensionamento automatico o un parco istanze EC2, devi specificare solo i tipi di istanza e la capacità di destinazione in base alle esigenze dell'applicazione. Per ulteriori informazioni, consulta Gruppi Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling e Creazione di un parco istanze EC2 in questa guida per l'utente.

Utilizzo della strategia di allocazione ottimizzata per prezzo e capacità

Le strategie di allocazione nei gruppi Auto Scaling consentono di effettuare il provisioning della capacità target senza la necessità di cercare manualmente i pool di capacità spot con capacità inutilizzata. È consigliabile utilizzare la strategia `price-capacity-optimized` perché questa effettua automaticamente il provisioning delle istanze dai pool di capacità spot più disponibili che hanno anche il prezzo più basso possibile. Inoltre, nel parco istanze EC2 è possibile sfruttare la strategia di allocazione `price-capacity-optimized`. Poiché la capacità dell'istanza spot viene restituita da pool con capacità ottimale, ciò riduce la possibilità che le istanze spot vengano recuperate. Per ulteriori informazioni sulle strategie di allocazione, consulta Istanze spot nella Guida per l'utente di Amazon EC2 Auto Scaling e Quando i carichi di lavoro hanno un costo di interruzione elevato in questa guida per l'utente.

Utilizza servizi integrati per gestire le tue istanze Spot AWS

Altri AWS servizi si integrano con Spot per ridurre i costi complessivi di elaborazione senza la necessità di gestire le singole istanze o flotte. Ti consigliamo di prendere in considerazione le seguenti soluzioni per i tuoi carichi di lavoro applicabili: Amazon EMR, Amazon Elastic Container Service AWS Batch, Amazon Elastic SageMaker Kubernetes Service, Amazon e Amazon. AWS Elastic Beanstalk GameLift Per ulteriori informazioni sulle best practice Spot con questi servizi, consulta il sito Web Amazon EC2 Istanze spot Workshops.

Qual è il metodo di richiesta Spot migliore da utilizzare?

Utilizzare la tabella seguente per determinare l'API da utilizzare per richiedere istanze spot.

API	Quando usarla?	Caso d'uso	Dovrei usare quest'API?
CreateAutoScalingGroup	• Sono necessari e più istanze con una configurazione singola o mista. • Vuoi automatizzare la gestione del ciclo di vita tramite un'API configurabile.	Crea un gruppo Auto Scaling che gestisce il ciclo di vita delle istanze mantenendo il numero di istanze desiderato. Supporta il dimensionamento orizzontale (aggiunta di più istanze) tra limiti minimi e massimi specificati.	Sì
CreateFleet	• Sono necessari e più istanze con una configurazione singola o mista. • Vuoi gestire autonomamente il ciclo di vita dell'istanza. • Se non hai bisogno di scalabilità automatica, ti consigliamo di utilizzare un parco di tipo `instant`.	Crea una parco di istanze on-demand e istanze spot in una singola richiesta, con più specifiche di avvio che variano a seconda del tipo di istanza, dell'AMI, della zona di disponibilità o della sottorete. La strategia di allocazione delle istanze spot è per impostazione predefinita `lowest-price` per unità, ma puoi modificarla in `price-capacity-`	Sì: in modalità `instant` se non occorre il dimensionamento automatico

API	Quando usarla?	Caso d'uso	Dovrei usare quest'API?
		`optimized` , `capacity-optimized` o `diversified` .	
RunInstances	• Stai già utilizzando l' RunInstances API per avviare istanze On-Demand e vuoi semplicemente passare all'avvio delle istanze Spot modificando un singolo parametro. • Non sono necessarie più istanze con diversi tipi di istanza.	Avvia un numero di istanze specificato utilizzando un'AMI e un tipo di istanza.	No, perché RunInstances non consente tipi di istanze misti in una singola richiesta

API	Quando usarla?	Caso d'uso	Dovrei usare quest'API?
RequestSpotFleet	• Sconsigliamo vivamente di utilizzare l' RequestSpotFleet API perché si tratta di un'API legacy senza investimenti pianificati. • Se desideri gestire il ciclo di vita dell'istanza, utilizza l'API. CreateFleet • Se non desideri gestire il ciclo di vita dell'ista nza, utilizza l'API. CreateAut oScalingGroup	NON USARE. RequestSpotFleet è un'API legacy senza investimenti pianificati.	No
RequestSpotInstanc es	• Sconsigliamo vivamente di utilizzare l' RequestSp otInstances API perché si tratta di un'API legacy senza investimenti pianificati.	NON UTILIZZARE. RequestSpotInstances è un'API legacy senza investimenti pianificati.	No

Come funzionano Istanze spot

Per avviare un'Istanza spot, è possibile creare una Richiesta di istanza spot oppure affidarsi ad Amazon EC2 che crea una richiesta di istanza spot per tuo conto. L'Istanza spot viene avviata quando viene soddisfatta la richiesta di istanza spot.

È possibile avviare un'istanza spot utilizzando più servizi diversi. Per ulteriori informazioni, consulta Nozioni di base sulle istanze spot Amazon EC2 Windows. In questa guida per l'utente, vengono descritti i seguenti modi per avviare un'istanza spot utilizzando EC2:

- Puoi creare una richiesta di istanza Spot utilizzando la procedura guidata di avvio dell'istanza nella console Amazon EC2 o il AWS CLI comando run-instances. Per ulteriori informazioni, consulta Creare una richiesta di istanza spot.
- È possibile creare un Parco istanze EC2, nel quale si specifica il numero desiderato di istanze spot. Amazon EC2 crea una richiesta di istanza spot per tuo conto per ogni istanza spot specificata nel parco istanze EC2. Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.
- È possibile creare una richiesta di istanza spot, nel quale si specifica il numero desiderato di istanze spot. Amazon EC2 crea una richiesta di istanza spot per tuo conto per ogni istanza spot specificata nella richiesta di parco istanze spot. Per ulteriori informazioni, consulta Creare una richiesta di parco istanze spot.

L'istanza Spot viene avviata se è disponibile capacità.

L'istanza spot viene eseguita fino a quando non la arresti o termini, o fino a quando Amazon EC2 non la interrompe (nota come interruzione di istanza spot).

Quando usi le istanze spot, devi essere preparato alle interruzioni. Amazon EC2 può interrompere la tua istanza spot quando la domanda di istanze spot aumenta o la fornitura di istanze spot diminuisce. Quando Amazon EC2 interrompe un'istanza spot, invia una notifica di interruzione dell'istanza spot che fornisce all'istanza un preavviso di due minuti prima che Amazon EC2 la interrompa. Non è possibile abilitare la protezione da interruzione per Istanze spot. Per ulteriori informazioni, consulta Interruzioni dell'istanza spot.

È possibile arrestare, avviare, riavviare o terminare un'istanza spot supportata da Amazon EBS. Il servizio Spot può arrestare, terminare o ibernare un'istanza spot quando la interrompe.

Indice

- Avviare le Istanze spot in un Gruppo di zona di disponibilità
- Avviare Istanze spot in un VPC

Avviare Istanze spot in un gruppo di avvio

Specificare un gruppo di avvio nella richiesta di istanza spot per indicare ad Amazon EC2 di avviare un insieme di istanze spot solo se può avviarle tutte. Inoltre, se il servizio spot deve terminare una delle istanze in un gruppo di avvio, deve terminarle tutte. Tuttavia, se si terminano una o più istanze in un gruppo di avvio, Amazon EC2 non termina le altre istanze nel gruppo di avvio.

Sebbene questa opzione possa essere utile, l'aggiunta di questo vincolo può ridurre le possibilità che la richiesta di istanza spot venga soddisfatta e aumentare le possibilità che le istanze spot vengano terminate. Ad esempio, se il gruppo di avvio comprende istanze in più zone di disponibilità e la capacità in una di queste zone di disponibilità si riduce e non è più disponibile, Amazon EC2 interrompe tutte le istanze per il gruppo di avvio.

Se si crea un'altra richiesta di istanza spot valida che specifica lo stesso gruppo di avvio (esistente) di una precedente richiesta valida, le nuove istanze vengono aggiunte al gruppo di avvio. Successivamente, se un'istanza di questo gruppo di avvio viene terminata, tutte le istanze del gruppo di avvio vengono terminate, il che include le istanze avviate dalla prima e dalla seconda richiesta.

Avviare le Istanze spot in un Gruppo di zona di disponibilità

Specifica un gruppo di zone di disponibilità nella richiesta di istanza spot per indicare ad Amazon EC2 di avviare una serie di istanze spot nella stessa zona di disponibilità. Amazon EC2 non deve interrompere tutte le istanze di un gruppo di zona di disponibilità allo stesso tempo. Se Amazon EC2 deve interrompere una delle istanze di un gruppo di zona di disponibilità, le altre restano in esecuzione.

Sebbene questa opzione possa essere utile, l'aggiunta di questo vincolo può ridurre le possibilità che la richiesta di istanza spot venga soddisfatta.

Se si specifica un gruppo di zona di disponibilità ma non una zona di disponibilità nella richiesta di istanza spot, il risultato dipende dalla rete specificata.

VPC predefinito

Amazon EC2 utilizza la zona di disponibilità per la sottorete specificata. Se non specifichi una sottorete, seleziona una zona di disponibilità e la rispettiva sottorete predefinita, ma non

necessariamente quella con il prezzo più basso. Se è stata cancellata la sottorete predefinita per una zona di disponibilità, è necessario specificare una sottorete diversa.

VPC non predefinito

Amazon EC2 utilizza la zona di disponibilità per la sottorete specificata.

Avviare Istanze spot in un VPC

Si specifica una sottorete per le Istanze spot allo stesso modo in cui si specifica una sottorete per le Istanze on demand.

- [VPC predefinito] Se si desidera che l'istanza spot venga avviata in una specifica zona di disponibilità a basso prezzo, è necessario specificare la sottorete corrispondente nella richiesta di istanza spot. Se non si specifica una sottorete, Amazon EC2 ne seleziona una e la zona di disponibilità per tale sottorete potrebbe non avere il prezzo Spot più basso.
- [VPC non predefinito] È necessario specificare la sottorete per l'istanza spot.

Cronologia dei prezzi dell'istanza spot

I prezzi delle istanze spot sono stabiliti da Amazon EC2 e regolati in modo graduale in base ai trend a lungo termine di offerta e domanda di capacità delle istanze spot.

Quando la tua richiesta spot è soddisfatta, le tue istanze spot vengono avviate al prezzo spot corrente, non superiore al prezzo on demand. È possibile visualizzare la cronologia del prezzo Spot degli ultimi 90 giorni, filtrata per tipo di istanza, sistema operativo e zona di disponibilità.

Per visualizzare i prezzi Spot correnti

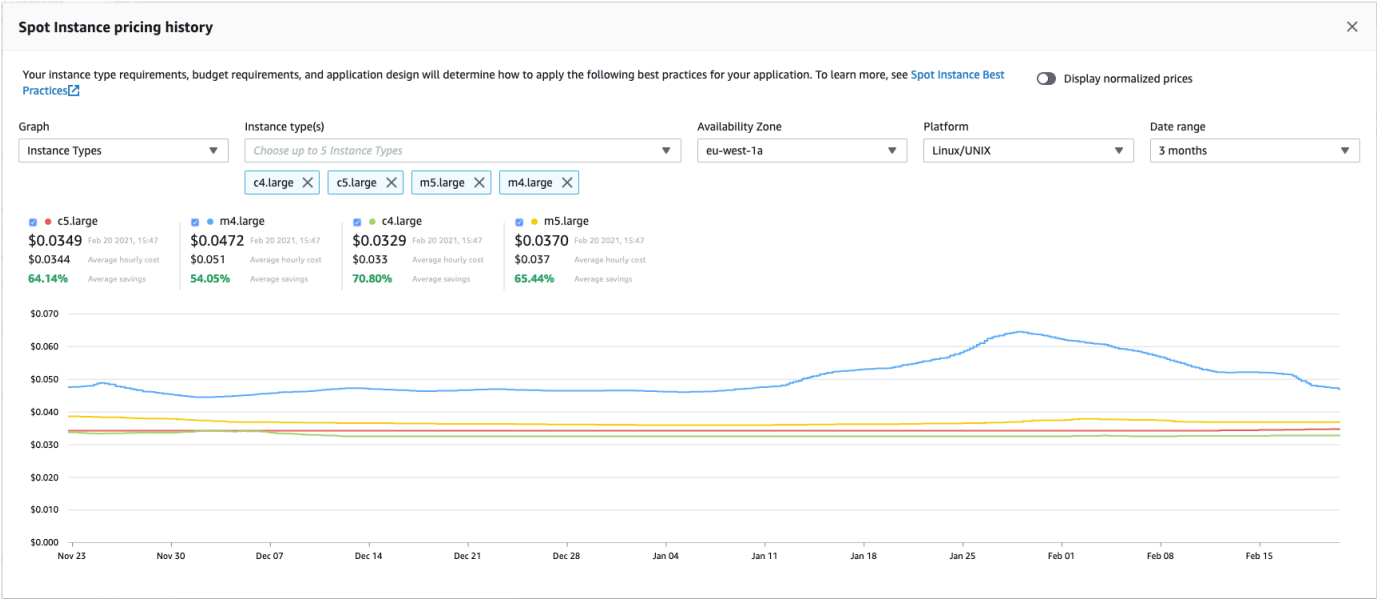
Per i prezzi delle istanze spot correnti, consulta Prezzi delle istanze spot Amazon EC2.

Per visualizzare la cronologia dei prezzi Spot utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona Cronologia prezzi.
4. Per Graph (Grafico)scegliere di confrontare la cronologia dei prezzi in base alle Availability Zones (Zone di disponibilità) o ai Instance Types (Tipi di istanze).

- Se selezioni Availability Zones (Zone di disponibilità), scegli l'Instance type (Tipo di istanza), il sistema operativo (Platform [Piattaforma]) e il Date range (Intervallo di date) per il quale visualizzare la cronologia dei prezzi.
- Se selezioni Instance Types (Tipi di istanza), scegli fino a cinque IInstance type(s) (Tipi di istanza), la Availability Zone (Zona di disponibilità), il sistema operativo (Platform [Piattaforma]) e il Date range (Intervallo di date) per il quale visualizzare la cronologia dei prezzi.

La seguente schermata mostra un confronto dei prezzi per i diversi tipi di istanza.



5. Sposta il puntatore del mouse sul grafico per visualizzare i prezzi in momenti specifici nell'intervallo di date selezionato. I prezzi sono visualizzati nei blocchi informativi sopra il grafico. Il prezzo visualizzato nella riga superiore mostra il prezzo in una data specifica. Il prezzo visualizzato nella seconda riga mostra il prezzo medio nell'intervallo di date selezionato.
6. Per visualizzare il prezzo per vCPU, attiva o disattiva Display normalized prices (Visualizza prezzi normalizzati). Per visualizzare il prezzo per il tipo di istanza, disattiva Display normalized prices (Visualizza prezzi normalizzati).

Visualizzare la cronologia del prezzo Spot tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni, consulta Accesso a Amazon EC2.

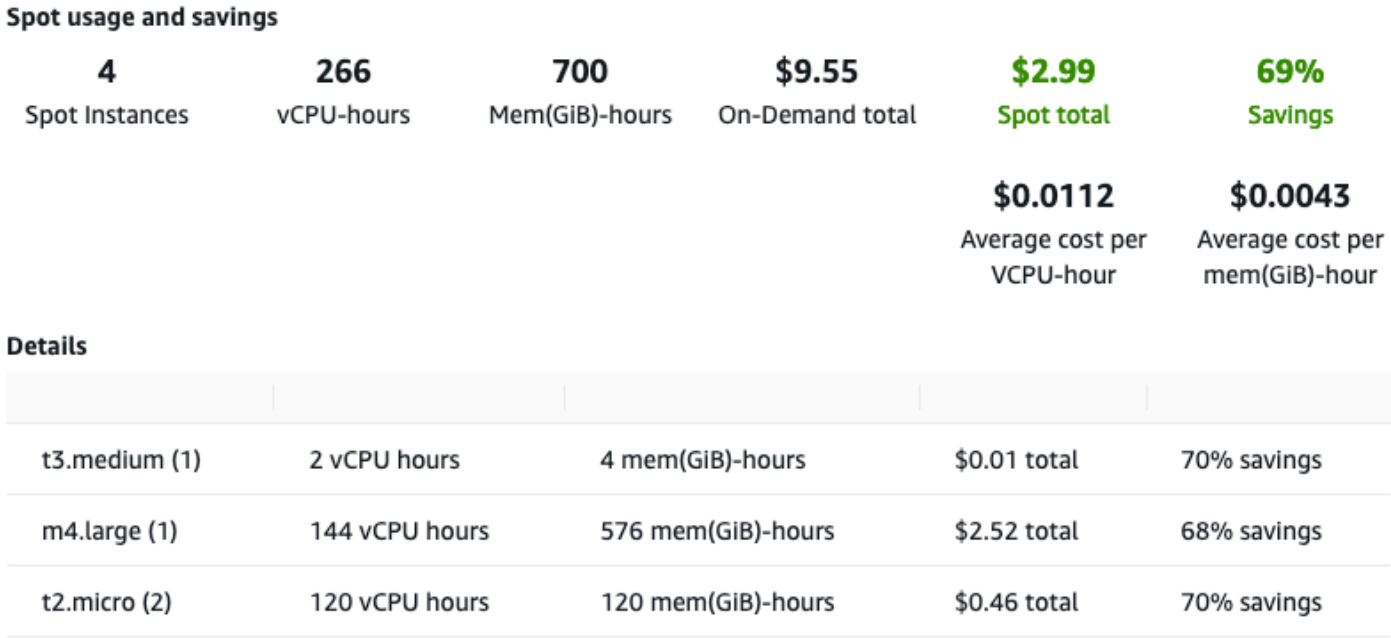
- describe-spot-price-history (AWS CLI)

- Get-EC2SpotPriceHistory (AWS Tools for Windows PowerShell)

Risparmio sull'acquisto di Istanze spot

È possibile visualizzare informazioni sull'utilizzo e sul risparmio per le Istanze spot a livello di singolo parco istanze o per tutte le Istanze spot in esecuzione. A livello di singolo parco istanze, le informazioni su utilizzo e risparmio includono tutte le istanze avviate e terminate dal parco istanze. Puoi visualizzare queste informazioni relative all'ultima ora o agli ultimi tre giorni.

Lo screenshot seguente della sezione Risparmio mostra le informazioni relative al risparmio e all'utilizzo Spot per un parco istanze spot.



Puoi visualizzare le seguenti informazioni su utilizzo e risparmio:

- Istanze spot - Il numero di Istanze spot avviate e terminate dal Parco istanze spot. Nel riepilogo del risparmio il numero rappresenta tutte le Istanze spot in esecuzione.
- vCPU-hours (vCPU/ora) – Il numero di ore di utilizzo della vCPU in tutte le Istanze spot per l'intervallo di tempo selezionato.
- Mem(GiB)-hours (Mem(GiB)/ora) – Il numero di ore di utilizzo dei GiB di memoria in tutte le Istanze spot per l'intervallo di tempo selezionato.
- On-Demand total (Totale on demand) – L'importo totale che avresti dovuto pagare per l'intervallo di tempo selezionato se avessi avviato queste istanze come Istanze on demand.

- Spot total (Totale Spot) – L'importo totale da pagare per l'intervallo di tempo selezionato.
- Savings (Risparmio) – La percentuale che risparmi non pagando il prezzo on demand.
- Average cost per vCPU-hour (Costo medio per vCPU/ora) – Il costo orario medio di utilizzo delle vCPU in tutte le Istanze spot per l'intervallo di tempo selezionato, calcolato come segue: Average cost per vCPU-hour (Costo medio per vCPU/ora) = Spot total (Totale Spot) / vCPU-hours (vCPU/ora).
- Costo medio per mem (GiB) -ora: costo orario medio di utilizzo GiBs di Spot in tutte le istanze Spot per l'intervallo di tempo selezionato, calcolato come segue: Costo medio per mem (GiB) -ora = totale Spot/Mem (GiB) -ore.
- Tabella Details (Dettagli) - I diversi tipi di istanza (il numero di istanze per tipo è indicato tra parentesi) che costituiscono il Parco istanze spot. Nel riepilogo del risparmio sono incluse tutte le Istanze spot in esecuzione.

Le informazioni relative al risparmio possono essere visualizzate solo utilizzando la console di Amazon EC2.

Per visualizzare le informazioni sui risparmi di una flotta Spot utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona l'ID di una richiesta della serie di istanze spot e scorri fino alla sezione Risparmio.

   In alternativa, seleziona la casella di controllo accanto all'ID richiesta del parco istanze spot e scegli la casella di controllo Risparmio.
4. Per impostazione predefinita, nella pagina sono visualizzate le informazioni relative a utilizzo e risparmio relative agli ultimi tre giorni. È possibile scegliere last hour (ultima ora) o last three days (ultimi tre giorni). Per i Parchi istanze spot lanciati meno di un'ora prima, la pagina mostra il risparmio stimato per l'ora.

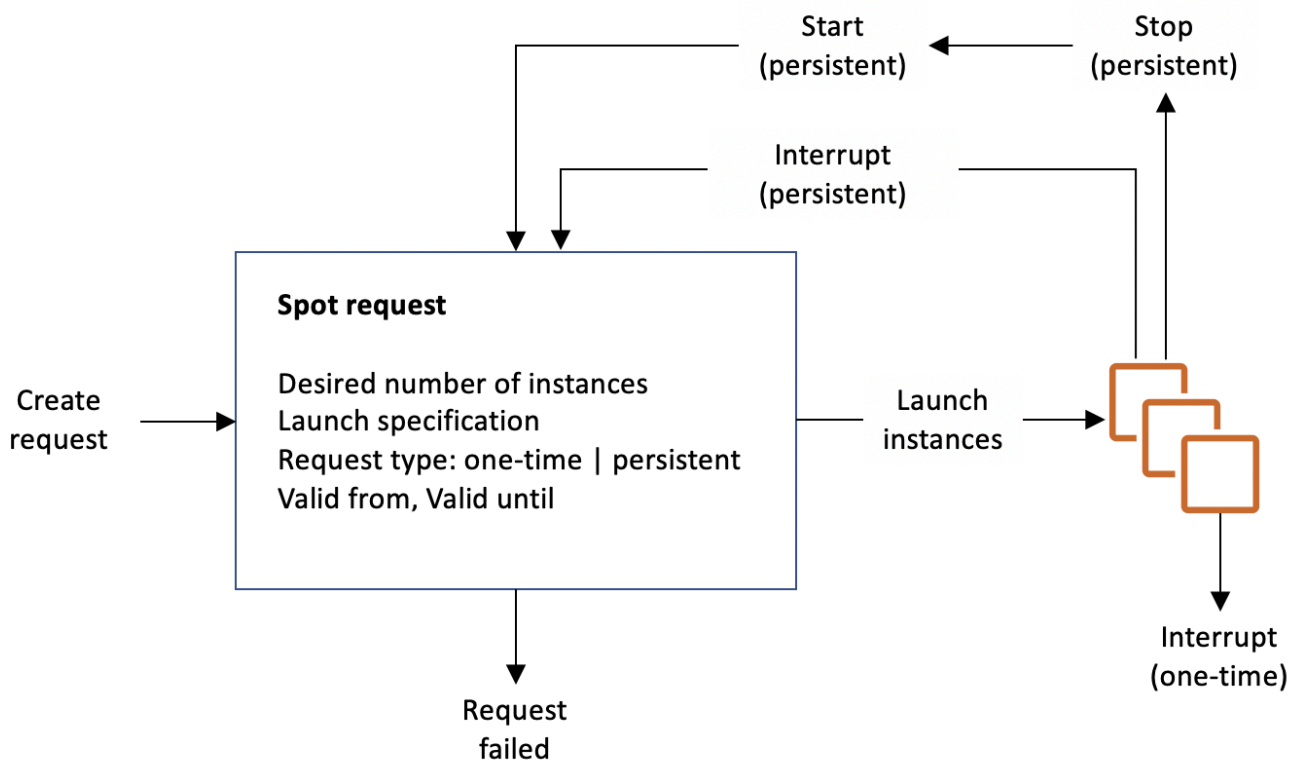
Per visualizzare le informazioni sui risparmi per tutte le istanze Spot in esecuzione utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona Riepilogo risparmio.

Utilizzo delle Istanze spot

Per utilizzare istanze spot, viene creata una richiesta di istanza spot che include il numero desiderato di istanze, il tipo di istanza e la zona di disponibilità. Quando è disponibile capacità, Amazon EC2 soddisfa la richiesta immediatamente. Altrimenti, Amazon EC2 attende finché la richiesta non può essere soddisfatta o finché la richiesta non viene annullata.

La figura seguente mostra come funzionano le richieste delle istanze spot. Il tipo di richiesta (una tantum o persistente) determina se la richiesta viene aperta nuovamente quando Amazon EC2 interrompe un'istanza spot o se un'istanza spot viene arrestata. Se la richiesta è persistente, viene riaperta dopo che l'istanza spot viene interrotta. Se la richiesta è persistente e si arresta l'istanza spot, la richiesta si apre solo dopo aver avviato l'istanza spot.



Indice

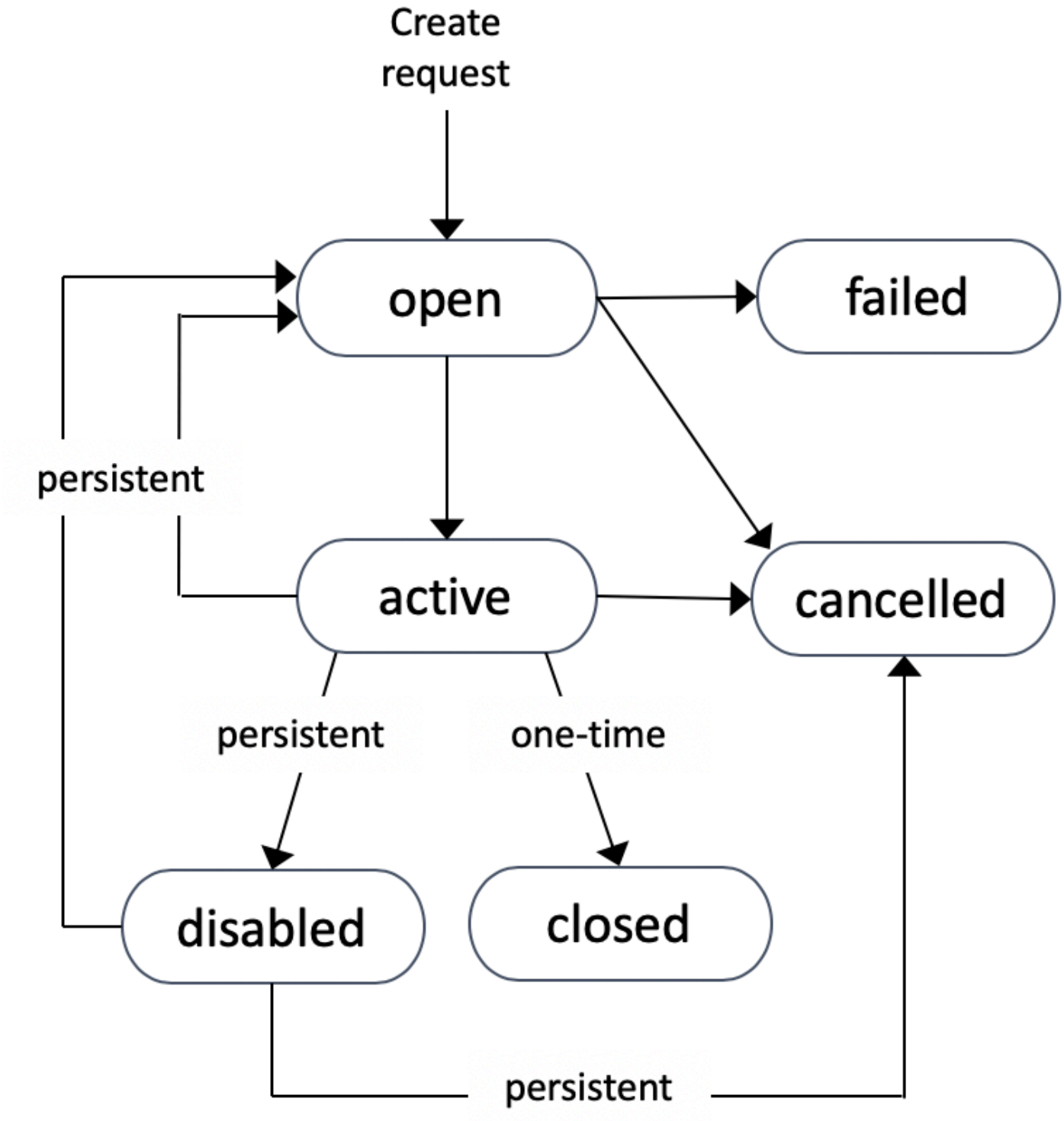
- Trova le tue istanze Spot
- Assegnare tag alle richieste di istanza spot
- Annulla una richiesta di istanza spot
- Arrestare un'istanza spot
- Avviare un'istanza spot
- Terminare un'istanza spot
- Esempio delle specifiche di avvio di una richiesta di istanza spot

Stati della richiesta di istanza spot

Una richiesta di istanza spot può avere uno dei seguenti stati:

- `open` - La richiesta è in attesa di essere soddisfatta.
- `active` - La richiesta è stata soddisfatta e ha un'istanza spot associata.
- `failed` - La richiesta ha uno o più parametri errati.
- `closed` - L'istanza spot è stata interrotta o terminata.
- `disabled` - L'istanza spot è stata interrotta.
- `cancelled` - La richiesta è stata annullata o è scaduta.

La figura che segue rappresenta le transizioni tra gli stati della richiesta. Le transizioni dipendono dal tipo di richiesta (una tantum o persistente).



Una richiesta di istanza spot una tantum rimane attiva fino a quando Amazon EC2 non avvia l'istanza spot, la richiesta scade oppure si annulla la richiesta. Se non è disponibile capacità, l'istanza spot viene terminata e la richiesta di istanza spot viene chiusa.

Una richiesta di istanza spot persistente rimane attiva fino a quando non scade o non viene annullata, anche se la richiesta viene soddisfatta. Se non è disponibile capacità, l'istanza spot viene interrotta. Dopo l'interruzione dell'istanza, quando diventa nuovamente disponibile capacità, l'istanza spot viene avviata, se era stata arrestata, o viene ripresa, se era stata ibernata. Puoi arrestare un'istanza spot e riavviarla se è disponibile capacità. Se l'istanza spot viene terminata (indipendentemente dal fatto che l'istanza spot sia in stato di arresto o esecuzione), la richiesta di istanza spot viene nuovamente aperta e Amazon EC2 avvia una nuova istanza spot. Per ulteriori informazioni, consulta Arrestare un'istanza spot, Avviare un'istanza spot e Terminare un'istanza spot.

È possibile monitorare lo stato delle richieste di istanza spot così come lo stato delle istanze spot avviate attraverso lo stato. Per ulteriori informazioni, consulta Stato della richiesta Spot.

Specificare una tenancy per le Istanze spot

È possibile eseguire un'istanza spot su hardware a tenant singolo. Le istanze Spot dedicate sono fisicamente isolate dalle istanze che appartengono ad altri account. AWS Per ulteriori informazioni, consultare Istanze dedicate Amazon EC2 e la pagina prodotto Istanze Amazon EC2 dedicate.

Per eseguire un'istanza spot dedicata, procedere in uno dei seguenti modi:

- Specifica una tenancy di `dedicated` durante la creazione della richiesta di istanza spot. Per ulteriori informazioni, consulta Creare una richiesta di istanza spot.
- Richiedere un'istanza spot in un VPC con una tenancy di istanza di `dedicated`. Per ulteriori informazioni, consulta Avvia istanze dedicate in un VPC con tenancy predefinita. Non è possibile richiedere un'istanza spot con una tenancy di `default` se viene richiesta in uno VPC con una tenancy di istanza di `dedicated`.

Tutte le famiglie di istanze supportano Istanze spot dedicato fatta eccezione per le istanze T Per ogni famiglia di istanze supportata, solo la dimensione di istanza più grande o la dimensione del metallo supporta le Istanze spot dedicate.

Ruolo collegato ai servizi per le richieste di istanza spot

Amazon EC2 utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri servizi AWS per tuo conto. Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente a un servizio. AWS I ruoli collegati ai servizi forniscono un modo sicuro per delegare le autorizzazioni ai AWS servizi perché solo il servizio collegato può assumere un ruolo collegato al servizio. Per ulteriori informazioni, consultare Utilizzo di ruoli collegati ai servizi nella Guida per l'utente di IAM.

Amazon EC2 utilizza il ruolo collegato al servizio denominato AWSServiceRoleForEC2Spotper avviare e gestire le istanze Spot per tuo conto.

Autorizzazioni concesse da AWSServiceRoleForEC2Spot

Amazon EC2 utilizza AWSServiceRoleForEC2Spotper completare le seguenti azioni:

- `ec2:DescribeInstances` - Descrive le istanze spot
- `ec2:StopInstances` - Arresta istanze spot
- `ec2:StartInstances` - Avvia istanze spot

Creazione del ruolo collegato ai servizi

In gran parte dei casi, non è necessario creare manualmente un ruolo collegato ai servizi. Amazon EC2 crea il ruolo AWSServiceRoleForEC2Spotcollegato al servizio la prima volta che richiedi un'istanza Spot utilizzando la console.

Se hai ricevuto una richiesta di istanza Spot attiva prima di ottobre 2017, quando Amazon EC2 ha iniziato a supportare questo ruolo collegato al servizio, Amazon EC2 ha creato il ruolo nel tuo account. AWSServiceRoleForEC2Spot AWS Per ulteriori informazioni, consulta Visualizzazione di un nuovo ruolo nell'account nella Guida per l'utente di IAM.

Se utilizzi AWS CLI o un'API per richiedere un'istanza Spot, devi prima assicurarti che questo ruolo esista.

Per creare AWSServiceRoleForEC2Spot utilizzando la console

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella pagina Select type of trusted entity (Seleziona tipo di entità attendibile) selezionare EC2, EC2 - Spot Instances (EC2 – Istanze spot), quindi scegliere Next: Permissions (Successivo: Autorizzazioni).
5. Nella pagina successiva, scegliere Next: Review (Successivo: Revisione).
6. Nella pagina Review (Revisione), scegliere Create Role (Crea ruolo).

Per creare AWSServiceRoleForEC2Spotutilizzando AWS CLI

Utilizza il comando create-service-linked-role come riportato di seguito.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Se non hai più bisogno di utilizzare le istanze Spot, ti consigliamo di eliminare il AWSServiceRoleForEC2Spotruolo. Dopo che questo ruolo è stato eliminato dall'account, Amazon EC2 creerà di nuovo il ruolo se verranno richieste le Istanze spot.

Concessione dell'accesso alle chiavi gestite dal cliente per l'uso con le AMI crittografate e gli snapshot EBS

Se specifichi un'AMI crittografata o uno snapshot Amazon EBS crittografato per le tue istanze Spot e utilizzi una chiave gestita dal cliente per la crittografia, devi concedere al AWSServiceRoleForEC2Spotruolo l'autorizzazione a utilizzare la chiave gestita dal cliente in modo che Amazon EC2 possa avviare istanze Spot per tuo conto. Per farlo, occorre aggiungere una concessione alla chiave gestita dal cliente, come mostrato nella procedura seguente.

Nel processo di assegnazione delle autorizzazioni, le concessioni rappresentano un'alternativa alle policy delle chiavi. Per ulteriori informazioni, consulta Utilizzo delle concessioni e Utilizzo delle policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

Per concedere al ruolo AWSServiceRoleForEC2Spot l'autorizzazione a utilizzare la chiave gestita dal cliente

- Utilizza il comando create-grant per aggiungere una concessione alla chiave gestita dal cliente e per specificare il principale (il ruolo AWSServiceRoleForEC2Spotcollegato al servizio) a cui viene concessa l'autorizzazione per eseguire le operazioni consentite dalla concessione. La chiave gestita dal cliente è specificata dal parametro `key-id` e dall'ARN della chiave gestita dal cliente. Il principale è specificato dal `grantee-principal` parametro e dall'ARN del ruolo collegato al AWSServiceRoleForEC2Spotservizio.

  ```
  aws kms create-grant \
      --region us-east-1 \
      --key-id arn:aws:kms:us-
  east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
      --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
  spot.amazonaws.com/AWSServiceRoleForEC2Spot \
      --operations "Decrypt" "Encrypt" "GenerateDataKey"
   "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
   "ReEncryptTo"
  ```

Creare una richiesta di istanza spot

Puoi utilizzare la procedura guidata di avvio dell'istanza nella console Amazon EC2 o il comando AWS CLI run-instances per richiedere un'istanza Spot nello stesso modo in cui puoi avviare un'istanza On-Demand. Questo metodo è consigliato solo per i seguenti motivi:

- Stai già utilizzando la procedura guidata di avvio o il comando run-instances per avviare istanze on demand e vuoi semplicemente passare all'avvio delle istanze spot modificando un singolo parametro.
- Non sono necessarie più istanze con diversi tipi di istanza.

Questo metodo generalmente non è raccomandato per l'avvio di istanze spot perché non è possibile specificare più tipi di istanza e non è possibile avviare istanze spot e on demand nella stessa richiesta. Per i metodi preferiti per l'avvio di istanze spot, che includono l'avvio di un parco istanze che include istanze spot e istanze on demand con più tipi di istanze, consulta Qual è il metodo di richiesta Spot migliore da utilizzare?

Se si richiedono più istanze spot alla volta, Amazon EC2 crea richieste di istanza spot separate, così da consentire di monitorare lo stato di ogni richiesta separatamente. Per ulteriori informazioni sul monitoraggio delle richieste di istanza spot, consulta Stato della richiesta Spot.

New console

Per creare una richiesta di istanza spot utilizzando la procedura guidata per l'avvio delle istanze

I passaggi da 1 a 9 sono gli stessi passaggi da utilizzare per avviare un'istanza on demand. Al passaggio 10, configuri la richiesta di istanza spot.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore della schermata seleziona la regione.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
4. (Facoltativo) In)Name and tags (Nome e tag), puoi assegnare un nome all'istanza e aggiungere un tag alla richiesta di istanza spot, all'istanza, ai volumi e alla grafica elastica. Per ulteriori informazioni sui tag, consulta Tagging delle risorse Amazon EC2..
   a. Per Name (Nome), inserisci un nome descrittivo per l'istanza.

Il nome dell'istanza è un tag, dove la chiave è Name (Nome) e il valore è il nome specificato. Se non si specifica un nome, l'istanza può essere identificata dal relativo ID, che viene generato automaticamente all'avvio dell'istanza.

b. Per aggiungere tag alla richiesta di istanza spot, all'istanza, ai volumi e alla grafica elastica, scegli Add additional tags (Aggiungi altri tag). Scegliere Add tag (Aggiungi tag), quindi immettere una chiave e un valore e selezionare il tipo di risorsa da taggare. Scegliere Add tag (Aggiungi tag) per ogni tag aggiuntivo.

5. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), scegli il sistema operativo (SO) per la tua istanza, quindi seleziona un'AMI. Per ulteriori informazioni, consulta Immagini di applicazioni e sistema operativo (Amazon Machine Image).
6. In Instance type (Tipo di istanza), seleziona il tipo di istanza che soddisfa i requisiti per la configurazione hardware e le dimensioni dell'istanza. Per ulteriori informazioni, consulta Tipo di istanza.
7. In Key pair (login) (Coppia di chiavi [login]), scegli una coppia di chiavi esistente oppure scegli Create new key pair (Crea nuova coppia di chiavi) per creane una nuova. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.

> **Important**
>
> Se si sceglie l'opzione Proceed without key pair (Not recommended) (Procedi senza una coppia di chiavi [non consigliato]), non sarà possibile connetterti all'istanza a meno che non si scelga un'AMI configurata per offrire agli utenti un metodo di accesso alternativo.

8. In Network settings (Impostazioni di rete), utilizza le impostazioni predefinite o scegli Edit (Modifica) per configurare le impostazioni di rete come necessario.

   I gruppi di sicurezza fanno parte delle impostazioni di rete e definiscono le regole del firewall per l'istanza. Tali regole specificano quale traffico di rete in entrata deve viene distribuito sulla tua istanza.

   Per ulteriori informazioni, consulta Impostazioni di rete.
9. L'AMI selezionata include uno o più volumi di storage, compreso il volume dispositivo root. In Configure storage (Configura archiviazione), è possibile specificare altri volumi da collegare

all'istanza scegliendo Add New Volume (Aggiungi nuovo volume). Per ulteriori informazioni, consulta Per configurare l'archiviazione.

10. In Advanced details (Dettagli avanzati), configura la richiesta di istanza spot nel modo seguente:

    a. In Purchasing option (Opzione di acquisto), seleziona la casella di spunta Request Spot Instances (Richiedi istanze spot).

    b. È possibile mantenere la configurazione predefinita per la richiesta dell'istanza spot o scegliere Customize (Personalizza) (a destra) per specificare impostazioni personalizzate per la richiesta di istanza spot.

    Quando scegli Customize (Personalizza) vengono visualizzati i seguenti campi.

    i. Maximum price (Prezzo massimo): puoi richiedere istanze spot al prezzo Spot, con limite massimo pari al prezzo on demand, oppure specificare l'importo massimo che intendi pagare.

> **Warning**
>
> Se specifichi un prezzo massimo, le tue istanze verranno interrotte con maggiore frequenza rispetto a quando scegli Nessun prezzo massimo.

- No maximum price (Nessun prezzo massimo): l'istanza spot verrà avviata al prezzo Spot corrente. Il prezzo non supererà mai il prezzo on demand. (Consigliato)
- Set your maximum price (per instance/hour) (Imposta il prezzo massimo [per istanza/ora]): puoi specificare l'importo massimo che intendi pagare.
  - Se specifichi un prezzo massimo inferiore al prezzo Spot corrente, l'istanza spot non viene avviata.
  - Se specifichi un prezzo massimo superiore al prezzo Spot corrente, la tua istanza spot viene avviata e viene addebitato il prezzo Spot corrente. Dopo l'esecuzione dell'istanza spot, se il prezzo Spot sale al di sopra del prezzo massimo, Amazon EC2 interrompe l'istanza spot.
  - Indipendentemente dal prezzo massimo specificato, ti verrà sempre addebitato il prezzo spot corrente.

Per esaminare le tendenze del prezzo Spot, consultare Cronologia dei prezzi dell'istanza spot.

ii. Request type (Tipo richiesta): il tipo di richiesta di istanza spot scelto determina cosa succede se l'istanza spot viene interrotta.

- One-time (Una tantum): Amazon EC2 effettua una richiesta una tantum per la tua istanza spot. Se l'istanza spot viene interrotta, la richiesta non viene inviata di nuovo.
- Persistent request (Richiesta persistente): Amazon EC2 invia una richiesta persistente per la tua istanza spot. Se l'istanza spot viene interrotta, la richiesta viene nuovamente inviata per ricostituire l'istanza spot interrotta.

Se non specifichi un valore, il valore predefinito è una richiesta una tantum.

iii. Valid to (Valido per): la data di scadenza di una richiesta di istanza spot persistente.

Questo campo non è supportato per le richieste una tantum. Una richiesta una tantum rimane attiva fino a quando tutte le istanze nella richiesta non vengono avviate o non si annulla la richiesta.

- No request expiry date (Nessuna data di scadenza della richiesta): la richiesta rimane attiva fino a quando non viene annullata.
- Set your request expiry date (Imposta la data di scadenza della richiesta): la richiesta persistente rimane attiva fino alla data specificata o fino alla cancellazione.

iv. Interruption behavior (Comportamento di interruzione): il comportamento scelto determina cosa succede quando un'istanza spot viene interrotta.

- Per le richieste persistenti, i valori validi sono Stop (Arresta) e Hibernate (Iberna). Quando un'istanza viene interrotta, si applicano gli addebiti per l'archiviazione del volume EBS.

> **Note**
>
> Le istanze spot ora utilizzano la stessa funzionalità di ibernazione delle istanze on demand. Per abilitare l'ibernazione, puoi scegliere Iberna qui oppure puoi scegliere Abilita dal campo Comportamento di

interruzione/ibernazione che appare più in basso nella procedura guidata di avvio dell'istanza. Per i prerequisiti di ibernazione, consulta la pagina Prerequisiti per l'ibernazione delle istanze Amazon EC2.

- Per richieste una tantum, è valido solo il valore Terminate (Termina).

Se non specifichi un valore, il valore predefinito è Terminate (Termina), che non è valido per una richiesta di istanza spot persistente. Se mantieni il valore predefinito e provi a lanciare una richiesta di istanza spot persistente, riceverai un errore.

Per ulteriori informazioni, consulta Comportamento delle interruzioni delle istanze Spot.

11. Nel pannello Summary (Riepilogo), per Number of instances (Numero di istanze), inserisci il numero di istanze da avviare.

> **Note**
>
> Amazon EC2 crea una richiesta separata per ciascuna istanza spot.

12. Nel pannello Summary (Riepilogo), rivedi i dettagli della tua istanza e apporta tutte le modifiche necessarie. Dopo aver inviato la richiesta di istanza spot, non è più possibile modificare i parametri della richiesta. È possibile passare direttamente a una sezione nella procedura guidata di avvio delle istanze scegliendo il relativo collegamento nel pannello Summary (Riepilogo). Per ulteriori informazioni, consulta Riepilogo.
13. Quando si è pronti per avviare l'istanza, scegliere Launch instance (Avvia istanza).

    Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

Old console

Per creare una richiesta di istanza spot utilizzando la procedura guidata per l'avvio delle istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore della schermata seleziona la regione.
3. Dal pannello di controllo della console Amazon EC2, scegliere Launch Instance (Avvia istanza).

4. Nella pagina Scegliere un'Amazon Machine Image (AMI) scegli un'AMI. Per ulteriori informazioni, consulta Fase 1: scelta di un'Amazon Machine Image (AMI).
5. Nella pagina Choose an Instance Type (Scegli un tipo di istanza), seleziona la configurazione hardware e le dimensioni dell'istanza da avviare, quindi scegli Next: Configure Instance Details (Successivo: Configura i dettagli dell'istanza). Per ulteriori informazioni, consulta Fase 2: scegliere un tipo di istanza.
6. Nella pagina Configure Instance Details (Configura i dettagli dell'istanza) configura la richiesta di istanza spot nel modo seguente:

   - Number of instances (Numero di istanze): immettere il numero di istanze da avviare.

     > **Note**
     >
     > Amazon EC2 crea una richiesta separata per ciascuna istanza spot.

   - (Opzionale) Per assicurarsi di disporre del numero corretto di istanze per la gestione del carico di richieste dell'applicazione, è possibile scegliere Launch into Auto Scaling Group (Avvio nel gruppo Auto Scaling) per creare una configurazione di avvio e un gruppo Auto Scaling. La funzionalità Auto Scaling dimensiona il numero di istanze nel gruppo in base alle specifiche. Per ulteriori informazioni, consulta Guida per l'utente di Amazon EC2 Auto Scaling.
   - Purchasing option (Opzioni di acquisto): selezionare Request Spot Instances (Richiedi istanze spot) per avviare un'istanza spot. Quando scegli questa opzione vengono visualizzati i seguenti campi.
   - Prezzo corrente: il prezzo Spot corrente in ogni zona di disponibilità viene visualizzato per il tipo di istanza selezionato.
   - (Opzionale) Prezzo massimo: puoi lasciare vuoto il campo oppure specificare l'importo massimo che sei disposto a pagare.

     > **Warning**
     >
     > Se specifichi un prezzo massimo, le tue istanze verranno interrotte con maggiore frequenza rispetto a quando lasci il campo vuoto.

     - Se specifichi un prezzo massimo inferiore al prezzo spot corrente, l'istanza spot non verrà avviata.

- Se specifichi un prezzo massimo superiore al prezzo Spot corrente, la tua istanza spot viene avviata e viene addebitato il prezzo Spot corrente. Dopo l'esecuzione dell'istanza spot, se il prezzo Spot sale al di sopra del prezzo massimo, Amazon EC2 interrompe l'istanza spot.
- Indipendentemente dal prezzo massimo specificato, ti verrà sempre addebitato il prezzo spot corrente.
- Se lasci vuoto il campo, pagherai il prezzo spot corrente.

- Persistent request (Richiesta persistente): scegli Richiesta persistente per inviare nuovamente la richiesta di istanza spot nel caso in cui la richiesta venga interrotta.
- Interruption behavior (Comportamento di interruzione): per impostazione predefinita, il servizio Spot termina un'istanza spot quando viene interrotta. Se scegli Richiesta persistente, puoi specificare che il servizio Spot si arresti o si iberni quando la tua istanza spot viene interrotta. Per ulteriori informazioni, consulta Comportamento delle interruzioni delle istanze Spot.
- (Opzionale) Request valid to (Richiesta valida fino a): scegli Modifica (Edit) per specificare quando scade la richiesta di istanza spot.

Per ulteriori informazioni sulla configurazione di una istanza spot, consulta Fase 3: configurare i dettagli dell'istanza.

7. L'AMI selezionata include uno o più volumi di storage, compreso il volume dispositivo root. Nella pagina Add Storage (Aggiungi storage), è possibile specificare altri volumi da collegare all'istanza scegliendo Add New Volume (Aggiungi nuovo volume). Per ulteriori informazioni, consulta Fase 4: aggiungere archiviazione.
8. Nella pagina Add Tags (Aggiungi tag), specificare i tag immettendo le combinazioni di chiave e valore. Per ulteriori informazioni, consulta Fase 5: aggiungi i tag.
9. Nella pagina Configure Security Group (Configura il gruppo di sicurezza), selezionare un gruppo di sicurezza per definire le regole del firewall per l'istanza. Tali regole specificano quale traffico di rete in entrata deve viene distribuito sulla tua istanza. Tutto il traffico rimanente verrà ignorato. Per ulteriori informazioni sui gruppi di sicurezza, consulta Gruppi di sicurezza Amazon EC2 per le tue istanze EC2. Seleziona o crea un gruppo di sicurezza e scegli Analizza e avvia. Per ulteriori informazioni, consulta Fase 6: configura il gruppo di sicurezza.
10. Nella pagina Review Instance Launch (Rivedi l'avvio dell'istanza), controllare i dettagli dell'istanza e apportare le modifiche necessarie scegliendo il collegamento Edit (Modifica)

appropriato. Al termine, scegliere Launch (Avvia). Per ulteriori informazioni, consulta Fase 7: rivedere l'avvio dell'istanza e selezionare la coppia di chiavi.

11. Nella finestra di dialogo Select an existing key pair or create a new key pair (Seleziona una coppia di chiavi esistente o crea una nuova coppia di chiavi), è possibile scegliere una coppia di chiavi esistenti o crearne una nuova. Ad esempio, seleziona Scegli una coppia di chiavi esistente, quindi scegli la coppia di chiavi creata durante la configurazione. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.

    > **Important**
    >
    > Se scegli l'opzione Proceed without key pair (Procedi senza una coppia di chiavi), non sarai in grado di connetterti all'istanza a meno che tu non scelga un'AMI configurata per offrire agli utenti un metodo di accesso alternativo.

12. Per avviare l'istanza, selezionare la casella di controllo di conferma, quindi scegliere Launch Instances (Avvia istanze).

    Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

AWS CLI

Per creare una richiesta di istanza spot utilizzando run-instances

Utilizza il comando run-instances e specifica le opzioni dell'istanza spot nel parametro `--instance-market-options`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 5 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --instance-market-options file://spot-options.json
```

Di seguito è riportata la struttura dati da specificare nel file JSON per `--instance-market-options`. Puoi inoltre specificare `ValidUntil` e `InstanceInterruptionBehavior`. Se non specifichi un campo nella struttura dati viene utilizzato il valore predefinito.

Nell'esempio seguente viene creata una richiesta `persistent`.

```
{
  "MarketType": "spot",
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
}
```

Per creare una richiesta di istanza Spot utilizzando request-spot-instances

> **Note**
>
> Sconsigliamo vivamente di utilizzare il request-spot-instancescomando per richiedere un'istanza Spot perché si tratta di un'API legacy senza investimenti pianificati. Per ulteriori informazioni, consulta Qual è il metodo di richiesta Spot migliore da utilizzare?

Utilizza il request-spot-instancescomando per creare una richiesta una tantum.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

Usa il request-spot-instancescomando per creare una richiesta persistente.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

Per i file di esempio delle specifiche di lancio da utilizzare con questi comandi, consultare Esempio delle specifiche di avvio di una richiesta di istanza spot. Se scarichi un file delle specifiche di avvio dalla console Spot Requests, devi invece utilizzare il request-spot-fleetcomando (la console Spot Requests specifica una richiesta di istanza Spot utilizzando una flotta Spot).

Trova le tue istanze Spot

Amazon EC2 avvia un'istanza spot quando è disponibile capacità. Un'istanza spot viene eseguita fino a quando non viene interrotta o fino a quando non la si termina.

Un'istanza Spot viene visualizzata nella pagina Istanze della console, insieme alle istanze On-Demand. Utilizza la seguente procedura per trovare le tue istanze Spot.

Console

Per trovare le tue istanze Spot utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Per trovare tutte le istanze Spot, nel riquadro di ricerca, scegli Instance lifecycle=spot.
4. Per verificare che un'istanza sia un'istanza Spot, seleziona l'istanza, scegli la scheda Dettagli e controlla il valore di Lifecycle. Il valore per un'istanza Spot è `spot` e il valore per un'istanza On-Demand è. `normal`

AWS CLI

Per trovare le tue istanze Spot, utilizza il AWS CLI

Usa il comando describe-instances con l'opzione. `--filters`

```
aws ec2 describe-instances \
    --filters "Name=instance-lifecycle,Values=spot"
```

Per determinare se un'istanza è un'istanza Spot

Utilizzate il comando describe-instances, utilizzando l'`--query`opzione per controllare il valore del ciclo di vita.

```
aws ec2 describe-instances \
    --instance-ids i-0123a456700123456 \
    --query "Reservations[*].Instances[*].InstanceLifecycle" \
    --output text
```

Se l'output è, l'istanza è un'`spot`istanza Spot. Se non è presente alcun output, l'istanza è un'istanza On-Demand.

Utilizza la seguente procedura per trovare le istanze Spot lanciate da una richiesta specifica di istanza Spot o Fleet Spot.

Console

Per trovare le istanze Spot per una richiesta utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot). L'elenco contiene sia le richieste di istanze Spot che le richieste Spot Fleet.
3. Se una richiesta di istanza Spot viene soddisfatta, Capacity è l'ID dell'istanza Spot. Per un Parco istanze spot, Capacity (Capacità) indica quanta capacità richiesta è stata soddisfatta. Per visualizzare gli ID delle istanze in un Parco istanze spot, scegliere la freccia per l'espansione o selezionare il parco istanze e scegliere Instances (Istanze).
4. Per una flotta Spot, Capacity indica quanta parte della capacità richiesta è soddisfatta. Per visualizzare gli ID delle istanze in un parco istanze Spot, scegli l'ID del parco istanze per aprirne la pagina dei dettagli e individuare il riquadro Istanze.

AWS CLI

Per trovare le istanze Spot per una richiesta, utilizza il AWS CLI

Usa il describe-spot-instance-requestscomando con l'`--query`opzione.

```
aws ec2 describe-spot-instance-requests \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

Di seguito è riportato un output di esempio:

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
    }
]
```

Assegnare tag alle richieste di istanza spot

Per categorizzare e gestire le richieste di istanza spot, è possibile contrassegnarle con tag contenenti metadati personalizzati. È possibile assegnare un tag a una richiesta di istanza spot alla sua creazione o successivamente. È possibile assegnare tag utilizzando la console Amazon EC2 o lo strumento da riga di comando.

Quando applichi un tag a una richiesta di istanza spot, alle istanze e ai volumi che vengono avviati dalla richiesta di istanza spot non viene automaticamente applicato il tag. È necessario applicare esplicitamente il tag alle istanze e ai volumi avviati dalla richiesta di istanza spot. Puoi assegnare un tag a un'istanza spot e ai volumi durante l'avvio o successivamente.

Per ulteriori informazioni sul funzionamento dei tag, consultare Tagging delle risorse Amazon EC2..

Indice

Prerequisiti

Concedi all'utente l'autorizzazione per taggare le risorse. Per ulteriori informazioni sulle policy IAM e sulle policy di esempio, consulta Esempio: aggiunta di tag alle risorse.

La policy IAM creata viene determinata dal metodo utilizzato per creare una richiesta di istanza spot.

- Se usi la procedura guidata per l'avvio dell'istanza o `run-instances` per richiedere le Istanze spot, consulta To grant a user the permission to tag resources when using the launch instance wizard or run-instances.
- Se utilizzi il comando `request-spot-instances` per richiedere istanze spot, consulta To grant a user the permission to tag resources when using request-spot-instances.

Per concedere a un utente l'autorizzazione ad applicare un tag alle risorse quando usa la procedura guidata per l'avvio dell'istanza o run-instances

Creare una policy IAM che include quanto segue:

- L'operazione `ec2:RunInstances`. Ciò concede all'utente l'autorizzazione per avviare un'istanza.
- Per `Resource`, specificare `spot-instances-request`. Ciò consente agli utenti di creare richieste di istanze spot che richiedono istanze spot.
- L'operazione `ec2:CreateTags`. Ciò concede all'utente l'autorizzazione per creare tag.
- Per `Resource`, specificare `*`. Ciò consente agli utenti di applicare un tag a tutte le risorse create durante l'avvio dell'istanza.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Quando utilizzi l' RunInstances azione per creare richieste di istanze Spot e tagghi le richieste di istanze Spot al momento della creazione, devi essere consapevole di come Amazon EC2 valuta la `spot-instances-request` risorsa nella RunInstances dichiarazione in cui viene valutata nella policy IAM come segue:

- Se non tagghi una richiesta di istanza Spot al momento della creazione, Amazon EC2 non valuta la `spot-instances-request` risorsa nell' RunInstancesistruzione.
- Se tagghi una richiesta di istanza Spot al momento della creazione, Amazon EC2 valuta la `spot-instances-request` risorsa nell'istruzione. RunInstances

Pertanto, per la risorsa `spot-instances-request`, alla policy IAM si applicano le seguenti regole:

- Se utilizzi RunInstances per creare una richiesta di istanza Spot e non intendi taggare la richiesta di istanza Spot al momento della creazione, non è necessario consentire esplicitamente la `spot-instances-request` risorsa; la chiamata avrà esito positivo.
- Se utilizzi RunInstances per creare una richiesta di istanza Spot e intendi taggare la richiesta di istanza Spot al momento della creazione, devi includere la `spot-instances-request` risorsa nell'istruzione RunInstances allow, altrimenti la chiamata avrà esito negativo.
- Se utilizzi RunInstances per creare una richiesta di istanza Spot e intendi contrassegnare la richiesta di istanza Spot al momento della creazione, devi specificare la `spot-instances-request` risorsa o includere un `*` carattere jolly nell'istruzione CreateTags allow, altrimenti la chiamata avrà esito negativo.

Per policy IAM di esempio, incluse le policy non supportate per le richieste di istanza spot, consulta Utilizzo delle Istanze spot.

Concedere a un utente l'autorizzazione a taggare le risorse durante l'utilizzo request-spot-instances

Creare una policy IAM che include quanto segue:

- L'operazione `ec2:RequestSpotInstances`. Ciò concede all'utente l'autorizzazione per creare una richiesta di istanza spot.
- L'operazione `ec2:CreateTags`. Ciò concede all'utente l'autorizzazione per creare tag.
- Per `Resource`, specificare `spot-instances-request`. Ciò consente agli utenti di applicare il tag solo alla richiesta di istanza spot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-request/*"
}
```

Assegnare tag a una nuova richiesta di istanza spot

Console

Per assegnare tag a una nuova richiesta di istanza spot utilizzando la console

1. Seguire la procedura Creare una richiesta di istanza spot.
2. Per aggiungere un tag, scegli Aggiungi tag nella pagina Aggiungi tag e immetti la chiave e il valore per il tag. Scegli Aggiungi un altro tag per ogni tag aggiuntivo.

   Per ogni tag, è possibile assegnare lo stesso tag alla richiesta di istanza spot, alle istanze spot e ai volumi. Per applicare tag a tutti e tre, assicurarsi che Instances (Istanze), Volumes (Volumi) e Requests (Richieste) siano selezionati. Per applicare solo uno o due tag, assicurati che le risorse a cui vuoi applicare il tag siano selezionate e che le altre risorse siano cancellate.
3. Completare i campi obbligatori per creare una richiesta di istanza spot, quindi scegliere Launch (Avvia). Per ulteriori informazioni, consulta Creare una richiesta di istanza spot.

AWS CLI

Per etichettare una nuova richiesta di istanza Spot utilizzando il AWS CLI

Per assegnare tag a una richiesta di istanza spot al momento della creazione, configurare la richiesta di istanza spot nel modo seguente:

- Specifica i tag per la richiesta di istanza spot utilizzando il parametro `--tag-specification`.
- Per `ResourceType`, specificare `spot-instances-request`. Indicando un altro valore, la richiesta di istanza spot non riesce.
- Per `Tags`, specificare la coppia chiave-valore. È possibile specificare più coppie chiave-valore.

Nel seguente esempio, alla richiesta di istanza spot sono assegnati due tag: Key=Environment e Value=Production, e Key=Cost-Center e Value=123.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

Assegnare tag a una richiesta di istanza spot esistente

Console

Per assegnare tag a una richiesta di istanza spot esistente utilizzando la console

Dopo aver creato una richiesta di istanza spot, è possibile aggiungere tag alla richiesta del parco istanze spot utilizzando la console.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di istanza spot.
4. Scegliere la scheda Tags e scegliere Create Tag (Crea tag).

Per assegnare tag a un'istanza spot esistente utilizzando la console

Dopo che la richiesta di istanza spot ha avviato l'istanza spot, puoi aggiungere i tag all'istanza utilizzando la console. Per ulteriori informazioni, consulta Aggiunta ed eliminazione di tag in una singola risorsa.

AWS CLI

Per etichettare una richiesta di istanza Spot o un'istanza Spot esistente utilizzando il AWS CLI

Utilizzare il comando create-tags per aggiungere un tag alle risorse esistenti. Nell'esempio seguente, la richiesta di istanza spot esistente e l'istanza spot includono il tag Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources sir-08b93456 i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

Visualizzare i tag della richiesta di istanza spot

Console

Per visualizzare i tag di una richiesta di istanza spot utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare la richiesta di istanza spot e scegliere la scheda Tags.

AWS CLI

Per descrivere i tag della richiesta di istanza spot

Puoi visualizzare i tag di una richiesta di istanza Spot descrivendo la richiesta di istanza Spot. Utilizza il describe-spot-instance-requestscomando per visualizzare la configurazione della richiesta di istanza Spot specificata, che include tutti i tag specificati per la richiesta.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-EXAMPLE1 \
    --query "SpotInstanceRequests[*].Tags"
```

Di seguito è riportato un output di esempio.

```
[
    [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Department",
            "Value": "101"
        }
    ]
]
```

Annulla una richiesta di istanza spot

È possibile annullare la richiesta di istanza spot se non la si desidera più. È possibile annullare solo le richieste di istanza spot che risultano `open`, `active` o `disabled`.

- La richiesta di istanza spot risulta `open` quando la richiesta non è stata ancora soddisfatta e non è stata avviata alcuna istanza.
- La richiesta di istanza spot risulta `active` quando la richiesta è stata soddisfatta e, di conseguenza, sono state avviate le istanze spot.
- La richiesta di istanza spot risulta `disabled` quando si arresta l'istanza spot.

Se la richiesta di istanza spot risulta `active` e ha un'istanza spot associata in esecuzione, l'annullamento della richiesta non termina l'istanza. Per ulteriori informazioni sulla terminazione delle istanze spot, consulta Terminare un'istanza spot.

Console

Per annullare una richiesta di istanza Spot utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di istanza Spot.
4. Scegli Operazioni e Annulla richiesta.
5. (Facoltativo) Se si è finito con le Istanze spot associate, è possibile terminarle. Nella finestra di dialogo Elimina richiesta Spot seleziona Termina istanze, quindi scegli Conferma.

AWS CLI

Per annullare una richiesta di istanza Spot utilizzando il AWS CLI

Utilizza il cancel-spot-instance-requestscomando per annullare la richiesta di istanza Spot specificata.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Arrestare un'istanza spot

Se al momento non hai bisogno dell'Istanze spot, ma vuoi riavviarla in un secondo momento senza perdere i dati persistenti nel volume Amazon EBS, puoi arrestarla. I passaggi per arrestare un'istanza spot sono simili a quelli richiesti per arrestare un'istanza on demand.

> **Note**
>
> Durante l'arresto di un'istanza spot, è possibile modificare alcuni attributi dell'istanza, ma non il tipo di istanza.
> Non addebitiamo costi per l'utilizzo di un'istanza spot arrestata o per il trasferimento di dati, ma li addebitiamo per l'archiviazione di tutti i volumi Amazon EBS.

Limitazioni

- È possibile arrestare un'istanza spot solo se l'istanza spot è stata avviata da una richiesta Spot `persistent`.
- Non è possibile arrestare un'istanza spot se la richiesta Spot associata è stata annullata. Se la richiesta dell'istanza spot viene annullata, è possibile solo terminare l'istanza spot.
- Non è possibile interrompere un'istanza spot se fa parte di un parco istanze o un gruppo di avvio o di un gruppo di zone di disponibilità.

Console

Per interrompere un'istanza Spot utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza Spot. Se non hai salvato l'ID dell'istanza Spot, vedithe section called “Trova le tue istanze Spot”.
4. Scegli Instance state (Stato istanza), Stop instance (Arresta istanza).
5. Quando viene richiesta la conferma, selezionare Stop (Arresta).

AWS CLI

Per interrompere un'istanza Spot utilizzando il AWS CLI

Utilizza il comando stop-instances per arrestare manualmente le tue istanze Spot.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

Avviare un'istanza spot

È possibile avviare un'istanza spot che hai arrestato in precedenza.

Prerequisiti

È possibile avviare un'istanza spot solo se:

- L'istanza spot è stata arrestata manualmente.
- L'istanza spot è supportata EBS.
- La capacità dell'istanza spot è disponibile.
- Il prezzo Spot è inferiore al prezzo massimo.

Limitazioni

- Non è possibile avviare un'istanza spot se fa parte del parco istanze o del gruppo di avvio o di un gruppo di zone di disponibilità.

I passaggi per avviare un'istanza spot sono simili a quelli richiesti per avviare un'istanza on demand.

Console

Per avviare un'istanza Spot utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza Spot. Se non hai salvato l'ID dell'istanza Spot, vedithe section called “Trova le tue istanze Spot”.
4. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).

AWS CLI

Per avviare un'istanza Spot AWS CLI

Utilizza il comando start-instances per avviare manualmente le tue istanze Spot.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

Terminare un'istanza spot

Se si termina un'istanza spot in esecuzione o arrestata che era stata avviata da una richiesta Spot persistente, la richiesta dell'istanza spot passa allo stato `open` per consentire che venga avviata una nuova istanza spot. Per garantire che non venga avviata una nuova istanza spot, è necessario annullare prima la richiesta Spot.

Se si annulla una richiesta dell'istanza spot `active` che ha un'istanza spot in esecuzione, l'istanza spot in esecuzione non viene terminata automaticamente ma sarà necessario terminarla manualmente.

Se si annulla una richiesta dell'istanza spot `disabled` che ha un'istanza spot interrotta, l'istanza spot interrotta viene terminata automaticamente dal servizio Spot di Amazon EC2. Potrebbe verificarsi un breve ritardo tra l'annullamento della richiesta dell'istanza spot e il momento in cui il servizio Spot termina l'istanza spot.

Per ulteriori informazioni, consulta Annulla una richiesta di istanza spot.

Console

Per terminare manualmente un'istanza spot utilizzando la console

1. Prima di terminare l'istanza, verificare che l'operazione non comporti la perdita dei dati. A tale scopo, controllare che i volumi Amazon EBS non vengano eliminati dopo l'interruzione e assicurarsi di aver copiato i dati necessari dai volumi di instance store nello storage persistente, ad esempio Amazon EBS o Amazon S3.
2. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
3. Nel riquadro di navigazione, seleziona Istanze.
4. Seleziona l'istanza Spot. Se non hai salvato l'ID dell'istanza Spot, vedithe section called “Trova le tue istanze Spot”.
5. Scegli Instance state (Stato istanza), Terminate instance (Termina istanza).
6. Quando viene richiesta la conferma, seleziona Terminate (Interrompi).

AWS CLI

Per terminare manualmente un'istanza Spot utilizzando AWS CLI

Utilizza il comando terminate-instances per terminare manualmente le tue istanze Spot.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

Esempio delle specifiche di avvio di una richiesta di istanza spot

Gli esempi seguenti mostrano le configurazioni di avvio che è possibile utilizzare con il request-spot-instancescomando per creare una richiesta di istanza Spot. Per ulteriori informazioni, consulta Creare una richiesta di istanza spot.

> **Important**
>
> Sconsigliamo vivamente di utilizzare il request-spot-instancescomando per richiedere un'istanza Spot perché si tratta di un'API legacy senza investimenti pianificati. Per ulteriori informazioni, consulta Qual è il metodo di richiesta Spot migliore da utilizzare?.

Esempi

- Esempio 1: Avvio di Istanze spot
- Esempio 2: Avviare le Istanze spot nella zona di disponibilità specificata
- Esempio 3: Avvio di Istanze spot nella sottorete specificata
- Esempio 4: Avvio di un'istanza spot dedicata

Esempio 1: Avvio di Istanze spot

L'esempio seguente non include una zona di disponibilità o una sottorete. Amazon EC2 seleziona automaticamente una zona di disponibilità. Amazon EC2 avvia le istanze nella sottorete predefinita della zona di disponibilità selezionata.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
```

```
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Esempio 2: Avviare le Istanze spot nella zona di disponibilità specificata

L'esempio seguente include una zona di disponibilità. Amazon EC2 avvia le istanze nella sottorete predefinita della zona di disponibilità specificata.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Esempio 3: Avvio di Istanze spot nella sottorete specificata

L'esempio seguente include una sottorete. Amazon EC2 avvia le istanze nella sottorete specificata. Se il VPC non è predefinito, l'istanza non riceve un indirizzo IPv4 pubblico per impostazione predefinita.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Per assegnare un indirizzo IPv4 pubblico a un'istanza in un VPC non predefinito, specificare il campo `AssociatePublicIpAddress` come mostrato negli esempi seguenti. Quando specifichi

un'interfaccia di rete, devi includere l'ID sottorete e l'ID gruppo di sicurezza tramite l'interfaccia di rete anziché tramite i campi `SubnetId` e `SecurityGroupIds` visualizzati nel blocco di codice precedente.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Esempio 4: Avvio di un'istanza spot dedicata

L'esempio seguente richiede un'istanza spot con una tenancy di `dedicated`. Un'istanza spot dedicata deve essere avviata in un VPC.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Stato della richiesta Spot

Per aiutarti a monitorare le richieste di istanza spot e a pianificare l'utilizzo delle istanze spot, usa lo stato della richiesta fornito da Amazon EC2. Per esempio, lo stato della richiesta può fornire il

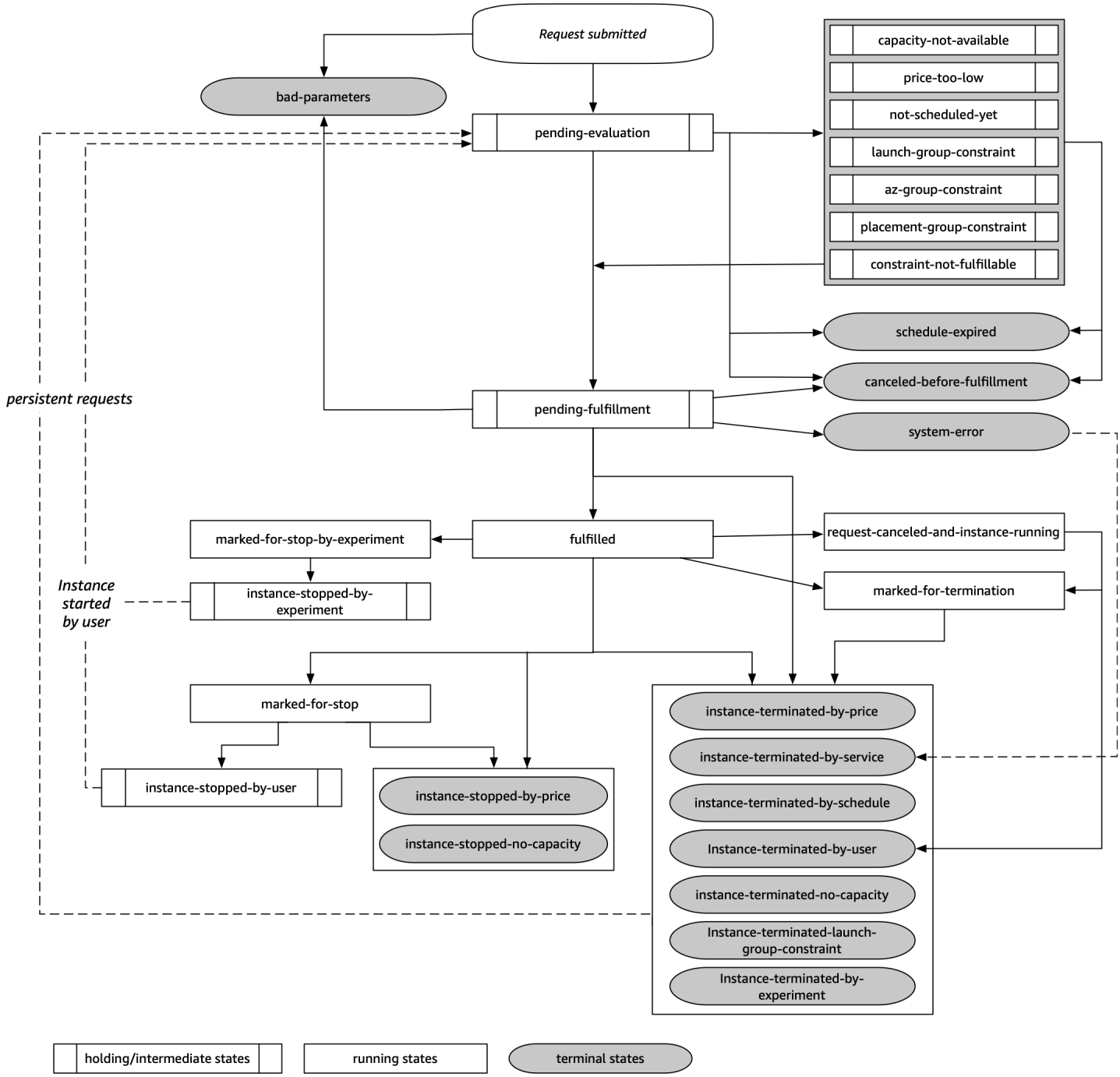
motivo per cui la propria richiesta Spot non è ancora stata soddisfatta, oppure elencare i vincoli che impediscono il soddisfacimento della richiesta Spot.

A ogni fase del processo, detto anche ciclo di vita della richiesta Spot, eventi specifici determinano gli stati successivi della richiesta.

Indice

Ciclo di vita di una richiesta Spot

Il diagramma seguente mostra i percorsi che la richiesta Spot può seguire durante tutto il suo ciclo di vita, dall'invio alla terminazione. Ogni fase è rappresentata come un nodo e il codice di stato per ogni nodo descrive lo stato della richiesta Spot e dell'istanza spot.



Valutazione in attesa

Appena creata, una richiesta di istanza spot passa allo stato `pending-evaluation`, a meno che uno o più parametri di richiesta non risultino non validi (`bad-parameters`).

Codice di stato	Stato della richiesta	Stato istanza
`pending-evaluation`	`open`	Non applicabile
`bad-parameters`	`closed`	Non applicabile

Sospensione

Se uno o più vincoli di richiesta sono validi ma non possono ancora essere soddisfatti o se non c'è sufficiente capacità, la richiesta va in uno stato di sospensione in attesa che i vincoli vengano soddisfatti. Le opzioni di richiesta influiscono sulla probabilità che la richiesta venga soddisfatta. In assenza di capacità, ad esempio, la richiesta rimane in stato di attesa fino a quando è disponibile capacità. Se si specifica un gruppo di zona di disponibilità, la richiesta rimane in uno stato di sospensione finché il vincolo della zona di disponibilità non viene soddisfatto.

Nel caso si verifichi un'interruzione di una delle zone di disponibilità, è possibile che la capacità EC2 inutilizzata disponibile per le richieste di istanza spot in altre zone di disponibilità possa essere interessata.

Codice di stato	Stato della richiesta	Stato istanza
`capacity-not-available`	`open`	Non applicabile
`price-too-low`	`open`	Non applicabile
`not-scheduled-yet`	`open`	Non applicabile
`launch-group-constraint`	`open`	Non applicabile
`az-group-constraint`	`open`	Non applicabile
`placement-group-constraint`	`open`	Non applicabile

Codice di stato	Stato della richiesta	Stato istanza
`constraint-not-fulfillable`	`open`	Non applicabile

Valutazione/adempimento-terminale in sospeso

La richiesta di istanza spot può passare allo stato `terminal` se si crea una richiesta valida solo durante un determinato periodo di tempo, che scade prima che la richiesta raggiunga la fase di evasione in sospeso. se si annulla la richiesta o se si verifica un errore di sistema.

Codice di stato	Stato della richiesta	Stato istanza
`schedule-expired`	`cancelled`	Non applicabile
`canceled-before-fulfillment` [1]	`cancelled`	Non applicabile
`bad-parameters`	`failed`	Non applicabile
`system-error`	`closed`	Non applicabile

[1] Se annulli la richiesta.

Adempimento in sospeso

Quando vengono soddisfatti eventuali vincoli specificati, la richiesta spot passa allo stato `pending-fulfillment`.

A questo punto, Amazon EC2 è quasi pronto ad assegnare le istanze richieste. Se il processo si arresta in questo momento, probabilmente è stato annullato dall'utente prima dell'avvio dell'istanza spot. o si è verificato un errore di sistema imprevisto.

Codice di stato	Stato della richiesta	Stato istanza
`pending-fulfillment`	`open`	

Codice di stato	Stato della richiesta	Stato istanza
		Non applicabile

Soddisfatta

Quando tutte le specifiche delle istanze spot vengono soddisfatte, la richiesta Spot viene soddisfatta. Amazon EC2 avvia le istanze spot; ciò può richiedere alcuni minuti. Se un'istanza spot viene ibernata o arrestata durante la sua interruzione, resta in questo stato finché la richiesta non può essere soddisfatta nuovamente o non viene annullata.

Codice di stato	Stato della richiesta	Stato istanza
`fulfilled`	`active`	`pending` → `running`
`fulfilled`	`active`	`stopped` → `running`

Se arresti un'istanza spot, la richiesta Spot passa allo stato `marked-for-stop` o `instance-stopped-by-user` fino a quando l'istanza spot può essere riavviata o la richiesta viene annullata.

Codice di stato	Stato della richiesta	Stato istanza
`marked-for-stop`	`active`	`stopping`
`instance-stopped-by-user`[1]	`disabled` o `cancelled` [2]	`stopped`

[1] Un'istanza spot passa allo stato `instance-stopped-by-user` se arresti l'istanza o esegui il comando di arresto dall'istanza. Dopo aver arrestato l'istanza, è possibile riavviarla. Al riavvio, la richiesta di istanza spot ritorna allo stato `pending-evaluation` e quindi Amazon EC2 avvia una nuova istanza spot quando vengono soddisfatti i vincoli.

[2] Lo stato della richiesta spot è `disabled` se l'istanza spot viene arrestata ma la richiesta non viene annullata. Lo stato della richiesta è `cancelled` se l'istanza spot viene arrestata e la richiesta scade.

Soddisfatta-terminale

Le istanze spot continuano l'esecuzione fino a quando è disponibile capacità per il tuo tipo di istanza e non termini l'istanza. Se Amazon EC2 deve terminare le istanze spot, la richiesta spot passa a uno stato terminale. Una richiesta passa allo stato terminale anche se si annulla la richiesta Spot o si terminano le Istanze spot.

Codice di stato	Stato della richiesta	Stato istanza
`request-canceled-and-instance-running`	`cancelled`	`running`
`marked-for-stop`	`active`	`running`
`marked-for-termination`	`active`	`running`
`instance-stopped-by-price`	`disabled`	`stopped`
`instance-stopped-by-user`	`disabled`	`stopped`
`instance-stopped-no-capacity`	`disabled`	`stopped`
`instance-terminated-by-price`	`closed` (una tantum), `open` (persistente)	`terminated`
`instance-terminated-by-schedule`	`closed`	`terminated`
`instance-terminated-by-service`	`cancelled`	`terminated`
`instance-terminated-by-user`	`closed` o `cancelled` [1]	`terminated`
`instance-terminated-no-capacity`	`closed` (una tantum), `open` (persistente)	`running` †

Codice di stato	Stato della richiesta	Stato istanza
`instance-terminated-no-capacity`	`closed` (una tantum), `open` (persistente)	`terminated`
`instance-terminated-launch-group-constraint`	`closed` (una tantum), `open` (persistente)	`terminated`

¹ Lo stato della richiesta è `closed` se termini l'istanza ma non annulli la richiesta. Lo stato della richiesta è `cancelled` se si termina l'istanza e si annulla la richiesta. Anche se si termina un'istanza spot prima di annullarne la richiesta, potrebbe verificarsi un ritardo prima che Amazon EC2 rilevi che l'istanza spot è stata terminata. In tal caso, lo stato della richiesta può essere `closed` o `cancelled`.

† Quando Amazon EC2 interrompe un'istanza spot se ha bisogno di ripristinare la capacitàe l'istanza è configurata per essere terminata in caso di interruzione, lo stato viene impostato immediatamente su `instance-terminated-no-capacity` (non è impostato su `marked-for-termination`). Tuttavia, l'istanza rimane nella stato `running` per 2 minuti per riflettere il periodo di 2 minuti quando riceve l'avviso di interruzione dell'istanza spot. Dopo 2 minuti, lo stato dell'istanza è impostato su `terminated`.

Esperimenti di interruzione

È possibile utilizzarli AWS Fault Injection Service per avviare un'interruzione dell'istanza Spot in modo da testare la risposta delle applicazioni sulle istanze Spot. Se AWS FIS interrompe un'istanza Spot, la tua richiesta Spot entra nello `marked-for-stop-by-experiment` stato e poi nello stato. `instance-stopped-by-experiment` Se AWS FIS termina un'istanza Spot, la richiesta Spot entra nello `instance-terminated-by-experiment` stato. Per ulteriori informazioni, consulta the section called “Avvia un'interruzione”.

Codice di stato	Stato della richiesta	Stato istanza
`marked-for-stop-by-experiment`	`active`	`running`
`instance-stopped-by-experiment`	`disabled`	`stopped`

Codice di stato	Stato della richiesta	Stato istanza
`instance-terminated-by-experiment`	`closed`	`terminated`

Richieste persistenti

Quando le istanze spot vengono terminate (dall'utente o da Amazon EC2), se la richiesta Spot è di tipo persistente, essa torna allo stato `pending-evaluation` e Amazon EC2 può avviare una nuova istanza spot quando vengono soddisfatti i vincoli.

Ottenere informazioni sullo stato della richiesta

Puoi ottenere informazioni sullo stato della richiesta utilizzando AWS Management Console o uno strumento a riga di comando.

Per ottenere informazioni sullo stato della richiesta utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Spot Requests (Richieste Spot) e selezionare la richiesta Spot.
3. Per verificare lo stato, nella scheda Descrizione selezionare il campo Stato.

Ottenere informazioni sullo stato della richiesta tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- describe-spot-instance-requests (AWS CLI)
- Get-EC2SpotInstanceRequest (AWS Tools for Windows PowerShell)

Codici di stato della richiesta Spot

Le informazioni sullo stato della richiesta Spot sono composte da un codice di stato, dall'ora di aggiornamento e da un messaggio di stato. Nel loro insieme, queste consentono di determinare la disposizione della richiesta Spot.

I codici di stato della richiesta Spot sono i seguenti:

`az-group-constraint`

Amazon EC2 non può avviare tutte le istanze richieste nella stessa zona di disponibilità.

`bad-parameters`

Uno o più parametri della richiesta Spot non sono validi (per esempio, la AMI specificata non esiste). Il messaggio di stato indica quale dei parametri non è valido.

`canceled-before-fulfillment`

L'utente ha annullato la richiesta Spot prima che fosse soddisfatta.

`capacity-not-available`

Non è disponibile una capacità sufficiente per l'istanza richiesta.

`constraint-not-fulfillable`

La richiesta Spot non può essere soddisfatta poiché uno o più vincoli non sono validi (per esempio, la zona di disponibilità non esiste). Il messaggio di stato indica quale dei vincoli non è valido.

`fulfilled`

La richiesta Spot è `active`, e Amazon EC2 sta lanciando le tue Istanze spot.

`instance-stopped-by-price`

La tua istanza è stata arrestata perché il prezzo Spot ha superato il prezzo massimo.

`instance-stopped-by-user`

L'istanza è stata arrestata perché un utente ha arrestato l'istanza o ha eseguito il comando di arresto dall'istanza.

`instance-stopped-no-capacity`

L'istanza è stata arrestata a causa delle esigenze di gestione della capacità EC2.

`instance-terminated-by-price`

La tua istanza è stata interrotta perché il prezzo Spot ha superato il prezzo massimo. Se la richiesta è persistente, il processo viene riavviato, quindi la richiesta è in attesa di valutazione.

`instance-terminated-by-schedule`

La tua istanza spot è stata terminata alla fine della durata programmata.

`instance-terminated-by-service`

L'istanza è stata terminata da uno stato di arresto.

`instance-terminated-by-user` o `spot-instance-terminated-by-user`

È stata terminata un'istanza spot soddisfatta, quindi lo stato della richiesta è `closed` (a meno che non si tratti di una richiesta persistente) e lo stato dell'istanza è `terminated`.

`instance-terminated-launch-group-constraint`

Una o più istanze del gruppo di avvio è stata terminata, quindi il vincolo del gruppo di avvio non viene più soddisfatto.

`instance-terminated-no-capacity`

L'istanza è stata terminata a causa di processi di gestione della capacità standard.

`launch-group-constraint`

Amazon EC2 non può avviare tutte le istanze richieste nello stesso momento. Tutte le istanze in un gruppo di avvio vengono avviate e terminate insieme.

`limit-exceeded`

È stato superato il limite numerico dei volumi EBS o dello archiviazione del volume totale. Per ulteriori informazioni su tali limiti e sulle modalità con cui chiedere un aumento, consulta Limiti Amazon EBS nella Riferimenti generali di Amazon Web Services.

`marked-for-stop`

L'istanza spot è contrassegnata per l'arresto.

`marked-for-termination`

L'istanza spot è contrassegnata per la terminazione.

`not-scheduled-yet`

La richiesta Spot non viene valutata fino alla data programmata.

`pending-evaluation`

Dopo aver effettuato una richiesta di istanza spot, essa passa allo stato `pending-evaluation` mentre il sistema valuta i parametri della richiesta.

`pending-fulfillment`

Amazon EC2 sta tentando di assegnare le Istanze spot.

`placement-group-constraint`

La richiesta Spot non può essere ancora soddisfatta in quanto l'istanza spot non può essere aggiunta al gruppo di posizionamento in questo momento.

`price-too-low`

La richiesta non può essere ancora soddisfatta in quanto il prezzo massimo è inferiore al prezzo Spot. In questo caso, non viene avviata alcuna istanza e la richiesta rimane `open`.

`request-canceled-and-instance-running`

La richiesta Spot è stata annullata mentre le Istanze spot sono ancora in esecuzione. La richiesta è `cancelled`, ma le istanze rimangono `running`.

`schedule-expired`

La richiesta Spot è scaduta poiché non è stata soddisfatta prima della data specificata.

`system-error`

Si è verificato un errore di sistema imprevisto. Se si tratta di un problema ricorrente, contatta AWS Support per ricevere assistenza.

Evento di approvazione della richiesta di istanza spot EC2

Quando una richiesta di istanza Spot viene soddisfatta, Amazon EC2 invia un evento EC2 Spot Instance Request Fulfillment ad Amazon. EventBridge Puoi creare una regola per intraprendere un'azione ogni volta che si verifica questo evento, ad esempio richiamando una funzione Lambda o notificando un argomento Amazon SNS.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "spot-instance-request-id": "sir-1a2b3c4d",
        "instance-id": "i-1234567890abcdef0"
```

```
    }
}
```

Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Raccomandazioni per il ribilanciamento delle istanze EC2

Un suggerimento di ribilanciamento dell'istanza EC2 è un segnale di notifica di un rischio elevato di interruzione per un'istanza spot. Il segnale può arrivare prima dell'avviso di interruzione dell'istanza spot di due minuti, dando la possibilità di gestire in modo proattivo la istanza spot. È possibile decidere di ribilanciare il carico di lavoro su Istanze spot nuove o esistenti che non presentano un rischio elevato di interruzione.

Per Amazon EC2 non è sempre possibile inviare il segnale di raccomandazione per il ribilanciamento prima dell'avviso di interruzione dell'istanza spot di due minuti. Pertanto, il segnale di raccomandazione di ribilanciamento può arrivare insieme all'avviso di interruzione di due minuti.

I consigli di ribilanciamento sono disponibili come EventBridge evento e come elemento nei metadati dell'istanza sull'istanza Spot. Gli eventi vengono emessi secondo il principio del massimo sforzo.

> **Note**
>
> Le raccomandazioni per il ribilanciamento sono supportate solo per le Istanze spot che sono state lanciate dopo il 5 novembre 2020 00:00 UTC.

Argomenti

- Ribilanciare le operazioni intraprese
- Monitorare i segnali di raccomandazione di ribilanciamento
- Servizi che utilizzano il segnale di raccomandazione per il ribilanciamento

Ribilanciare le operazioni intraprese

Queste sono alcune delle possibili operazioni di ribilanciamento che si possono intraprendere:

Arresto di tipo graceful

Quando si riceve il segnale di suggerimento di ribilanciamento per un'istanza spot, è possibile avviare le procedure di arresto dell'istanza, che potrebbero includere il completamento dei

processi prima di arrestarli. Ad esempio, è possibile caricare i registri di sistema o applicativi su Amazon Simple Storage Service (Amazon S3), è possibile chiudere gli operatori di Amazon SQS o completare l'annullamento della registrazione dal Domain Name System (DNS). Inoltre, è possibile salvare il lavoro in una memoria esterna per poi riprenderlo in un secondo momento.

Impedire la pianificazione di nuove operazioni

Quando si riceve il segnale di suggerimento di ribilanciamento per un'istanza spot, è possibile impedire la programmazione di nuove operazioni sull'istanza, continuando a utilizzare l'istanza fino al completamento delle operazioni programmate.

Avvio proattivo di nuove istanze sostitutive

È possibile configurare i gruppi Auto Scaling, il Parco istanze EC2 o il Parco istanze spot per l'avvio automatico di istanze spot sostitutive quando viene emesso un segnale di suggerimento di ribilanciamento. Per maggiori informazioni, consulta Utilizzo del ribilanciamento della capacità per gestire le interruzioni spot di Amazon EC2 nella Guida per l'utente di Dimensionamento automatico Amazon EC2, nonché Ribilanciamento della capacità per il parco istanze EC2 e Ribilanciamento della capacità per la serie di istanze spot in questa guida per l'utente.

Monitorare i segnali di raccomandazione di ribilanciamento

È possibile monitorare il segnale di raccomandazione di ribilanciamento in modo che, quando viene emesso, è possibile eseguire le operazioni specificate nella sezione precedente. Il segnale di raccomandazione di ribilanciamento viene reso disponibile come evento inviato ad Amazon EventBridge (precedentemente noto come Amazon CloudWatch Events) e come metadati dell'istanza sull'istanza Spot.

Monitorare i segnali di raccomandazione di ribilanciamento:

- Usa Amazon EventBridge
- Utilizzare i metadati delle istanze

Usa Amazon EventBridge

Quando viene emesso il segnale di raccomandazione di ribilanciamento per un'istanza Spot, l'evento relativo al segnale viene inviato ad Amazon. EventBridge Se EventBridge rileva uno schema di evento che corrisponde a uno schema definito in una regola, EventBridge richiama uno o più obiettivi specificati nella regola.

Di seguito è riportato un evento di esempio per il segnale di raccomandazione di ribilanciamento.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

I campi seguenti costituiscono il modello di evento definito nella regola:

`"detail-type": "EC2 Instance Rebalance Recommendation"`

Identifica che l'evento è un evento di raccomandazione di ribilanciamento

`"source": "aws.ec2"`

Identifica che l'evento proviene da Amazon EC2

Crea una regola EventBridge

Puoi scrivere una EventBridge regola e automatizzare le azioni da intraprendere quando il modello di evento corrisponde alla regola.

L'esempio seguente crea una EventBridge regola per inviare un'e-mail, un messaggio di testo o una notifica push mobile ogni volta che Amazon EC2 emette un segnale di raccomandazione di ribilanciamento. Il segnale viene emesso come evento di `EC2 Instance Rebalance Recommendation`, che attiva l'azione definita dalla regola.

Prima di creare la EventBridge regola, devi creare l'argomento Amazon SNS per l'e-mail, il messaggio di testo o la notifica push per dispositivi mobili.

Per creare una EventBridge regola per un evento di raccomandazione di ribilanciamento

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.

3. Per Define rule detail (Definisci dettagli della regola), effettua le seguenti operazioni:

   a. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.

      Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso bus di eventi.

   b. Per Event bus (Bus di eventi), scegli default. Quando un servizio AWS nell'account genera un evento, passa sempre al bus di eventi di default dell'account.

   c. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).

   d. Seleziona Successivo.

4. Per Build event pattern (Crea modello di eventi), procedi come segue:

   a. Per Event source, scegli AWS eventi o eventi EventBridge partner.

   b. Per Event pattern (Modello di eventi), ai fini di questo esempio, specifica il seguente modello di eventi in modo che corrisponda all'evento `EC2 Instance Rebalance Recommendation`, quindi scegli Save (Salva).

      ```
      {
       "source": ["aws.ec2"],
       "detail-type": ["EC2 Instance Rebalance Recommendation"]
      }
      ```

      Per aggiungere il modello di eventi, puoi utilizzare un modello scegliendo Event pattern form (Formato del modello di eventi) o specificare il tuo modello scegliendo Custom pattern (JSON editor) (Modello personalizzato (editor JSON)), come segue:

      i. Per utilizzare un modello per creare il modello di eventi, procedi come segue:

         A. Scegli Event pattern form (Formato del modello di eventi).

         B. Per Event source (Origine evento), scegli AWS services (Servizi).

         C. In AWS Service, scegli Serie di istanze spot EC2.

         D. Per Event type (Tipo di evento), scegli EC2 Instance Rebalance Recommendation (Suggerimento per il ribilanciamento dell'istanza EC2).

         E. Per personalizzare il modello, scegli Edit pattern (Modifica modello) e apporta le modifiche in modo che corrisponda al modello di eventi di esempio.

      ii. (Alternativa) Per specificare un modello di eventi personalizzato, procedi come segue:

A. Scegli Custom pattern (JSON editor) (Modello personalizzato (editor JSON)).

B. Nella casella Event pattern (Modello di eventi), aggiungi il modello di eventi per questo esempio.

c. Seleziona Successivo.

5. Per Select target(s) (Seleziona destinazione/i), esegui queste operazioni:

a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).

b. Per Select a target (Seleziona una destinazione, scegli SNS topic (Argomento SNS) per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando si verifica l'evento.

c. Per Argomento, scegliere un argomento esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) nella Amazon Simple Notification Service Developer Guide.

d. (Facoltativo) In Additional settings (Impostazioni aggiuntive), facoltativamente puoi configurare impostazioni aggiuntive. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi (passaggio 16) nella Amazon EventBridge User Guide.

e. Seleziona Successivo.

6. (Opzionale) Per Tags (Tag), se desideri puoi assegnare uno o più tag alla regola, quindi scegli Next (Successivo).

7. Per Review and create (Verifica e crea), procedi come segue:

a. Verifica i dettagli della regola e modificali se necessario.

b. Scegli Crea regola.

Per ulteriori informazioni, consulta EventBridge le regole di Amazon e i modelli di EventBridge eventi di Amazon nella Amazon EventBridge User Guide

Utilizzare i metadati delle istanze

La categoria Metadati istanza `events/recommendations/rebalance` fornisce l'ora approssimativa (fuso UTC) in cui il segnale di raccomandazione di ribilanciamento è stato emesso per un'istanza spot.

Ti consigliamo di controllare la presenza di segnali di raccomandazione di ribilanciamento ogni 5 secondi in modo da non perdere l'opportunità di agire in base alle raccomandazione di ribilanciamento.

Se l'istanza spot riceve un suggerimento di ribilanciamento, l'ora in cui il segnale è stato emesso sarà presente nei metadati dell'istanza. È possibile recuperare l'ora in cui il segnale è stato emesso come segue.

Usa il comando per il tuo sistema operativo.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Di seguito è riportato un esempio di output, che indica l'ora (fuso UTC) in cui il segnale di suggerimento di ribilanciamento è stato emesso per l'istanza spot.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Se il segnale non è stato emesso per l'istanza, `events/recommendations/rebalance` non è presente e viene visualizzato un errore HTTP 404 quando si tenta di recuperarlo.

Servizi che utilizzano il segnale di raccomandazione per il ribilanciamento

Amazon EC2 Auto Scaling, i parchi istanze EC2 e i parchi istanze spot utilizzano il segnale di suggerimento di ribilanciamento per semplificare il mantenimento della disponibilità del carico di lavoro aumentando in modo proattivo il parco istanze con una nuova istanza spot prima che un'istanza in esecuzione riceva l'avviso di interruzione dell'istanza spot dopo due minuti. È possibile fare in modo che questi servizi monitorino e rispondano in modo proattivo alle modifiche che influiscono sulla disponibilità delle proprie Istanze spot. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Utilizzo del ribilanciamento della capacità per gestire le interruzioni spot di Amazon EC2 nella Guida per l'utente di Dimensionamento automatico Amazon EC2
- Ribilanciamento della capacità nell'argomento Parco istanze EC2 di questa guida per l'utente
- Ribilanciamento della capacità nell'argomento della serie di istanze spot di questa guida per l'utente

Interruzioni dell'istanza spot

È possibile lanciare Istanze spot sulla capacità EC2 di riserva per risparmi notevoli, per poi restituirle quando Amazon EC2 ha nuovamente bisogno della capacità. Quando Amazon EC2 recupera un'istanza spot, chiamiamo questo evento un'interruzione dell'istanza spot.

Quando Amazon EC2 interrompe un'istanza spot, termina, interrompe o iberna l'istanza, a seconda di ciò che hai specificato quando hai creato la richiesta Spot.

La richiesta di Istanze spot può variare significativamente da un momento all'altro e anche la disponibilità di Istanze spot può variare significativamente a seconda di quante istanze EC2 inutilizzate sono disponibili. È sempre possibile che l'istanza spot venga interrotta.

Un'istanza on demand specificata in un Parco istanze EC2 o in un Parco istanze spot non può essere interrotta.

Indice

- Terminare le Istanze spot interrotte
- Preparati alle interruzioni delle istanze Spot
- Avvio dell'interruzione di un'istanza spot
- Avvisi di interruzione dell'istanza spot
- Cercare Istanze spot interrotte
- Determinare se Amazon EC2 ha terminato un'istanza spot
- Fatturazione delle Istanze spot interrotte

Motivi dell'interruzione dell'istanza Spot

Di seguito sono elencati i possibili motivi per cui Amazon EC2 potrebbe interrompere le Istanze spot:

Capacity

Amazon EC2 può interrompere l'istanza spot quando ne ha bisogno. EC2 recupera l'istanza principalmente per riutilizzare la capacità, ma il recupero può verificarsi anche per altri motivi, come la manutenzione dell'host o la disattivazione dell'hardware.

Prezzo

Il prezzo spot è inferiore al prezzo massimo.

Nella richiesta spot puoi specificare il prezzo massimo. Se specifichi un prezzo massimo, tuttavia, le tue istanze verranno interrotte con maggiore frequenza rispetto a quando non lo specifichi.

Vincoli

Se la richiesta include un vincolo, come un gruppo di avvio o un gruppo della zona di disponibilità, queste istanze spot vengono terminate come gruppo quando il vincolo non può più essere soddisfatto.

Puoi visualizzare le percentuali di interruzione cronologiche per il tipo di istanza in Spot Instance Advisor (Consulente istanze spot).

Comportamento delle interruzioni delle istanze Spot

È possibile specificare che Amazon EC2 esegua una delle seguenti operazioni quando interrompe un'istanza spot:

- Arrestare delle Istanze spot interrotte
- Ibernare le Istanze spot interrotte
- Terminare le Istanze spot interrotte (questo è il comportamento predefinito).

Specificare il comportamento di interruzione

È possibile specificare il comportamento di interruzione quando si crea una richiesta Spot. Se non si specifica un comportamento di interruzione, il valore predefinito per Amazon EC2 è terminare Istanze spot quando vengono interrotti.

Il modo in cui si specifica il comportamento di interruzione è diverso a seconda di come si richiede Istanze spot.

- Se si configurano le istanze spot tramite la procedura guidata di avvio dell'istanza, è possibile specificare il comportamento di interruzione nel modo seguente: nella procedura guidata di avvio dell'istanza, espandi Dettagli avanzati e seleziona la casella di controllo Richiedi istanze spot. Scegliere Customize (Personalizza). Da Comportamento di interruzione, scegli un comportamento di interruzione. Se il comportamento di interruzione è l'ibernazione, in alternativa puoi scegliere Abilita per Comportamento di interruzione/ibernazione.
- Se richiedi le istanze spot utilizzando il comando della CLI run-instances, puoi specificare il comportamento di interruzione nel modo seguente: nella configurazione della richiesta, (`--instance-market-options`), per `InstanceInterruptionBehavior`, specifica un comportamento di interruzione. Se il comportamento di interruzione è `hibernate`, in alternativa puoi abilitare l'ibernazione utilizzando il parametro `--hibernation-options Configured=true`.
- Se si configurano le Istanze spot in un modello di avvio, è possibile specificare il comportamento di interruzione nel modo seguente: nel modello di avvio espandere Dettagli avanzati e selezionare la casella di controllo Richiedi Istanze spot. Scegliere Personalizza e quindi, da Comportamento interruzione, scegliere un comportamento di interruzione.
- Se si richiede di Istanze spot utilizzare la console Spot, è possibile specificare il comportamento di interruzione nel modo seguente: selezionare la casella di controllo Mantieni capacità di destinazione quindi scegliere un comportamento di interruzione, da Comportamento interruzione.
- Se si configura Istanze spot in una configurazione di avvio quando si utilizza l'interfaccia CLI del parco istanze create-fleet è possibile specificare il comportamento di interruzione nel modo seguente: Per `InstanceInterruptionBehavior`, specificare un comportamento di interruzione.

- Se si configurano le istanze Spot nella configurazione della richiesta quando si utilizza la request-spot-fleetCLI, è possibile specificare il comportamento di interruzione come segue: `InstanceInterruptionBehavior` Per, specificare un comportamento di interruzione.
- Se configuri le istanze Spot utilizzando la request-spot-instancesCLI, puoi specificare il comportamento di interruzione come segue: `--instance-interruption-behavior` Per, specifica un comportamento di interruzione.

> **Note**
>
> Sconsigliamo vivamente di utilizzare request-spot-instancesi comandi request-spot-fleetand per richiedere le istanze Spot perché si tratta di API legacy senza investimenti pianificati. Per ulteriori informazioni, consulta Qual è il metodo di richiesta Spot migliore da utilizzare?

Arrestare delle Istanze spot interrotte

È possibile specificare che Amazon EC2 arresti le istanze spot quando vengono interrotte. Per ulteriori informazioni, consulta Specificare il comportamento di interruzione.

Considerazioni

- Solo Amazon EC2 può riavviare un'istanza spot interrotta.
- Per un'istanza spot avviata da una richiesta di istanza spot `persistent` , Amazon EC2 riavvia l'istanza arrestata quando la capacità è disponibile nella stessa zona di disponibilità e per lo stesso tipo di istanza dell'istanza arrestata (è necessario utilizzare la stessa specifica).
- Per istanze spot lanciate da un Parco istanze EC2 o un Parco istanze spot di tipo `maintain`: Dopo l'interruzione di un'istanza spot, Amazon EC2 avvia un'istanza sostitutiva per mantenere la capacità di destinazione. Amazon EC2 individua i migliori pool di capacità spot in base alla strategia di allocazione specificata (`lowestPrice`, `diversified` o `InstancePoolsToUseCount`); non attribuisce priorità al pool con le istanze interrotte in precedenza. In seguito, se la strategia di allocazione porta a un pool contenente le istanze interrotte in precedenza, Amazon EC2 riavvia le istanze interrotte per soddisfare la capacità target.

  Ad esempio, considera una Serie di istanze spot con la strategia di allocazione `lowestPrice`. All'avvio iniziale, un pool `c3.large` soddisfa i criteri `lowestPrice` per la specifica di avvio. In seguito, quando le istanze `c3.large` vengono interrotte, Amazon EC2 interrompe le istanze e rifornisce la capacità da un altro pool che risponde alla strategia `lowestPrice`. Questa volta,

il pool è `c4.large` e Amazon EC2 avvia istanze `c4.large` per soddisfare la capacità target. Analogamente, la Serie di istanze spot può spostarsi in un pool `c5.large` la volta successiva. In ciascuna di queste transizioni, Amazon EC2 non definisce le priorità dei pool con istanze interrotte in precedenza, ma definisce priorità puramente sulla strategia di allocazione specificata. La strategia `lowestPrice` può riportare a pool con istanze interrotte in precedenza. Ad esempio, se le istanze vengono interrotte nel pool `c5.large` e la strategia `lowestPrice` riporta ai pool `c3.large` o `c4.large`, le istanze interrotte in precedenza vengono riavviate per soddisfare la capacità target.

- Durante l'arresto di un'istanza spot, è possibile modificare alcuni attributi dell'istanza, ma non il tipo di istanza. Se si distacca o si elimina un volume EBS, questo non è collegato all'avvio dell'istanza spot. Se si distacca il volume root e Amazon EC2 tenta di avviare l'istanza spot, l'istanza non verrà avviata e Amazon EC2 terminerà l'istanza arrestata.
- È possibile terminare un'istanza spot durante il suo arresto.
- Se si annulla una richiesta dell'istanza spot, un parco istanze EC2 o un parco istanze spot, Amazon EC2 termina tutte le istanze spot associate arrestate.
- Mentre un'istanza spot viene arrestata, il costo viene addebitato solo per i volumi EBS, che vengono conservati. Con il Parco istanze EC2 e il Parco istanze spot, se sono presenti molte istanze arrestate, è possibile superare il limite numerico di volumi EBS per il proprio account. Per ulteriori informazioni su come viene addebitato l'addebito quando un'istanza spot viene interrotta, consultare Fatturazione delle Istanze spot interrotte.
- Assicurarsi di avere familiarità con le implicazioni dell'arresto di un'istanza. Per ulteriori informazioni su cosa accade quando un'istanza viene arrestata, consultare Differenze tra riavvio, arresto, ibernazione e interruzione.

Prerequisiti

Per arrestare un'Istanza spot è necessario che siano soddisfatti i prerequisiti seguenti:

Tipo di richiesta Spot

Tipo di richiesta di istanza spot - Deve essere `persistent`. Non è possibile specificare un gruppo di avvio nella richiesta di istanza spot.

Tipo di richiesta Parco istanze EC2 o Parco istanze spot - Deve essere `maintain`.

Tipo di volume root

Il volume root deve essere un volume EBS e non un volume di archivio istanza.

Ibernare le Istanze spot interrotte

È possibile specificare che Amazon EC2 iberni le istanze spot quando vengono interrotte. Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.

Ora Amazon EC2 offre per le istanze spot la stessa esperienza di ibernazione attualmente disponibile per le istanze on demand. Offre un supporto più ampio, dove per l'ibernazione delle istanze spot ora sono offerte le seguenti caratteristiche:

- Più AMI supportate
- Più famiglie di istanze supportate
- Ibernazione avviata dall'utente

Terminare le Istanze spot interrotte

Quando Amazon EC2 interrompe un'istanza spot, termina l'istanza per impostazione predefinita, a meno che non specifichi un comportamento di interruzione diverso, ad esempio l'arresto o l'ibernazione. Per ulteriori informazioni, consulta Specificare il comportamento di interruzione.

Preparati alle interruzioni delle istanze Spot

La richiesta di Istanze spot può variare significativamente da un momento all'altro e anche la disponibilità di Istanze spot può variare significativamente a seconda di quante istanze EC2 inutilizzate sono disponibili. È sempre possibile che l'istanza spot venga interrotta. Pertanto, è necessario assicurarsi che l'applicazione sia preparata per un'interruzione dell'istanza spot.

Consigliamo di seguire queste best practice in modo da essere pronti all'interruzione dell'istanza spot.

- Creare la propria richiesta Spot utilizzando un gruppo Auto Scaling. Se le istanze spot vengono interrotte, il gruppo Auto Scaling lancerà automaticamente le istanze sostitutive. Per ulteriori informazioni, consultare la sezione relativa ai Gruppi con dimensionamento automatico con più tipi di istanze e opzioni di acquisto nella Guida per l'utente di Dimensionamento automatico Amazon EC2.
- Accertarsi che l'istanza sia pronta non appena la richiesta viene soddisfatta utilizzando un'Amazon Machine Image (AMI) che contiene la configurazione software richiesta. È possibile anche utilizzare i dati dell'utente per eseguire i comandi al startup.
- Quando l'istanza viene arrestata o terminata, i dati nei volumi dell'archivio dell'istanza vengono persi. Esegui il backup di tutti i dati importanti contenuti nei volumi dell'archivio dell'istanza in un archivio più persistente, ad esempio Amazon S3, Amazon EBS o Amazon DynamoDB.

- È opportuno archiviare regolarmente i dati importanti in un luogo che non sia interessato dalla terminazione dell'istanza spot. Per esempio, è possibile utilizzare Amazon S3, Amazon EBS o DynamoDB.
- Dividere il lavoro in piccole attività (utilizzando un'architettura basata su griglia, Hadoop o coda) o utilizzare i checkpoint in modo da poter salvare il lavoro con frequenza.
- Amazon EC2 emette un segnale di suggerimento di ribilanciamento dell'istanza spot quando l'istanza presenta un rischio elevato di interruzione. È possibile fare affidamento sul suggerimento di ribilanciamento per gestire in modo proattivo le interruzioni dell'istanza spot senza dover attendere l'avviso di interruzione dell'istanza spot dopo due minuti. Per ulteriori informazioni, consulta Raccomandazioni per il ribilanciamento delle istanze EC2.
- Utilizzare gli avvisi di interruzione dell'istanza spot dopo due minuti per monitorare lo stato delle proprie istanze spot. Per ulteriori informazioni, consulta Avvisi di interruzione dell'istanza spot.
- Anche se compiamo ogni sforzo per fornire questi avvisi con il massimo anticipo possibile, può accadere che l'istanza spot venga terminata prima che gli avvisi siano inviati. Verificare l'applicazione per assicurarsi che gestisca correttamente un'interruzione improvvisa dell'istanza, anche se si stanno monitorando i segnali di raccomandazione di ribilanciamento e gli avvisi di interruzione. È possibile farlo eseguendo l'applicazione utilizzando una Istanza on demand e terminando la Istanza on demand per conto proprio.
- Esegui un esperimento di iniezione controllata dei guasti AWS Fault Injection Service per verificare la risposta dell'applicazione quando l'istanza Spot viene interrotta. Per ulteriori informazioni, consultare Tutorial: test delle interruzioni dell'istanza Spot tramite AWS FIS nella Guida per l'utente di AWS Fault Injection Service .

Avvio dell'interruzione di un'istanza spot

Puoi selezionare una richiesta di istanza spot o una richiesta di serie di istanze spot nella console di Amazon EC2 e avviare un'interruzione dell'istanza spot in modo da poter provare in che modo le applicazioni sulle tue istanze spot gestiscono le interruzioni. Quando avvii l'interruzione di un'istanza spot, Amazon EC2 segnala che l'istanza spot verrà interrotta entro due minuti e quindi, dopo due minuti, l'istanza spot viene interrotta.

Il servizio sottostante che esegue l'interruzione dell'istanza Spot è AWS Fault Injection Service ().AWS FIS Per informazioni su AWS FIS, consulta AWS Fault Injection Service.

> **Note**
>
> I comportamenti di interruzione sono `terminate`, `stop` e `hibernate`. Se imposti il comportamento di interruzione su `hibernate`, quando avvii l'interruzione di un'istanza spot il processo di ibernazione inizia immediatamente.

L'avvio di un'interruzione di un'istanza Spot è supportato in tutti i paesi Regioni AWS tranne Asia Pacifico (Giacarta), Asia Pacifico (Osaka), Cina (Pechino), Cina (Ningxia) e Medio Oriente (Emirati Arabi Uniti).

Argomenti

Avvio dell'interruzione di un'istanza spot

Puoi usare la console EC2 per avviare rapidamente l'interruzione di un'istanza spot. Quando si seleziona una richiesta di istanza spot, è possibile avviare l'interruzione di un'istanza spot. Quando si seleziona una richiesta di una serie di istanze spot, è possibile avviare l'interruzione di più istanze spot in una sola volta.

Per esperimenti più avanzati per testare le interruzioni delle istanze Spot, puoi creare esperimenti personalizzati utilizzando la console. AWS FIS

Avvio dell'interruzione di una istanza spot in una richiesta di istanza spot tramite la console EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Richieste spot.
3. Seleziona la richiesta di un'istanza spot e scegli Actions (Operazioni), Initiate interruption (Avvia interruzione). Per avviare un'interruzione non è possibile selezionare più richieste di istanza spot.
4. Nella finestra di dialogo Initiate Spot Instance interruption (Avvia interruzione istanza spot), in Service access (Accesso al servizio), usa il ruolo predefinito o scegli un ruolo esistente. Per scegliere un ruolo esistente, seleziona Usa un ruolo di servizio esistente quindi per Ruolo IAM seleziona il ruolo da utilizzare.

5. Quando sei pronto all'avvio dell'interruzione di un'istanza spot, scegli Initiate interruption (Avvia interruzione).

Avvio dell'interruzione di una o più istanze spot in una richiesta di istanze spot tramite la console EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Richieste spot.
3. Seleziona la richiesta di una serie di istanze spot e scegli Operazioni, Avvia interruzione. Per avviare un'interruzione non è possibile selezionare più richieste di serie di istanze spot.
4. Nella finestra di dialogo Specifica il numero di istanze spot, in Numero di istanze da interrompere, inserisci il numero di istanze spot da interrompere, quindi scegli Conferma.

> **Note**
>
> Il numero non può superare il numero di istanze Spot presenti nel parco istanze o la quota prevista per il numero di istanze Spot che AWS FIS possono essere interrotte per esperimento.

5. Nella finestra di dialogo Initiate Spot Instance interruption (Avvia interruzione istanza spot), in Service access (Accesso al servizio), usa il ruolo predefinito o scegli un ruolo esistente. Per scegliere un ruolo esistente, seleziona Usa un ruolo di servizio esistente quindi per Ruolo IAM seleziona il ruolo da utilizzare.
6. Quando sei pronto all'avvio dell'interruzione di un'istanza spot, scegli Initiate interruption (Avvia interruzione).

Creazione di esperimenti più avanzati per testare le interruzioni delle istanze spot tramite la console AWS FIS

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Richieste spot.
3. Scegli Actions (Operazioni), Create advanced experiments (Crea esperimenti avanzati).

   La AWS FIS console si apre. Per ulteriori informazioni, consulta Tutorial: Test delle interruzioni di istanze spot tramite AWS FIS nella Guida per l'utente di AWS Fault Injection Service .

Verifica dell'interruzione dell'istanza spot

Dopo l'avvio dell'interruzione, si verifica quanto segue:

- L'istanza spot riceve una raccomandazione di ribilanciamento dell'istanza.
- Un avviso di interruzione dell'istanza Spot viene emesso due minuti prima dell' AWS FIS interruzione dell'istanza.
- Dopo due minuti, l'istanza spot viene interrotta.
- Un'istanza Spot che è stata interrotta AWS FIS rimane interrotta fino al riavvio.

Verificare che l'istanza sia stata interrotta dopo l'avvio dell'interruzione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, apri Spot Requests (Richieste spot) e Instances (Istanze) in schede o finestre separate del browser.
3. Per le richieste Spot, seleziona la richiesta di istanza spot o la richiesta della serie di istanze spot. Lo stato iniziale è `fulfilled`. Dopo l'interruzione dell'istanza, lo stato cambia come segue, a seconda del comportamento dell'interruzione:
   - `terminate`: lo stato diventa `instance-terminated-by-experiment`.
   - `stop`: lo stato diventa `marked-for-stop-by-experiment` e poi `instance-stopped-by-experiment`.
4. Per Istanze, seleziona l'istanza spot. Lo stato iniziale è `Running`. Due minuti dopo la ricezione dell'avviso di interruzione dell'istanza spot, lo stato cambia come segue, a seconda del comportamento dell'interruzione:
   - `stop`: lo stato diventa `Stopping` e poi `Stopped`.
   - `terminate`: lo stato diventa `Shutting-down` e poi `Terminated`.

Quote

Hai Account AWS la seguente quota predefinita per il numero di istanze Spot che AWS FIS possono essere interrotte per esperimento.

Nome	Predefinita	Adattabile	Descrizione
		Sì	

Nome	Predefinita	Adattabile	Descrizione
Obiettivo SpotInstances per aws:ec2:send-spot-instance-interruptions	Ogni regione supportata: 5		Il numero massimo di istanze Spot a cui aws:ec2: send-spot-instance-interruptions può indirizzare quando identifichi gli obiettivi utilizzando i tag, per esperimento.

È possibile richiedere un aumento della quota. Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente per Service Quotas.

Per visualizzare tutte le quote di AWS FIS, apri la console Service Quotas. Nel riquadro di navigazione, scegliere Servizi AWS , quindi selezionare AWS Fault Injection Service. Puoi visualizzare tutte le quote di AWS Fault Injection Service anche nella Guida per l'utente di AWS Fault Injection Service .

Avvisi di interruzione dell'istanza spot

Una notifica di interruzione di istanza spot è un avviso che viene emesso due minuti prima che Amazon EC2 arresti o termini l'istanza spot. Se si specifica l'ibernazione come comportamento di interruzione, si riceve un avviso di interruzione ma senza i due minuti di preavviso perché il processo di ibernazione comincia immediatamente.

Il modo migliore per gestire nel modo appropriato le interruzioni delle istanze spot è progettare l'applicazione affinché sia tollerante ai guasti. A tale scopo, puoi sfruttare gli avvisi di interruzione dell'istanza spot. Si consiglia di controllare queste notifiche di interruzione ogni 5 secondi.

Gli avvisi di interruzione sono resi disponibili come EventBridge evento e come elementi nei metadati dell'istanza sull'istanza Spot. Gli avvisi di interruzione vengono emessi in base al miglior sforzo possibile.

EC2 Spot Instance interruption notice

Quando Amazon EC2 sta per interrompere l'istanza spot, emette un evento due minuti prima dell'interruzione effettiva (tranne che per l'ibernazione, che riceve l'avviso di interruzione ma non

con due minuti di anticipo, perché l'ibernazione inizia immediatamente). Questo evento può essere rilevato da Amazon EventBridge. Per ulteriori informazioni sugli EventBridge eventi, consulta la Amazon EventBridge User Guide. Per un esempio dettagliato che illustra come creare e utilizzare le regole degli eventi, consulta Taking Advantage of Amazon EC2 Spot Instance Interruption Notices.

Di seguito è illustrato un esempio dell'evento di interruzione dell'istanza spot. I valori possibili per `instance-action` sono `hibernate`, `stop` e `terminate`.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2a:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

> **Note**
>
> Il formato ARN dell'evento di interruzione dell'istanza Spot è. `arn:aws:ec2:availability-zone:instance/instance-id` Questo formato è diverso dal formato ARN delle risorse EC2.

instance-action

Se l'istanza spot è contrassegnata per essere arrestata o terminata dal Amazon EC2, nei metadati dell'istanza è presente la voce `instance-action`. In caso contrario, non è presente. È possibile recuperarlo `instance-action` utilizzando Instance Metadata Service Version 2 (IMDSv2) come segue.

Usa il comando per il tuo sistema operativo.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

La voce `instance-action` specifica l'azione e l'orario indicativo, in UTC, in cui si verificherà l'azione.

L'esempio seguente indica l'orario in cui questa istanza verrà arrestata.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

L'esempio seguente indica l'orario in cui questa istanza verrà terminata.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Se Amazon EC2 non si sta preparando ad arrestare o terminare l'istanza o se l'istanza è stata terminata dall'utente stesso, `instance-action` non è presente nei metadati dell'istanza e viene restituito un errore HTTP 404 quando si cerca di recuperarla.

termination-time

Questa voce viene mantenuta per la compatibilità con le versioni precedenti; è necessario utilizzare `instance-action`.

Se la tua istanza Spot è contrassegnata per la chiusura da Amazon EC2 (a causa di un'interruzione dell'istanza Spot su cui è impostato il comportamento di interruzione o `terminate` a causa dell'annullamento di una richiesta persistente di istanza Spot), `termination-time` l'elemento è presente nei metadati dell'istanza. In caso contrario, non è presente. Puoi recuperarlo utilizzando iMDSv2 come segue. `termination-time`

Usa il comando per il tuo sistema operativo.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
[ec2-user ~]$ if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo
 termination_scheduled; fi
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

L'`termination-time`elemento specifica l'ora approssimativa in UTC in cui l'istanza riceverà il segnale di spegnimento. Di seguito è riportato un output di esempio.

```
2015-01-05T18:02:00Z
```

Se Amazon EC2 non si prepara a terminare l'istanza (perché non c'è alcuna interruzione dell'istanza Spot o perché il comportamento di interruzione è impostato su `stop` o`hibernate`), o se hai terminato l'istanza Spot tu stesso, l'`termination-time`elemento non è presente nei metadati dell'istanza (quindi ricevi un errore HTTP 404) o contiene un valore che non è un valore temporale.

Se Amazon EC2 non riesce a terminare l'istanza, lo stato della richiesta viene impostato su `fulfilled`. I valore `termination-time` rimane nei metadati di istanza con l'orario indicativo originario, che ora è in passato.

Cercare Istanze spot interrotte

Nella console, il riquadro Istanze visualizza tutte le istanze, incluso Istanze spot. Il ciclo di vita dell'istanza di un'istanza spot è `spot`. Lo stato dell'istanza di un'istanza spot è `stopped` o `terminated`, a seconda del comportamento di interruzione configurato. Per un'istanza spot ibernata, lo stato dell'istanza è `stopped`.

Per trovare un'istanza spot interrotta utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.

3. Applica il seguente filtro: Ciclo di vita dell'istanza=spot.
4. Applica il filtro Stato istanza=arrestata o IStato istanza=terminata a seconda del comportamento di interruzione che hai configurato.
5. Per ogni istanza spot, nella scheda Dettagli, in Dettagli istanza, trova Messaggio transizione stato. I codici seguenti indicano che l'istanza spot è stata interrotta.
   - `Server.SpotInstanceShutdown`
   - `Server.SpotInstanceTermination`
6. Per ulteriori dettagli sul motivo dell'interruzione, controlla il codice di stato della richiesta spot. Per ulteriori informazioni, consulta the section called “Stato della richiesta Spot”.

Per trovare le istanze Spot interrotte, utilizza AWS CLI

È possibile elencare i Istanze spot interrotti utilizzando il comando describe-instances con il parametro `--filters`. Per elencare solo gli ID di istanza nell'output, aggiungere il parametro `--query`.

Se il comportamento di interruzione dell'istanza consiste nel terminare le istanze spot, utilizza il seguente comando:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=terminated Name=state-reason-code,Values=Server.SpotInstanceTermination \
    --query "Reservations[*].Instances[*].InstanceId"
```

Se il comportamento di interruzione dell'istanza consiste nell'arrestare le istanze spot, utilizza il seguente comando:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=stopped Name=state-reason-code,Values=Server.SpotInstanceShutdown \
    --query "Reservations[*].Instances[*].InstanceId"
```

Determinare se Amazon EC2 ha terminato un'istanza spot

Se un'istanza Spot viene terminata, puoi CloudTrail verificare se Amazon EC2 ha terminato l'istanza Spot. In AWS CloudTrail, il nome dell'evento `BidEvictedEvent` indica che Amazon EC2 ha terminato l'istanza spot.

Per visualizzare gli eventi in BidEvictedEvent CloudTrail

1. Apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione scegliere Event history (Cronologia eventi).
3. Nel menu a discesa del filtro, scegli Nome evento, quindi nel campo del filtro a destra, inserisci. BidEvictedEvent
4. Scegli BidEvictedEventnell'elenco risultante per visualizzarne i dettagli. In Event record (Record evento), è possibile trovare l'ID istanza.

Per ulteriori informazioni sull'utilizzo CloudTrail, consultaRegistra le chiamate API di Amazon EC2 utilizzando AWS CloudTrail.

Fatturazione delle Istanze spot interrotte

Quando un'istanza spot viene interrotta, l'addebito per l'utilizzo dell'istanza e dei volumi EBS, e di eventuali costi aggiuntivi, avviene come segue.

Utilizzo di istanze

Chi interrompe l'istanza spot	Sistema operativo	Interrotta nella prima ora	Interrotta in qualsiasi momento dopo la prima ora
Se l'istanza spot viene arrestata o terminata dall'utente	Windows e Linux (escluso SUSE)	Addebito dei secondi utilizzati	Addebito dei secondi utilizzati
	SUSE	Addebito dell'ora intera anche se utilizzata parzialme nte.	Addebito delle ore intere utilizzate e addebito di un'ora intera per l'ora parziale interrotta.
Se l'istanza spot viene interrotta da Amazon EC2	Windows e Linux (escluso SUSE)	Nessun addebito	Addebito dei secondi utilizzati
	SUSE	Nessun addebito	Addebito delle ore intere utilizzate e

Chi interrompe l'istanza spot	Sistema operativo	Interrotta nella prima ora	Interrotta in qualsiasi momento dopo la prima ora
			nessun addebito per l'ora parziale interrotta.

Utilizzo del volume EBS

Mentre un'istanza spot viene arrestata, il costo viene addebitato solo per i volumi EBS, che vengono conservati.

Con il Parco istanze EC2 e il Parco istanze spot, se sono presenti molte istanze arrestate, è possibile superare il limite numerico di volumi EBS per il proprio account.

Costi aggiuntivi

Se l'istanza Spot in esecuzione prevede costi per altri servizi, ad esempio per il trasferimento dei dati, gli indirizzi IP elastici o l'utilizzo di altri servizi AWS gestiti, ti verrà addebitato il relativo utilizzo. I costi vengono addebitati a prescindere da chi interrompe l'istanza spot o da quando è stata interrotta. Anche se l'utilizzo dell'istanza spot non viene addebitato quando Amazon EC2 la interrompe nella prima ora, possono essere addebitati costi aggiuntivi.

Per informazioni in merito ai costi aggiuntivi, consulta Prezzi di Amazon EC2 on demand.

Punteggio di posizionamento spot

La funzione Spot Placement Score può consigliare una AWS regione o una zona di disponibilità in base ai requisiti di capacità Spot. La capacità spot fluttua e non si può essere sicuri che otterrai sempre la capacità di cui hai bisogno. Un punteggio di posizionamento spot indica quanto è probabile che una richiesta Spot abbia esito positivo in una regione o in una zona di disponibilità.

> **Note**
>
> Un punteggio di posizionamento spot non fornisce alcuna garanzia in termini di capacità disponibile o rischio di interruzione. Un punteggio di posizionamento spot serve solo come suggerimento.

Vantaggi

È possibile utilizzare la funzione del punteggio di posizionamento spot per quanto segue:

- Per trasferire e scalare la capacità di calcolo Spot in una regione diversa, in base alle necessità, in risposta all'aumento del fabbisogno di capacità o alla diminuzione della capacità disponibile nella regione corrente.
- Per identificare la zona di disponibilità ottimale in cui eseguire carichi di lavoro a singola zona di disponibilità.
- Per simulare le future esigenze di capacità spot in modo da poter scegliere una regione ottimale per l'espansione dei carichi di lavoro basati su Spot.
- Per trovare una combinazione ottimale di tipi di istanza per soddisfare le esigenze di capacità spot.

Argomenti

Costi

L'utilizzo della funzione del punteggio di posizionamento spot non comporta costi supplementari.

Come funziona il punteggio di posizionamento spot

Quando si utilizza la funzione del punteggio di posizionamento spot, si specifica innanzitutto i requisiti di calcolo per le istanze spot, quindi Amazon EC2 restituisce le 10 principali regioni o zone di disponibilità in cui è probabile che la propria richiesta Spot abbia esito positivo. Ogni regione o zona di disponibilità viene valutata su una scala da 1 a 10, con 10 che indica che è molto probabile che la tua richiesta Spot abbia esito positivo e 1 che indica invece che è improbabile che la tua richiesta Spot abbia esito positivo.

Per utilizzare la funzione del punteggio di posizionamento spot, completare la seguente procedura:

- Fase 1: specifica dei requisiti Spot
- Fase 2: filtro della risposta del punteggio di posizionamento spot
- Fase 3: esame dei suggerimenti
- Fase 4: utilizzo dei suggerimenti

Fase 1: specifica dei requisiti Spot

Innanzitutto, è necessario specificare la capacità spot di destinazione desiderata e i requisiti di calcolo, come segue:

1. Specificare la capacità spot di destinazione e, facoltativamente, l'unità di capacità di destinazione.

   È possibile specificare la capacità spot di destinazione desiderata in termini di numero di istanze o vCPU o in termini di quantità di memoria in MiB. Per specificare la capacità di destinazione in numero di vCPU o in quantità di memoria, è necessario specificare l'unità di capacità di destinazione come `vcpu` o `memory-mib`. In caso contrario, per impostazione predefinita sarà impostato sul numero di istanze.

   Specificando la capacità di destinazione in termini di numero di vCPU o in quantità di memoria, potrai utilizzare queste unità per il conteggio della capacità totale. Ad esempio, se si desidera utilizzare un mix di istanze di dimensioni diverse, è possibile specificare la capacità di destinazione come numero totale di vCPU. La funzione del punteggio di posizionamento spot considera quindi ogni tipo di istanza nella richiesta in base al numero di vCPU e conta il numero totale di vCPU anziché il numero totale di istanze nel totale della capacità di destinazione.

Ad esempio, si supponga di specificare una capacità di destinazione totale di 30 vCPU e che l'elenco dei tipi di istanza sia costituito da c5.xlarge (4 vCPU), m5.2xlarge (8 vCPU) e r5.large (2 vCPU). Per ottenere un totale di 30 vCPU, è possibile avere un mix di 2 vCPU c5.xlarge (2*4 vCPU), 2 m5.2xlarge (2*8 vCPU) e 3 vCPU r5.large (3*2 vCPU).

2. Specificare i tipi di istanza o gli attributi di istanza.

   È possibile specificare i tipi di istanza da utilizzare oppure specificare gli attributi di istanza necessari per i requisiti di calcolo e quindi consentire ad Amazon EC2 di identificare i tipi di istanza con tali attributi. Questo è noto come selezione del tipo di istanza basata su attributi.

   Non è possibile specificare sia i tipi di istanza che gli attributi di istanza nella stessa richiesta di punteggio di posizionamento spot.

   Se si specificano i tipi di istanza, è necessario specificare almeno tre tipi di istanza diversi, altrimenti Amazon EC2 restituirà un punteggio di posizionamento spot basso. Analogamente, se si specificano attributi di istanza, devono essere risolti con almeno tre tipi di istanza diversi.

Per esempi dei diversi modi per specificare i requisiti Spot, consultare Configurazioni di esempio.

Fase 2: filtro della risposta del punteggio di posizionamento spot

Amazon EC2 calcola il punteggio di posizionamento spot per ogni regione o zona di disponibilità e restituisce le 10 regioni o le 10 zone di disponibilità principali in cui è probabile che la tua richiesta Spot abbia esito positivo. Il valore di default restituisce un elenco di regioni con un punteggio. Se si prevede di avviare tutta la tua capacità spot in una singola zona di disponibilità, è utile richiedere un elenco di zone di disponibilità con punteggio.

È possibile specificare un filtro regione per limitare le regioni che verranno restituite nella risposta.

È possibile combinare il filtro regione e una richiesta di zone di disponibilità con punteggio. In questo modo, le zone di disponibilità con punteggio saranno limitate alle regioni per le quali si è applicato il filtro. Per trovare la zona di disponibilità con punteggio più alto in una regione, specificare solo quella regione e la risposta restituirà un elenco di tutte le zone di disponibilità in tale regione.

Fase 3: esame dei suggerimenti

Il punteggio di posizionamento spot per ogni regione o zona di disponibilità viene calcolato in base alla capacità di destinazione, alla composizione dei tipi di istanza, alle tendenze di utilizzo Spot cronologiche e correnti e all'ora della richiesta. Poiché la capacità spot è costantemente fluttuante,

la stessa richiesta di punteggio di posizionamento spot può produrre punteggi diversi se il punteggio viene calcolato in momenti diversi.

Le regioni e le zone di disponibilità vengono valutate su una scala da 1 a 10. Un punteggio di 10 indica che è molto probabile, ma non garantito, che la propria richiesta Spot abbia esito positivo. Un punteggio di 1 indica che la tua richiesta Spot ha bassissime probabilità di successo. Lo stesso punteggio potrebbe essere restituito per diverse regioni o zone di disponibilità.

Se vengono restituiti punteggi bassi, è possibile modificare i requisiti di calcolo e ricalcolare il punteggio. È possibile anche richiedere suggerimenti sul punteggio di posizionamento spot per gli stessi requisiti di calcolo in diversi momenti della giornata.

Fase 4: utilizzo dei suggerimenti

Un punteggio di posizionamento spot è rilevante solo se la tua richiesta Spot ha esattamente la stessa configurazione della configurazione del punteggio di posizionamento spot (capacità di destinazione, unità di capacità di destinazione e tipi di istanza o attributi di istanza) ed è configurato per utilizzare la strategia di allocazione `capacity-optimized`. In caso contrario, la probabilità di ottenere la capacità spot disponibile non sarà in linea con il punteggio.

Mentre un punteggio di posizionamento spot funge da linea guida e nessun punteggio garantisce che la propria richiesta Spot sia pienamente o parzialmente soddisfatta, è possibile utilizzare le seguenti informazioni per ottenere i migliori risultati:

- Utilizzo della stessa configurazione: il punteggio di posizionamento spot è rilevante solo se la configurazione della richiesta Spot (capacità di destinazione, unità di capacità di destinazione e tipi di istanza o attributi di istanza) nel gruppo Auto Scaling, nel parco istanze EC2 o nella serie di istanze spot è uguale a quella immessa per ottenere il punteggio di posizionamento spot.

  Se nella richiesta di punteggio di posizionamento spot è stata utilizzata la selezione del tipo di istanza basata su attributi, è possibile utilizzare la selezione del tipo di istanza basata su attributi per configurare il gruppo Auto Scaling, il parco istanze EC2 o la serie di istanze spot. Per ulteriori informazioni, consultare Creazione di un gruppo Auto Scaling con una serie di requisiti per i tipi di istanza utilizzati, Selezione del tipo di istanza basata su attributi per il parco istanze EC2 e Selezione del tipo di istanza basata su attributi per serie di istanze spot.

  > **Note**
  >
  > Se si è specificata la capacità di destinazione in termini di numero di vCPU o di quantità di memoria e hai specificato i tipi di istanza nella configurazione del punteggio di

posizionamento spot, tenere presente che al momento non è possibile creare questa configurazione nel gruppo Auto Scaling, nel parco istanze EC2 o nella serie di istanze spot. Invece, si dovrà impostare manualmente il peso dell'istanza utilizzando il parametro `WeightedCapacity`.

- Utilizzo della strategia di allocazione **`capacity-optimized`**: qualsiasi punteggio presuppone che la richiesta del parco istanze sia configurata per utilizzare tutte le zone di disponibilità (per richiedere la capacità tra le regioni) o una singola zona di disponibilità (se si richiede la capacità in una zona di disponibilità) e la strategia di allocazione spot `capacity-optimized` perché la propria richiesta di capacità spot abbia successo. Se si utilizzano altre strategie di allocazione, come `lowest-price`, la probabilità di ottenere la capacità spot disponibile non sarà in linea con il punteggio.
- Agire subito su un punteggio: il suggerimento del punteggio di posizionamento spot riflette la capacità spot disponibile al momento della richiesta e la stessa configurazione può produrre punteggi diversi se calcolati in momenti diversi a causa delle fluttuazioni della capacità spot. Mentre un punteggio di 10 significa che la propria richiesta di capacità spot è altamente probabile, ma non garantita, per ottenere risultati ottimali consigliamo di agire immediatamente su un punteggio. Consigliamo inoltre di ottenere un nuovo punteggio ogni volta che si prova a eseguire una richiesta di capacità.

Limitazioni

- Limite di capacità di destinazione – il limite di capacità di destinazione del punteggio di posizionamento spot si basa sul tuo recente utilizzo Spot, tenendo conto della potenziale crescita dell'utilizzo. Se non si ha un utilizzo Spot recente, forniamo un limite di default minimo allineato al limite della richiesta Spot.
- Limite di configurazioni di richieste: possiamo limitare il numero di nuove configurazioni di richieste a un periodo di 24 ore se rileviamo modelli non associati all'uso previsto della funzione del punteggio di posizionamento spot. Se si raggiunge il limite, è possibile riprovare le configurazioni delle richieste già utilizzate, ma non è possibile specificare nuove configurazioni di richiesta fino al successivo periodo di 24 ore.
- Numero minimo di tipi di istanza: se si specificano i tipi di istanza, è necessario specificare almeno tre tipi di istanza diversi, altrimenti Amazon EC2 restituirà un punteggio di posizionamento spot basso. Analogamente, se si specificano attributi di istanza, devono essere risolti con almeno tre tipi di istanza diversi. I tipi di istanza sono considerati diversi se hanno un nome diverso. Ad esempio, m5.8xlarge, m5a.8xlarge e m5.12xlarge sono considerati diversi.

Autorizzazioni IAM richieste

Per impostazione predefinita, le identità IAM (utenti, ruoli o gruppi) non dispongono dell'autorizzazione per utilizzare la funzione del punteggio di posizionamento spot. Per consentire alle identità IAM di utilizzare la funzione del punteggio di posizionamento spot, è necessario creare una policy IAM che conceda l'autorizzazione per utilizzare l'operazione API di `ec2:GetSpotPlacementScores`EC2. Quindi è necessario collegare la policy alle identità IAM che richiedono questa autorizzazione.

Di seguito viene riportata una policy IAM di esempio che concede le autorizzazioni per l'operazione API di `ec2:GetSpotPlacementScores` EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

Per informazioni sulla modifica di una policy IAM, consultare Editing IAM policies (Modifica di policy IAM) nella Guida per l'utente di IAM.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.

- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Calcolo di un punteggio di posizionamento spot

È possibile calcolare un punteggio di posizionamento spot utilizzando la console Amazon EC2 o la AWS CLI.

Argomenti

- Calcolo di un punteggio di posizionamento spot specificando gli attributi di istanza (console)
- Calcolo di un punteggio di posizionamento spot specificando i tipi di istanza (console)
- Calcolo di un punteggio di posizionamento spot (AWS CLI)

Calcolo di un punteggio di posizionamento spot specificando gli attributi di istanza (console)

Come calcolare un punteggio di posizionamento spot specificando gli attributi di istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Scegliere Spot placement score (Punteggio di posizionamento spot).
4. Scegliere Enter requirements (Inserisci i requisiti).
5. Per Target capacity (Capacità di destinazione), inserire la capacità desiderata in termini di numero di istanze o vCPU o la quantità di memoria (MiB).
6. Per Instance type requirements (Requisiti per il tipo di istanza), per specificare i requisiti di calcolo e consentire ad Amazon EC2 di identificare i tipi di istanza ottimali con questi requisiti, scegliere Specify instance attributes that match your compute requirements (Specifica gli attributi di istanza che corrispondono ai requisiti di calcolo).
7. Per vCPUs (vCPU) inserire il numero minimo e massimo desiderato di vCPU. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.
8. Per Memory (GiB) (Memoria [GiB]) inserire la quantità minima e massima di memoria desiderata. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.
9. Per Architettura della CPU, seleziona l'architettura dell'istanza desiderata.

10. (Facoltativo) Per Additional instance attributes (Attributi istanza aggiuntivi), facoltativamente, è possibile specificare uno o più attributi per esprimere i requisiti di calcolo in modo più dettagliato. Ogni attributo aggiuntivo aggiunge ulteriori vincoli alla tua richiesta. È possibile omettere gli attributi aggiuntivi, nel qual caso saranno utilizzati i valori di default. Per una descrizione di ogni attributo e dei relativi valori predefiniti, consulta get-spot-placement-scoresAmazon EC2 Command Line Reference.
11. (Facoltativo) Per visualizzare i tipi di istanza con gli attributi specificati, espandere Preview matching instance types (Anteprima tipi di istanza corrispondenti). Per escludere che i tipi di istanza vengano utilizzati nella valutazione del posizionamento, selezionare le istanze e quindi scegliereEscludi tipi di istanze.
12. Scegliere Load placement scores (Carica punteggi di posizionamento) e controllare i risultati.
13. (Facoltativo) Per visualizzare il punteggio di posizionamento spot per regioni specifiche, per Regions to evaluate (Regioni da valutare), selezionare le regioni da valutare, quindi scegliere Calculate placement scores (Calcola punteggi di posizionamento).
14. (Facoltativo) Per visualizzare il punteggio di posizionamento spot per le zone di disponibilità nelle regioni visualizzate, seleziona la casella di controllo Provide placement scores per Availability Zone (Fornisci punteggi di posizionamento per zona di disponibilità). Un elenco delle zone di disponibilità con punteggio è utile se si desidera avviare tutta la tua capacità spot in una singola zona di disponibilità.
15. (Facoltativo) Per modificare i requisiti di calcolo e ottenere un nuovo punteggio di posizionamento, scegliere Edit (Modifica), apportare le modifiche necessarie e quindi scegliere Calculate placement scores (Calcola punteggi di posizionamento).

Calcolo di un punteggio di posizionamento spot specificando i tipi di istanza (console)

Come calcolare un punteggio di posizionamento spot specificando i tipi di istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Scegliere Spot placement score (Punteggio di posizionamento spot).
4. Scegliere Enter requirements (Inserisci i requisiti).
5. Per Capacità di destinazione, inserire la capacità desiderata in termini di numero di istanze o vCPU o la quantità di memoria (MiB).
6. Per Instance type requirements (Requisiti del tipo di istanza), per specificare i tipi di istanza da utilizzare, scegliere Manually select instance types (Seleziona manualmente i tipi di istanza).

7. Scegliere Select instance types (Seleziona tipi di istanza), selezionare i tipi di istanza da utilizzare e quindi scegliere Select (Seleziona). Per trovare rapidamente i tipi di istanza, è possibile utilizzare la barra del filtro per filtrare i tipi di istanza in base a proprietà diverse.
8. Scegliere Carica punteggi di posizionamento e controllare i risultati.
9. (Facoltativo) Per visualizzare il punteggio di posizionamento spot per regioni specifiche, per Regions to evaluate (Regioni da valutare), selezionare le regioni da valutare, quindi scegliere Calculate placement scores (Calcola punteggi di posizionamento).
10. (Facoltativo) Per visualizzare il punteggio di posizionamento spot per le zone di disponibilità nelle regioni visualizzate, seleziona la casella di controllo Provide placement scores per Availability Zone (Fornisci punteggi di posizionamento per zona di disponibilità). Un elenco delle zone di disponibilità con punteggio è utile se si desidera avviare tutta la tua capacità spot in una singola zona di disponibilità.
11. (Facoltativo) Per modificare l'elenco dei tipi di istanze e ottenere un nuovo punteggio di posizionamento, scegliere Edit (Modifica), apportare le modifiche necessarie e quindi scegliere Calculate placement scores (Calcola punteggi di posizionamento).

Calcolo di un punteggio di posizionamento spot (AWS CLI)

Come calcolare il punteggio di posizionamento spot

1. (Facoltativo) Per generare tutti i possibili parametri che possono essere specificati per la configurazione del punteggio di posizionamento Spot, utilizza il get-spot-placement-scorescomando e il `--generate-cli-skeleton` parametro.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --generate-cli-skeleton
```

Output previsto

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
```

```
            ""
        ],
        "InstanceRequirementsWithMetadata": {
            "ArchitectureTypes": [
                "x86_64_mac"
            ],
            "VirtualizationTypes": [
                "hvm"
            ],
            "InstanceRequirements": {
                "VCpuCount": {
                    "Min": 0,
                    "Max": 0
                },
                "MemoryMiB": {
                    "Min": 0,
                    "Max": 0
                },
                "CpuManufacturers": [
                    "amd"
                ],
                "MemoryGiBPerVCpu": {
                    "Min": 0.0,
                    "Max": 0.0
                },
                "ExcludedInstanceTypes": [
                    ""
                ],
                "InstanceGenerations": [
                    "previous"
                ],
                "SpotMaxPricePercentageOverLowestPrice": 0,
                "OnDemandMaxPricePercentageOverLowestPrice": 0,
                "BareMetal": "excluded",
                "BurstablePerformance": "excluded",
                "RequireHibernateSupport": true,
                "NetworkInterfaceCount": {
                    "Min": 0,
                    "Max": 0
                },
                "LocalStorage": "included",
                "LocalStorageTypes": [
                    "hdd"
                ],
```

```
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Creare un file di configurazione JSON utilizzando l'output del passaggio precedente e configurarlo come segue:

   a. Per `TargetCapacity`, inserire la capacità spot desiderata in termini di numero di istanze o vCPU o quantità di memoria (MiB).

   b. Per `TargetCapacityUnitType`, inserire l'unità per la capacità di destinazione. Se si omette questo parametro, verrà utilizzato il parametro di default `units`.

      Valori validi: `units` (che si traduce in numero di istanze) | `vcpu` | `memory-mib`

c. Per `SingleAvailabilityZone`, specificare `true` per una risposta che restituisce un elenco di zone di disponibilità con punteggio. Un elenco delle zone di disponibilità con punteggio è utile se si desidera avviare tutta la tua capacità spot in una singola zona di disponibilità. Se si omette questo parametro, verrà utilizzato il parametro di default `false` e la risposta restituirà un elenco di regioni con punteggio.

d. (Facoltativo) Per `RegionNames`, specificare le regioni da utilizzare come filtro. È necessario specificare il codice regione, ad esempio, `us-east-1`.

   Con un filtro regione, la risposta restituisce solo le regioni specificate. Se si è specificato `true` per `SingleAvailabilityZone`, la risposta restituisce solo le zone di disponibilità nelle regioni specificate.

e. È possibile includere `InstanceTypes` o `InstanceRequirements`, ma non entrambi nella stessa configurazione.

   Specificare una delle seguenti opzioni nella configurazione JSON:

   - Per specificare un elenco di tipi di istanze, specificare i tipi di istanza nel parametro `InstanceTypes`. Specificare almeno tre tipi di istanza diversi. Se si specificano solo uno o due tipi di istanza, il punteggio di posizionamento spot sarà un punteggio basso. Per l'elenco dei tipi di istanza, consultare Tipi di istanza di Amazon EC2.
   - Per specificare gli attributi dell'istanza in modo che Amazon EC2 identifichi i tipi di istanza che corrispondono a tali attributi, specificare gli attributi che si trovano nella struttura `InstanceRequirements`.

     È necessario fornire valori per `VCpuCount`, `MemoryMiB` e `CpuManufacturers`. È possibile omettere gli altri attributi, nel qual caso saranno utilizzati i valori di default. Per una descrizione di ogni attributo e dei relativi valori predefiniti, consulta get-spot-placement-scoresAmazon EC2 Command Line Reference.

   Per gli esempi di configurazione, consulta Configurazioni di esempio.

3. Per ottenere il punteggio di posizionamento Spot per i requisiti specificati nel file JSON, usa il get-spot-placement-scorescomando e specifica il nome e il percorso del file JSON utilizzando il parametro. `--cli-input-json`

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
```

```
    --cli-input-json file://file_name.json
```

Output di esempio se `SingleAvailabilityZone` è impostato su `false` o se viene omesso (se omesso, verrà utilizzato il valore di default `false`): viene restituito un elenco di regioni con punteggio

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Output di esempio se `SingleAvailabilityZone` è impostato su `true`: viene restituito un elenco di zone di disponibilità con punteggio

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1"
        "Score": 8
    },
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3"
        "Score": 6
    },
   ...
```

Configurazioni di esempio

Quando si utilizza AWS CLI, è possibile utilizzare le seguenti configurazioni di esempio.

Configurazioni di esempio

- Esempio: specifica dei tipi di istanza e della capacità di destinazione
- Esempio: specifica dei tipi di istanza e della capacità di destinazione in termini di memoria

- Esempio: specifica degli attributi per la selezione del tipo di istanza basata su attributi
- Esempio: specifica degli attributi per la selezione del tipo di istanza basata su attributi e restituzione di un elenco di zone di disponibilità con punteggio

Esempio: specifica dei tipi di istanza e della capacità di destinazione

La configurazione di esempio seguente specifica tre diversi tipi di istanza e una capacità spot di destinazione di 500 istanze spot.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500
}
```

Esempio: specifica dei tipi di istanza e della capacità di destinazione in termini di memoria

Il seguente esempio di configurazione specifica tre diversi tipi di istanza e una capacità spot di destinazione di 500.000 MiB di memoria, in cui il numero di istanze spot da avviare deve fornire un totale di 500.000 MiB di memoria.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

Esempio: specifica degli attributi per la selezione del tipo di istanza basata su attributi

La seguente configurazione di esempio è configurata per la selezione del tipo di istanza basata su attributi ed è seguita da una spiegazione della configurazione di esempio.

```
{
```

```
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

`InstanceRequirementsWithMetadata`

Per utilizzare la selezione dell'istanza basata su attributi, è necessario includere la struttura `InstanceRequirementsWithMetadata` nella configurazione e specificare gli attributi desiderati per le istanze spot.

Nell'esempio precedente, vengono specificati i seguenti attributi di istanza:

- `ArchitectureTypes`: il tipo di architettura dei tipi di istanza deve essere `arm64`.
- `VirtualizationTypes`: il tipo di virtualizzazione dei tipi di istanza deve essere `hvm`.
- `VCpuCount`: i tipi di istanza devono avere un minimo di 1 e un massimo di 12 vCPU.
- `MemoryMiB`: i tipi di istanza devono avere un minimo di 512 MiB di memoria. Omettendo il parametro `Max`, si sta indicando che non esiste un limite massimo.

Si noti che sono disponibili diversi altri attributi facoltativi che è possibile specificare. Per l'elenco degli attributi, consulta get-spot-placement-scoresAmazon EC2 Command Line Reference.

`TargetCapacityUnitType`

Il parametro `TargetCapacityUnitType` specifica l'unità per la capacità di destinazione. Nell'esempio, la capacità di destinazione è `5000` e il tipo di unità della capacità di destinazione è `vcpu`, che insieme specificano una capacità di destinazione desiderata di 5.000 vCPU, dove il numero di istanze spot da avviare deve fornire un totale di 5000 vCPU.

Esempio: specifica degli attributi per la selezione del tipo di istanza basata su attributi e restituzione di un elenco di zone di disponibilità con punteggio

La seguente configurazione di esempio è configurata per la selezione del tipo di istanza basata su attributi. Specificando `"SingleAvailabilityZone": true`, la risposta restituirà un elenco di zone di disponibilità con punteggio.

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

Tieni traccia dei costi delle tue istanze Spot iscrivendoti a un feed di dati

Per facilitare la comprensione delle spese per le proprie istanze spot, Amazon EC2 fornisce un feed di dati che descrive l'utilizzo e i prezzi delle proprie istanze spot. Tale feed di dati viene inviato a un bucket Amazon S3 specificato al momento dell'iscrizione al feed di dati.

I file dei feed di dati arrivano nel bucket in genere una volta all'ora. Se non si dispone di un'istanza spot in esecuzione durante una determinata ora, per quell'ora non si riceve un file di feed di dati.

Ogni ora di utilizzo dell'istanza Spot è in genere coperta da un unico file di dati. Questi file vengono compressi (gzip) prima di essere consegnati al tuo bucket. Amazon EC2 può scrivere più file per una data ora di utilizzo in cui i file sono grandi (ad esempio, quando il contenuto del file per quell'ora supera i 50 MB prima della compressione).

> **Note**
>
> Puoi creare un solo feed di dati di istanze Spot per volta Account AWS.

Il feed di dati delle istanze Spot è supportato in tutte le AWS regioni tranne Cina (Pechino), Cina (Ningxia), AWS GovCloud (Stati Uniti) e le regioni che sono disabilitate per impostazione predefinita.

Indice

Nome e formato del file di feed di dati

Il nome del file di feed di dati dell'istanza spot utilizza il formato seguente (con data e ora in UTC):

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Per esempio, se il nome del proprio bucket è **`DOC-EXAMPLE-BUCKET`** e il proprio prefisso è **`my-prefix`**, i nomi dei propri file sono simili ai seguenti:

```
DOC-EXAMPLE-BUCKET.s3.amazonaws.com/my-prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Per ulteriori informazioni sui nomi dei bucket, consultare Regole per la denominazione dei bucket in Guida per l'utente di Amazon S3.

I file di feed di dati dell'istanza spot sono delimitati da tabulatori. Ogni riga del file di dati corrisponde a un'ora di istanza e contiene i campi elencati nella tabella seguente.

Campo	Descrizione

Campo	Descrizione
`Timestamp`	Il timestamp utilizzato per stabilire il prezzo applicato per l'utilizzo di questa istanza.
`UsageType`	Il tipo di utilizzo e il tipo di istanza per cui viene addebitato il costo. Per la `m1.small` Istanze spot, questo campo è impostato su `SpotUsage` . Per tutti gli altri tipi di istanza, questo campo è impostato su `SpotUsage:` {instance-type}. Ad esempio, `SpotUsage:c1.medium` .
`Operation`	Il prodotto per il quale viene richiesto il pagamento. Per le Istanze spot, di Linux, questo campo è impostato su `RunInstances` . Per le Istanze spot, di Windows, questo campo è impostato su `RunInstances:0002` . L'utilizzo dello Spot è raggruppato in base alla zona di disponibilità.
`InstanceID`	L'ID dell'istanza spot che ha generato l'utilizzo dell'istanza.
`MyBidID`	L'ID della richiesta di istanza spot che ha generato l'utilizzo dell'istanza.
`MyMaxPrice`	Il prezzo massimo specificato per questa richiesta .
`MarketPrice`	Il prezzo Spot nell'orario specificato nel campo `Timestamp` .
`Charge`	Prezzo addebitato per l'utilizzo di questa istanza.
`Version`	La versione del feed di dati. La versione possibile è 1.0.

Requisiti bucket Amazon S3

Al momento dell'iscrizione al feed di dati, bisogna specificare un bucket Amazon S3 in cui memorizzare i file di feed di dati.

Prima di scegliere un bucket Amazon S3 per il feed di dati, considerare quanto segue:

- È necessario disporre delle autorizzazioni `FULL_CONTROL` per il bucket. Se si è il proprietario del bucket, si è in possesso dell'autorizzazione per impostazione predefinita. Altrimenti, il proprietario del bucket deve concedere Account AWS questa autorizzazione.
- Quando ti iscrivi a un data feed, queste autorizzazioni vengono utilizzate per aggiornare l'ACL del bucket e concedere l'autorizzazione all'account del AWS data feed. `FULL_CONTROL` L'account del AWS data feed scrive i file del data feed nel bucket. Se il proprio account non dispone delle autorizzazioni necessarie, i file di feed di dati non possono essere scritti nel bucket. Per ulteriori informazioni, consulta Logs sent to Amazon S3 nella CloudWatch Amazon Logs User Guide.

  > **Note**
  >
  > Se aggiorni l'ACL e rimuovi le autorizzazioni per l'account del AWS data feed, i file del data feed non possono essere scritti nel bucket. Bisogna iscriversi nuovamente al feed di dati per ricevere i file di feed di dati.

- Ogni file di feed di dati ha il proprio ACL (separato da quello per il bucket). Il proprietario del bucket dispone dell'autorizzazione `FULL_CONTROL` ai file di dati. L'account del AWS data feed dispone di autorizzazioni di lettura e scrittura.
- Se hai disabilitato gli ACL per i tuoi bucket, aggiungi una policy sui bucket che consenta il pieno controllo degli utenti sulla scrittura nel bucket. Per ulteriori informazioni, consulta Rivedere e aggiornare le politiche dei bucket che utilizzano chiavi di condizione relative agli ACL.
- Se elimini l'abbonamento al feed di dati, Amazon EC2 non rimuove le autorizzazioni di lettura e scrittura per l'account del feed di AWS dati né sul bucket né sui file di dati. È necessario rimuovere tali autorizzazioni.
- È necessario utilizzare una chiave gestita dal cliente se si crittografa il bucket Amazon S3 utilizzando la crittografia lato server con AWS KMS una chiave memorizzata in (SSE-KMS). AWS Key Management Service Per ulteriori informazioni, consulta la crittografia lato server con bucket Amazon S3 nella Amazon Logs User Guide. CloudWatch

  > **Note**
  >
  > Per il data feed di istanze Spot, la risorsa che genera i file S3 non è più Amazon CloudWatch Logs. Pertanto, devi rimuovere la sezione `aws:SourceArn` dalla policy di autorizzazione del bucket S3 e dalla policy KMS.

Iscriversi al feed di dati per l'istanza spot

Per iscriverti al tuo feed di dati, usa il create-spot-datafeed-subscription AWS CLI comando.

```
aws ec2 create-spot-datafeed-subscription \
    --bucket DOC-EXAMPLE-BUCKET \
    [--prefix my-prefix]
```

Output di esempio

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "111122223333",
        "Bucket": "DOC-EXAMPLE-BUCKET",
        "Prefix": "my-prefix",
        "State": "Active"
    }
}
```

Descrivere il feed di dati per l'istanza spot

Per descrivere la tua sottoscrizione al data feed, usa il describe-spot-datafeed-subscription AWS CLI comando.

```
aws ec2 describe-spot-datafeed-subscription
```

Output di esempio

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "123456789012",
        "Prefix": "spotdata",
        "Bucket": "DOC-EXAMPLE-BUCKET",
        "State": "Active"
    }
}
```

Visualizzare i dati nel feed di dati

Nel AWS Management Console, apri AWS CloudShell. Usa il seguente comando s3 sync per recuperare i file.gz dal bucket S3 per il tuo data feed e archiviarli nella cartella specificata.

```
aws s3 sync s3://DOC-EXAMPLE-BUCKET ./data-feed
```

Per visualizzare i contenuti di un file .gz, passare alla cartella in cui sono stati archiviati i contenuti del bucket S3.

```
cd data-feed
```

Utilizzare il comando ls per visualizzare i nomi dei file. Utilizzare il comando zcat con il nome del file per visualizzare i contenuti del file compresso. Il seguente è un comando di esempio.

```
zcat  111122223333.2023-12-09-07.001.b959dbc6.gz
```

Di seguito è riportato un output di esempio.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
 Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium       RunInstances:SV050
 i-0c3e0c0b046e050df     sir-pwq6nmfp    0.0510000000 USD        0.0142000000 USD
  0.0142000000 USD        1
```

Eilminare il feed di dati per l'istanza spot

Per eliminare il tuo feed di dati, usa il comando. delete-spot-datafeed-subscription AWS CLI

```
aws ec2 delete-spot-datafeed-subscription
```

Quote di istanze Spot

Sono previste delle quote per il numero di istanze Spot in esecuzione e per le richieste di istanze Spot in sospeso per Account AWS per regione. Una volta soddisfatta una richiesta di istanza Spot in sospeso, la richiesta non viene più conteggiata ai fini del raggiungimento della quota, poiché a tal fine verrà conteggiata l'istanza in esecuzione.

Le quote delle istanze spot vengono gestiti in termini di numero di unità di elaborazione centrale virtuali (vCPU) che vengono utilizzate o verranno utilizzate dalle istanze spot in esecuzione in attesa dell'evasione delle richieste aperte. Se termini le istanze spot ma non annulli le richieste di istanze

spot, le richieste vengono conteggiate ai fini della quota di vCPU delle istanze spot fino a quando Amazon EC2 non rileva la terminazione delle istanze spot e chiude le richieste.

Per le istanze spot forniamo i seguenti tipi di quota:

- Tutte le richieste di istanza spot DL
- Tutte le richieste di istanza spot F
- Tutte le richieste di istanza spot G e VT
- Tutte le richieste di istanza spot Inf
- Tutte le richieste di istanza spot P
- Tutte le richieste di istanza spot standard (A, C, D, H, I, M, R, T, Z)
- Tutte le richieste di istanza spot Trn
- Tutte le richieste di istanza spot X

Ogni tipo di quota specifica il numero massimo di vCPU per una o più famiglie di istanza. Per informazioni sulle diverse famiglie di istanze, sulle generazioni e le dimensioni, consulta Tipi di istanze Amazon EC2.

È possibile avviare una qualsiasi combinazione di tipi di istanza che soddisfano le mutevoli esigenze dell'applicazione. Ad esempio, con una quota di richieste di istanze spot tutte standard di 256 vCPU, puoi avviare 32 istanze spot `m5.2xlarge` (32 x 8 vCPU) oppure 16 istanze spot `c5.4xlarge` (16 x 16 vCPU).

Attività

- Monitoraggio delle quote e dell'utilizzo delle istanze spot
- Richiesta di un aumento della quota

Monitoraggio delle quote e dell'utilizzo delle istanze spot

Puoi visualizzare e gestire le quote delle istanze spot utilizzando i seguenti metodi:

- La pagina delle Service Quotas di Amazon EC2 nella console delle Service Quotas
- get-service-quota AWS CLI

Per ulteriori informazioni, vedere Service Quotas di Amazon EC2 Visualizzazione delle quote di servizio nella Service Quotas User Guide.

Con l'integrazione di Amazon CloudWatch Metrics, puoi monitorare l'utilizzo di EC2 rispetto alle tue quote. Puoi anche configurare gli allarmi per ricevere un avviso quando stai per raggiungere le quote. Per ulteriori informazioni, consulta Service Quotas e Amazon CloudWatch alarms nella Service Quotas User Guide Visualizzazione delle quote di servizio Amazon User Guide. CloudWatch

Richiesta di un aumento della quota

Anche se Amazon EC2 aumenta automaticamente le quote delle istanze spot in base al tuo utilizzo, se necessario puoi richiedere un aumento della quota. Ad esempio, se si intende avviare più istanze spot di quante consentite dalla quota corrente, è possibile richiedere un aumento della quota. Puoi richiedere un aumento della quota anche se invii una richiesta di istanza spot e ricevi l'errore `Max spot instance count exceeded`. Per richiedere un aumento di una quota, è possibile utilizzare la console Service Quotas descritta alla pagina Service Quotas di Amazon EC2.

Istanze a prestazioni espandibili

I tipi di istanza T sono istanze con prestazioni espandibili. Se avvii le tue istanze spot utilizzando un tipo di istanza espandibile, e prevedi di utilizzare l'istanza spot espandibile immediatamente e per un breve periodo, senza alcun tempo di inattività per accumulare crediti CPU, suggeriamo di avviarla in Modalità Standard per evitare costi più elevati. Se avvii le istanze spot a prestazioni espandibili in Modalità Illimitata ed espandi la capacità di CPU immediatamente, l'espansione implicherà il dispendio dei crediti in più. Se l'istanza viene utilizzata per un periodo di tempo limitato, non riesce ad accumulare crediti CPU per ripagare i crediti extra, che i vengono quindi addebitati al termine dell'istanza.

La modalità illimitata è adatta per la Istanze spot con prestazioni burstable solo se l'istanza viene eseguita per un periodo di tempo sufficiente ad accumulare i crediti CPU per l'espansione. In caso contrario, il pagamento di crediti in eccedenza rende le prestazioni Istanze spot espandibili più costose rispetto all'utilizzo di altre istanze. Per ulteriori informazioni, consulta Quando utilizzare la modalità illimitata rispetto alla CPU fissa.

Le istanze T2, se configurate in modalità Standard, ottengono crediti di avvio. Le istanze T2 sono le uniche istanze a prestazioni espandibili che ottengono crediti di avvio. I crediti di avvio hanno lo scopo di fornire un'esperienza di avvio iniziale produttiva per le istanze T2, fornendo risorse di calcolo sufficienti per configurare l'istanza. Non sono consentiti avvii ripetuti di istanze T2 per accedere a nuovi crediti di avvio. Se occorre una CPU duratura, è possibile guadagnare crediti (rimanendo inattivi per un certo periodo) utilizzando la Unlimited mode (Modalità Illimitata) per istanze spot T2 o un tipo di istanza con una CPU dedicata.

Host dedicati di Amazon EC2

Un host dedicato Amazon EC2 è un server fisico completamente dedicato al tuo utilizzo. Facoltativamente, puoi scegliere di condividere la capacità dell'istanza con altri AWS account. Per ulteriori informazioni, consulta Condivisione di host dedicati Amazon EC2 su più account.

Gli host dedicati forniscono visibilità e controllo sul posizionamento delle istanze e supportano l'affinità con gli host. Ciò significa che puoi avviare ed eseguire istanze su host specifici e assicurarti che le istanze vengano eseguite solo su host specifici. Per ulteriori informazioni, consulta Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host.

Gli host dedicati forniscono un supporto completo per la licenza BYOL (Bring Your Own License). Consentono di utilizzare le licenze software esistenti per socket, per core o per macchina virtuale, tra cui Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux o altre licenze software legate a macchine virtuali, socket o core fisici, in base ai termini della licenza.

Se hai bisogno che le tue istanze vengano eseguite su hardware dedicato, ma non hai bisogno di visibilità o controllo sul posizionamento delle istanze e non hai bisogno di utilizzare licenze software per socket o per core, puoi prendere in considerazione l'utilizzo di istanze dedicate. Le istanze dedicate e gli host dedicati possono essere entrambi utilizzati per avviare istanze Amazon EC2 su server fisici dedicati. Non ci sono differenze di prestazioni, sicurezza o fisiche tra le Istanze dedicate e le istanze negli Host dedicati. Tuttavia, ci sono alcune differenze fondamentali tra loro. La tabella seguente evidenzia alcune differenze chiave tra istanze dedicate e host dedicati:

	Dedicated Host	Dedicated Instance
Server fisico dedicato	Server fisico con capacità di istanza completamente dedicata all'uso dell'utente.	Server fisico dedicato a un singolo account cliente.
Condivisione della capacità delle istanze	Può condividere la capacità dell'istanza con altri account.	Non supportato
Fatturazione	Fatturazione per host	Fatturazione per istanza
Visibilità di socket, core e ID host	Fornisce la visibilità del numero di socket e core fisici	Nessuna visibilità

	Dedicated Host	Dedicated Instance
Affinità a livello di host e istanza	Consente di distribuire in modo omogeneo le istanze sullo stesso server fisico nel tempo	Non supportato
Posizionamento delle istanze interessate	Fornisce ulteriore visibilità e controllo sul posizionamento delle istanze su un server fisico	Non supportato
Ripristino automatico dell'istanza	Supportato. Per ulteriori informazioni, consulta Ripristino dell'host dedicato Amazon EC2.	Supportata
Modello di licenza Bring Your Own License (BYOL)	Supportato	Supporto parziale*
Prenotazioni della capacità	Non supportato	Supportata

* Le licenze Microsoft SQL Server con mobilità delle licenze tramite Software Assurance e Windows Virtual Desktop Access (VDA) possono essere utilizzate con l'istanza dedicata.

Per ulteriori informazioni sulle istanze dedicate, consulta la pagina Istanze dedicate Amazon EC2.

Restrizioni degli Host dedicati

Prima di allocare le occorrenze degli Host dedicati, considera le seguenti limitazioni e restrizioni:

- Per eseguire RHEL, SUSE Linux e SQL Server su Host dedicati, è necessario portare le proprie AMI. Le AMI RHEL, SUSE Linux e SQL Server offerte AWS o disponibili su non Marketplace AWS possono essere utilizzate con host dedicati. Per ulteriori informazioni su come creare un'AMI personalizzata, consulta Porta le tue licenze software agli host dedicati di Amazon EC2.

Questa restrizione non si applica agli host allocati per istanze di memoria elevata (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`). Le AMI Linux RHEL e SUSE offerte da AWS o disponibili su Marketplace AWS possono essere utilizzate con questi host.

- È previsto un limite per il numero di host dedicati in esecuzione per famiglia di istanze per account AWS per regione. Le quote si applicano solo alle istanze in esecuzione. Se l'istanza è in sospeso, in arresto o arrestata, non viene conteggiata ai fini della quota. Per visualizzare le quote del tuo account o richiederne un aumento, utilizza la console Service Quotas.
- Le istanze eseguite su un Host dedicato possono essere avviate solo in un VPC.
- I gruppi Auto Scaling sono supportati solo quando si utilizza un modello di avvio che specifica un gruppo di risorse host. Per ulteriori informazioni, consulta Creazione di un modello di avvio con impostazioni avanzate nella Guida per l'utente di Dimensionamento automatico Amazon EC2.
- Le istanze di Amazon RDS non sono supportate.
- Il livello AWS di utilizzo gratuito non è disponibile per gli host dedicati.
- Il controllo del posizionamento delle istanze fa riferimento alla gestione degli avvii delle istanze sulle occorrenze degli Host dedicati. Non è possibile eseguire l'avvio di Host dedicati nei gruppi di collocazione.
- Se assegni un host per un tipo di istanza virtualizzata, successivamente non potrai modificare il tipo di istanza in `.metal`. Ad esempio, se assegni un host per il tipo di istanza `m5.large`, non puoi modificare il tipo di istanza in `m5.metal`.

  Allo stesso modo, se assegni un host per un tipo di istanza `.metal`, successivamente non potrai modificare il tipo di istanza in un'istanza virtualizzata. Ad esempio, se assegni un host per il tipo di istanza `m5.metal`, non puoi modificare il tipo di istanza in `m5.large`.

Indice

- Modifica l'impostazione di posizionamento automatico per un host dedicato Amazon EC2 esistente
- Modifica i tipi di istanza supportati per un host dedicato Amazon EC2 esistente
- Modifica la tenancy e l'affinità dell'host dedicato Amazon EC2 per un'istanza Amazon EC2
- Rilascia un host dedicato Amazon EC2
- Acquista prenotazioni per host dedicati per ricevere sconti sulla fatturazione
- Condivisione di host dedicati Amazon EC2 su più account
- Host dedicati Amazon EC2 su AWS Outposts
- Ripristino dell'host dedicato Amazon EC2
- Manutenzione dell'host per l'host dedicato Amazon EC2
- Monitora lo stato dei tuoi host dedicati Amazon EC2
- Tieni traccia delle modifiche alla configurazione dell'host dedicato di Amazon EC2 utilizzando AWS Config

Prezzi e fatturazione dell'host dedicato Amazon EC2

Il prezzo di un Host dedicato varia in base all'opzione di pagamento.

Opzioni di pagamento

- Host dedicati on-demand
- Dedicated Host Reservations
- Savings Plans
- Prezzi per Windows Server su Host dedicati

Host dedicati on-demand

La fatturazione on-demand viene automaticamente attivata quando esegui l'allocazione di un Host dedicato all'account.

Il prezzo on demand per un Host dedicato varia in base alla famiglia di istanze e alla regione. Il pagamento è al secondo (con un minimo di 60 secondi) per Host dedicato attivo, indipendentemente dalla quantità o dalla dimensione delle istanze che scegli di avviare su di esso. Per ulteriori informazioni sulla tariffazione on demand, consulta la pagina relativa ai prezzi on demand degli Host dedicati di Amazon EC2.

Puoi rilasciare un Host dedicato on-demand in qualsiasi momento per interrompere l'addebito dei relativi costi. Per informazioni sul rilascio di un Host dedicato, consulta Rilascia un host dedicato Amazon EC2.

Dedicated Host Reservations

Prenotazioni di host dedicati offre uno sconto significativo rispetto al prezzo on demand degli Host dedicati. Le prenotazioni sono disponibili con tre diverse opzioni di pagamento:

- Nessun pagamento anticipato —Le prenotazioni di questo tipo garantiscono uno sconto sull'uso dell'Host dedicato in un determinato periodo e non richiedono alcun pagamento anticipato. Opzione disponibile per un periodo di un anno o di tre anni. Solo alcune famiglie di istanze supportano il periodo di tre anni per Nessuna prenotazione anticipata.
- Pagamento anticipato parziale — Una parte della prenotazione deve essere pagata in anticipo, mentre le restanti ore nel periodo scelto vengono fatturate in base a una tariffa scontata. Opzione disponibile per un periodo di un anno o di tre anni.
- Pagamento anticipato intero costo — Questa soluzione offre il prezzo effettivo più basso. Si tratta di un'opzione disponibile per un periodo di un anno e di tre anni, che copre l'intero costo anticipato del periodo, senza costi aggiuntivi futuri.

Prima di poter acquistare le prenotazioni, devi disporre di occorrenze degli Host dedicati attive nel tuo account. Ogni prenotazione può coprire uno o più host che supportano la stessa famiglia di istanze in una singola zona di disponibilità. Le prenotazioni vengono applicate alla famiglia di istanze presenti sull'host e non alle dimensioni delle istanze. Se hai tre Host dedicati con dimensioni di istanze diverse (`m4.xlarge`, `m4.medium` e `m4.large`) puoi associare un'unica prenotazione `m4` con tutti gli Host dedicati. La famiglia di istanze e la zona di disponibilità della prenotazione devono corrispondere a quelle degli host dedicati a cui intendi associarla.

Quando una prenotazione è associata a un Host dedicato, l'Host dedicato può essere rilasciato solo dopo il termine della prenotazione.

Per ulteriori informazioni sui prezzi delle prenotazioni, consulta la pagina dei Prezzi degli Host dedicati di Amazon EC2.

Savings Plans

I Savings Plans sono un modello tariffario flessibile che offre risparmi significativi sulle Istanze on demand. Con i Savings Plans, ti impegni a garantire una quantità di utilizzo coerente, in USD all'ora,

per un periodo di uno o tre anni. Questo ti offre la flessibilità di utilizzare il Host dedicati che più si adatta alle tue esigenze e di continuare a risparmiare denaro, piuttosto che impegnarsi con un Host dedicato specifico. Per ulteriori informazioni, consulta la Guida per l'utente dei Savings Plans di AWS.

> **Note**
>
> I Savings Plans non sono supportati con `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e host dedicati `u-24tb1.metal`.

Prezzi per Windows Server su Host dedicati

Conformemente alle condizioni di licenza di Microsoft, puoi portare le tue licenze per Windows Server e SQL Server negli Host dedicati. Non sono previsti costi aggiuntivi per l'uso del software se decidi di portare le tue licenze personali.

Inoltre, puoi anche usare le AMI di Windows Server fornite da Amazon per eseguire le versioni più recenti di Windows Server sui Host dedicati. Ciò è comune per i contesti in cui disponi di licenze SQL Server idonee per l'esecuzione su Host dedicati ma serve Windows Server per eseguire il carico di lavoro di SQL Server. Le AMI Windows Server fornite da Amazon sono supportate solo sui tipi di istanze della generazione corrente. Per maggiori informazioni, consulta Prezzi degli host dedicati di Amazon EC2.

Configurazioni della capacità delle istanze di Amazon EC2 Dedicated Host

Gli host dedicati supportano diverse configurazioni (core fisici, socket e vCPU) che consentono di eseguire istanze di famiglie e dimensioni diverse.

Quando assegni un host dedicato nel tuo account, puoi scegliere una configurazione che supporti o un tipo di istanza singola, oppure più tipi di istanze appartenenti alla stessa famiglia di istanze. Il numero di istanze che puoi eseguire su un host dipende dalla configurazione scelta.

Indice

Supporto per tipi di istanza singola

Puoi allocare un host dedicato che supporti un solo tipo di istanza. Con questa configurazione, ogni istanza che lanci sull'host dedicato deve essere dello stesso tipo dell'istanza specificata al momento dell'allocazione dell'host.

Ad esempio, puoi allocare un host che supporti solo il tipo di istanza `m5.4xlarge`. In questo caso, puoi eseguire solo istanze `m5.4xlarge` su quell'host.

Il numero di istanze che puoi avviare sull'host dipende dal numero di core fisici forniti dall'host e dal numero di core consumati dal tipo di istanza specificato. Ad esempio, se assegni un host per istanze `m5.4xlarge` l'host fornisce 48 core fisici e ciascuna `m5.4xlarge`istanza consuma 8 core fisici. Ciò significa che puoi avviare fino a 6 istanze su quell'host (48 core fisici/ 8 core per istanza = 6 istanze).

Supporto per più tipi di istanze

È possibile allocare un host dedicato che supporti più tipi di istanze all'interno della stessa famiglia di istanze. Ciò ti consente di eseguire diversi tipi di istanze sullo stesso host, purché le istanze siano della stessa famiglia e l'host disponga di una capacità di istanza sufficiente.

Ad esempio, puoi allocare un host che supporti tipi di istanze diverse all'interno della famiglia di istanze `R5`. In questo caso, puoi lanciare qualsiasi combinazione di tipi di istanza `R5` ad esempio`r5.large`,`r5.xlarge`,`r5.2xlarge`, e`r5.4xlarge`, su quell'host, fino alla capacità fisica principale dell'host.

Le seguenti famiglie di istanze supportano gli host dedicati con supporto per più tipi di istanze:

- Scopo generale: A1, M5, M5n, M6i e T3
- Ottimizzate per il calcolo: C5, C5n, and C6i
- Memoria ottimizzata:R5, R5n e R6i

Il numero di istanze che è possibile eseguire sull'host dipende dal numero di core fisici forniti dall'host e dal numero di core consumati da ogni tipo di istanza che viene eseguita sull'host. Ad esempio, se assegni un host `R5` che fornisce 48 core fisici, e tu esegui due istanze `r5.2xlarge` (4 core x 2 istanze) e tre istanze `r5.4xlarge` (8 core x 3 istanze), queste istanze consumano un totale di 32 core e quindi puoi eseguire qualsiasi combinazione di istanze `R5` purché non superino i 16 core rimanenti.

Tuttavia, per ogni famiglia di istanze, esiste un limite al numero di istanze che è possibile eseguire per ogni dimensione di istanza. Ad esempio, un Host dedicato R5 supporta fino a 2 istanze `r5.8xlarge`, utilizzando 32 core fisici. È quindi possibile utilizzare istanze R5 aggiuntive di altre dimensioni per riempire l'host fino alla capacità core. Per il numero supportato di dimensioni di istanze di ogni famiglia di istanze, consulta Tabella per la configurazione degli host dedicati.

La tabella seguente mostra esempi di combinazioni di istanze:

Famiglia di istanze	Esempi di combinazioni di tipi di istanza
R5	• Esempio 1: 4 x `r5.4xlarge` + 4 x `r5.2xlarge` • Esempio 2: 1 x `r5.12xlarge` + 1 x `r5.4xlarge` + 1 x `r5.2xlarge` + 5 x `r5.xlarge` + 2 x `r5.large`
C5	• Esempio 1: 1 x `c5.9xlarge` + 2 x `c5.4xlarge` + 1 x `c5.xlarge` • Esempio 2: 4 x `c5.4xlarge` + 1 x `c5.xlarge` + 2 x `c5.large`
M5	• Esempio 1: 4 x `m5.4xlarge` + 4 x `m5.2xlarge` • Esempio 2: 1 x `m5.12xlarge` + 1 x `m5.4xlarge` + 1 x `m5.2xlarge` + 5 x `m5.xlarge` + 2 x `m5.large`

Considerazioni

Tieni presente che quando lavori con host dedicati che supportano più tipi di istanze:

- Con gli host dedicati di tipo N, come C5n, M5n e R5n, non è possibile combinare istanze di dimensioni inferiori (`2xlarge` e più piccole) con istanze di dimensioni maggiori (`4xlarge` e più grandi, incluse `metal`). Se hai bisogno contemporaneamente di istanze di dimensioni più piccole e

più grandi su host dedicati di tipo N devi allocare host separati per le istanze di dimensioni minori e maggiori.

- Si consiglia di avviare prima le istanze più grandi, poi utilizzare la capacità di istanza rimanente con le istanze più piccole in base alle esigenze.

Istanze T3 espandibili su host dedicati Amazon EC2

Gli host dedicati supportano istanze T3 con prestazioni espandibili. Le istanze T3 forniscono un modo efficiente nei costi per utilizzare il software di licenza BYOL idoneo su hardware dedicato. Le dimensioni ridotte della vCPU delle istanze T3 consentono di consolidare i carichi di lavoro su un numero inferiore di host e ottimizzare l'utilizzo delle licenze per core.

Gli host dedicati T3 sono più adatti per l'esecuzione del software BYOL con utilizzo della CPU da basso a moderato. Sono incluse le licenze software idonee per socket, core o macchina virtuale, quali Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux e Oracle Database. Esempi di carichi di lavoro adatti per gli host dedicati T3 sono database di dimensioni medie e ridotte, desktop virtuali, ambienti di sviluppo e test, archivi di codice e prototipi di prodotto. Gli host dedicati T3 non sono consigliati per carichi di lavoro con un utilizzo prolungato della CPU o per carichi di lavoro che subiscono espansioni della CPU mentre è in uso.

Le istanze T3 sugli host dedicati utilizzano lo stesso modello di credito delle istanze T3 sull'hardware di tenancy condiviso. Tuttavia, supportano solo la modalità di credito `standard`, mentre non supportano la modalità di credito `unlimited`. Nella modalità `standard`, le istanze T3 su host dedicati possono guadagnare, spendere e accumulare crediti nello stesso modo previsto per le istanze espandibili sull'hardware di tenancy condiviso. Le istanze espandibili forniscono un livello di base di prestazioni della CPU, con la possibilità di superare temporaneamente questo livello. Per superare la baseline, l'istanza spende i crediti accumulati nel suo saldo del credito CPU. Una volta esauriti i crediti accumulati, l'utilizzo della CPU viene ridotto al livello di base. Per ulteriori informazioni sulla modalità `standard`, consulta la pagina Come funzionano le istanze a prestazioni espandibili Standard.

Gli host dedicati T3 supportano tutte le funzionalità offerte dagli host dedicati Amazon EC2, incluse le dimensioni di istanze multiple su un singolo host, gruppi di risorse host e BYOL.

Dimensioni e configurazioni dell'istanza T3 supportate

Gli host dedicati T3 eseguono istanze T3 espandibili di scopo generico che condividono le risorse della CPU dell'host, fornendo prestazioni della CPU di base e la possibilità di passare a un livello

superiore quando necessario. Ciò consente agli host dedicati T3, che possiedono 48 core, di supportare fino a un massimo di 192 istanze per host. Per utilizzare in modo efficiente le risorse dell'host e fornire le migliori prestazioni dell'istanza, l'algoritmo di posizionamento delle istanze Amazon EC2 calcola automaticamente il numero supportato di istanze e le combinazioni di dimensioni delle istanze che possono essere avviate sull'host.

Gli host dedicati T3 supportano più tipi di istanza sullo stesso host. Tutte le istanze T3 sono supportate su host dedicati. È possibile eseguire diverse combinazioni di istanze T3 fino al limite della CPU dell'host.

Nella tabella seguente sono riportati i tipi di istanze supportati, le prestazioni di ciascun tipo di istanza e il numero massimo di istanze di ogni dimensione che è possibile avviare.

Tipo di istan	vCPU	Memoria (GiB)	Utilizzo di base della CPU per vCPU	Larghezza di banda burst di rete (Gbps)	Larghezza di banda burst Amazon EBS (Mbps)	Numero massimo di istanze per host dedicato
t3.na	2	0,5	5%	5	Fino a 2.085	192
t3.m	2	1	10%	5	Fino a 2.085	192
t3.sn	2	2	20%	5	Fino a 2.085	192
t3.m	2	4	20%	5	Fino a 2.085	192
t3.la	2	8	30%	5	2.780	96
t3.xl	4	16	40%	5	2.780	48
t3.2x e	8	32	40%	5	2.780	24

Monitorare l'utilizzo della CPU per gli host dedicati T3

Puoi utilizzare il CloudWatch parametro `DedicatedHostCPUUtilization` Amazon per monitorare l'utilizzo della vCPU di un host dedicato. Il parametri è disponibile nello spazio dei nomi `EC2` e nella dimensione `Per-Host-Metrics`. Per ulteriori informazioni, consulta Parametri degli host dedicati.

Porta le tue licenze software agli host dedicati di Amazon EC2

Gli Host dedicati ti consentono di utilizzare licenze software esistenti per socket, core o macchina virtuale. Quando utilizzi la tua licenza, sei responsabile della sua gestione. Amazon EC2 offre tuttavia caratteristiche che aiutano a rispettare la conformità delle licenze, come l'affinità e il posizionamento delle istanze interessate.

Di seguito sono descritte le procedure generali da seguire per utilizzare immagini di macchine virtuali con contratto multilicenza di tipo BYOL in Amazon EC2.

1. Verificare che le condizioni di licenza che determinano l'uso delle immagini di macchine virtuali ne consentano l'utilizzo in un ambiente cloud virtualizzato. Per ulteriori informazioni sui programmi di licenze Microsoft, consulta l'argomento relativo alle opzioni di licenza per i software Microsoft su Amazon Web Services.
2. Dopo aver verificato se l'immagine della macchina virtuale può essere utilizzata in Amazon EC2, importala utilizzando VM Import/Export. Per ulteriori informazioni su come importare l'immagine della macchina virtuale, consulta la Guida per l'utente di VM Import/Export.
3. Dopo avere importato l'immagine della macchina virtuale, da questa è possibile avviare le istanze negli Host dedicati attivi dell'account.
4. Quando vengono eseguite queste istanze, in base al sistema operativo in uso, potrebbe venire richiesto di attivare queste istanze mediante il server KMS (ad esempio, Windows Server o Windows SQL Server). Non è possibile attivare l'AMI Windows importata nel server Amazon KMS per Windows.

> **Note**
>
> Per tenere traccia del modo in cui vengono utilizzate le immagini AWS, abilita la registrazione host in. AWS ConfigÈ possibile AWS Config utilizzarlo per registrare le modifiche alla configurazione su un host dedicato e utilizzare l'output come fonte di dati per il reporting delle licenze. Per ulteriori informazioni, consulta Tieni traccia delle modifiche alla configurazione dell'host dedicato di Amazon EC2 utilizzando AWS Config.

Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host

Il controllo del posizionamento per Host dedicati viene eseguito sia a livello di istanza che a livello di host.

Auto-posizionamento

L'auto-posizionamento viene configurato a livello di host e consente di gestire se le istanze vengono avviate su un host specifico o su qualsiasi host disponibile che dispone di configurazioni corrispondenti.

Quando l'auto-posizionamento di un Host dedicato è disabilitato, sono accettati solo gli avvii di istanza della tenancy host in cui sia specificato il relativo ID host univoco. Questa rappresenta l'impostazione di default per le nuove occorrenze degli Host dedicati.

Quando l'auto-posizionamento di un Host dedicato è abilitato, è accettato qualsiasi avvio non mirato corrispondente alla relativa configurazione del tipo di istanza.

Quando viene avviata un'istanza, devi configurare la relativa tenancy. L'avvio di un'istanza in un Host dedicato senza definire un valore specifico per `HostId` consente l'avvio dell'istanza su qualsiasi Host dedicato con l'auto-posizionamento abilitato e con il tipo di istanza corrispondente.

Affinità host

L'affinità host viene configurata a livello di istanza. Definisce la relazione di avvio tra un'istanza e un Host dedicato.

Quando l'affinità è impostata su `Host`, un'istanza avviata su un host specifico, se arrestata, verrà sempre riavviata sullo stesso host. Ciò è valido sia per gli avvii mirati che per quelli non mirati.

Quando l'affinità è impostata su `Default`, se si arresta e quindi riavvia un'istanza, tale istanza può essere riavviata su qualsiasi host disponibile. Tuttavia, l'istanza eseguirà un tentativo di riavvio sull'ultimo Host dedicato su cui è stata avviata (sulla base del miglior tentativo).

Assegna un host dedicato Amazon EC2 da utilizzare nel tuo account

Per iniziare a utilizzare un host dedicato, devi prima allocarlo nel tuo account. Dopo aver allocato l'Host dedicato, la capacità Host dedicato viene resa immediatamente disponibile nell'account e puoi iniziare ad avviare istanze sull'Host dedicato.

Quando assegni un host dedicato nel tuo account, puoi scegliere una configurazione che supporti o un tipo di istanza singola, oppure più tipi di istanze appartenenti alla stessa famiglia di istanze. Il numero di istanze che puoi eseguire su un host dipende dalla configurazione scelta. Per ulteriori informazioni, consulta Configurazioni della capacità delle istanze di Amazon EC2 Dedicated Host.

Console

Per allocare un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati), quindi Allocate Host dedicato (Alloca host dedicati).
3. Per Instance family (Famiglia di istanze), scegliere la famiglia di istanze per l'Host dedicato.
4. Specificare se l'Host dedicato supporta più dimensioni di istanze all'interno della famiglia di istanze selezionata o solo un tipo di istanza specifico. Scegli una delle seguenti operazioni.
   - Per configurare l'Host dedicato per supportare più tipi di istanze nella famiglia di istanze selezionata, per Support multiple instance types (Supporto per più tipi di istanza) selezionare Enable (Abilita). L'abilitazione di questa opzione consente di avviare diverse dimensioni di istanza dalla stessa famiglia di istanze sull'Host dedicato. Ad esempio, se si sceglie la famiglia di istanze `m5` e si seleziona questa opzione, è possibile avviare le istanze `m5.xlarge` e `m5.4xlarge` sull'Host dedicato.
   - Per configurare l'Host dedicato per supportare un tipo di istanza singolo all'interno della famiglia di istanze selezionata, deselezionare Support multiple instance types (Supporto per più tipi di istanze), quindi per Instance type (Tipo di istanza), scegliere il tipo di istanza da supportare. L'abilitazione di questa opzione consente di avviare un singolo tipo di istanza sull'Host dedicato. Ad esempio, se si sceglie questa opzione e si specifica `m5.4xlarge` come il tipo di istanza supportato, è possibile avviare solo istanze `m5.4xlarge` sull'Host dedicato.
5. Per Availability Zone (Zona di disponibilità), scegliere la zona di disponibilità in cui allocare l'Host dedicato.
6. Per consentire all'Host dedicato di accettare avvii di istanze non mirati che corrispondono a questo tipo di istanza, per Instance auto-placement (Autoposizionamento istanza), scegliere Attiva. Per ulteriori informazioni sull'auto-posizionamento, consulta Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host.
7. Per abilitare il ripristino per l'Host dedicato, per Host recovery (Ripristino host), scegliere Enable (Attiva). Per ulteriori informazioni, consulta Ripristino dell'host dedicato Amazon EC2.
8. Per Quantity (Quantità), immettere il numero di Host dedicati da allocare.
9. (Facoltativo) Seleziona Aggiungi nuovo tag e immetti una chiave e un valore di tag.
10. Selezionare Alloca.

AWS CLI

Per allocare un Host dedicato

Usa il comando allocate-hosts AWS CLI . Il comando seguente consente di allocare un Host dedicato che supporta più tipi di istanza della famiglia di istanze `m5` nella zona di disponibilità `us-east-1a`. Nell'host, il ripristino host è abilitato e l'auto-posizionamento è disabilitato.

```
aws ec2 allocate-hosts --instance-family "m5" --availability-zone "us-east-1a" --
auto-placement "off" --host-recovery "on" --quantity 1
```

Il comando seguente alloca un Host dedicato che supporta avvii di istanze non mirati `m4.large` nella zona di disponibilità `eu-west-1a`, abilita il ripristino host e applica un tag con la chiave `purpose` e il valore `production`.

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a"
 --auto-placement "on" --host-recovery "on" --quantity 1 --tag-specifications
 'ResourceType=dedicated-host,Tags=[{Key=purpose,Value=production}]'
```

PowerShell

Per allocare un Host dedicato

Usa il comando. New-EC2Host AWS Tools for Windows PowerShell Il comando seguente consente di allocare un Host dedicato che supporta più tipi di istanza della famiglia di istanze `m5` nella zona di disponibilità `us-east-1a`. Nell'host, il ripristino host è abilitato e l'auto-posizionamento è disabilitato.

```
PS C:\> New-EC2Host -InstanceFamily m5 -AvailabilityZone us-east-1a -
AutoPlacement Off -HostRecovery On -Quantity 1
```

I comandi seguenti allocano un Host dedicato che supporta avvii di istanze non mirati `m4.large` nella zona di disponibilità `eu-west-1a`, abilitano il ripristino host e applicano un tag con la chiave `purpose` e il valore `production`.

Il parametro `TagSpecification` utilizzato per aggiungere un tag a Host dedicato al momento della creazione, richiede un oggetto che specifichi il tipo di risorsa da taggare, la chiave del tag e il valore del tag. I seguenti comandi creano l'oggetto richiesto.

```
PS C:\> $tag = @{ Key="purpose"; Value="production" }
```

```
PS C:\> $tagspec = new-object Amazon.EC2.Model.TagSpecification
PS C:\> $tagspec.ResourceType = "dedicated-host"
PS C:\> $tagspec.Tags.Add($tag)
```

Il comando seguente alloca il Host dedicato e applica il tag specificato all'oggetto `$tagspec`.

```
PS C:\> New-EC2Host -InstanceType m4.large -AvailabilityZone eu-west-1a -
AutoPlacement On -HostRecovery On -Quantity 1 -TagSpecification $tagspec
```

Avvia istanze Amazon EC2 su un host dedicato Amazon EC2

Dopo aver allocato un Host dedicato, puoi avviare istanze su tale host. Non puoi avviare istanze con la tenancy `host` se non disponi di occorrenze attive degli Host dedicati con una capacità disponibile sufficiente per il tipo di istanza che stai avviando.

> **Tip**
>
> Per gli host dedicati che supportano più dimensioni di istanza, si consiglia di avviare prima le istanze di grandi dimensioni e di riempire la capacità di istanza rimanente con le istanze di dimensioni più piccole in base alle esigenze.

Prima di avviare le istanze, considera le seguenti limitazioni. Per ulteriori informazioni, consulta Restrizioni degli Host dedicati.

Puoi avviare un'istanza su un Host dedicato utilizzando uno dei seguenti metodi.

Console

Per avviare un'istanza su un Host dedicato specifico dalla pagina Host dedicati

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Host dedicati (Host dedicati).
3. Nella pagina Dedicated Hosts (Host dedicati), seleziona un host e scegli Operazioni, Avvia istanze sull'host.
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI dall'elenco.

> **Note**
>
> Le AMI di SQL Server, SUSE e RHEL fornite da Amazon EC2 non possono essere utilizzate con le occorrenze degli Host dedicati.

5. Nella sezione Tipo di istanza, seleziona il tipo di istanza da avviare.

> **Note**
>
> Se l'Host dedicato supporta solo un singolo tipo di istanza, il tipo di istanza supportato viene selezionato per impostazione predefinita e non può essere modificato.
> Se l'Host dedicato supporta più tipi di istanza, occorre selezionare un tipo di istanza all'interno della famiglia di istanze supportata in base alla capacità di istanze disponibile dell'Host dedicato. Si consiglia di avviare prima le istanze di grandi dimensioni e di riempire la capacità di istanza rimanente con le istanze di dimensioni più piccole in base alle esigenze.

6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da associare all'istanza.
7. Nella sezione Dettagli avanzati, per Tenancy Affinity, scegli una delle seguenti opzioni:

   - Disattivata: l'affinità con l'host è disattivata. L'istanza viene avviata sull'host specificato, ma non è garantito il riavvio sullo stesso host dedicato se interrotta.
   - Un ID host dedicato: l'affinità host è abilitata. Se interrotta, l'istanza si riavvia sempre sull'host specificato, se dispone di capacità. Se l'host non dispone di capacità, l'istanza non può essere riavviata; è necessario stabilire l'affinità con un host diverso.

   Per ulteriori informazioni sull'affinità, consulta Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host.

> **Note**
>
> Le opzioni Tenancy e Host sono preconfigurate in base all'host selezionato.

8. Configura le opzioni rimanenti dell'istanza in base alla necessità. Per ulteriori informazioni, consulta Avvio di un'istanza utilizzando parametri definiti.

9. Scegliere Launch Instance (Avvia istanza).

Per avviare un'istanza su un Host dedicato tramite la procedura guidata di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Istanze, Avvia istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI dall'elenco.

   > **Note**
   >
   > Le AMI di SQL Server, SUSE e RHEL fornite da Amazon EC2 non possono essere utilizzate con le occorrenze degli Host dedicati.

4. Nella sezione Tipo di istanza, seleziona il tipo di istanza da avviare.
5. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da associare all'istanza.
6. Nella sezione Avanzate, effettua le operazioni seguenti:

   a. Per Tenancy, scegli Host dedicato.

   b. Per Target host by (Host di destinazione per), seleziona Host ID (ID host).

   c. Per Target host ID (ID host di destinazione), seleziona l'host su cui avviare l'istanza.

   d. Per l'affinità Tenancy, scegli una delle seguenti opzioni:

      - Disattivata: affinità host disattivata. L'istanza viene avviata sull'host specificato, ma non è garantito il riavvio sullo stesso host dedicato se interrotta.
      - Un ID host dedicato: l'affinità host è abilitata. Se interrotta, l'istanza si riavvia sempre sull'host specificato, se dispone di capacità. Se l'host non dispone di capacità, l'istanza non può essere riavviata; è necessario stabilire l'affinità con un host diverso.

      Per ulteriori informazioni sull'affinità, consulta Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host.

7. Configura le opzioni rimanenti dell'istanza in base alla necessità. Per ulteriori informazioni, consulta Avvio di un'istanza utilizzando parametri definiti.
8. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Per avviare un'istanza su un'Host dedicato

Utilizzate il AWS CLI comando run-instances e specificate l'affinità, la tenancy e l'host dell'istanza nel parametro request. `Placement`

PowerShell

Per avviare un'istanza su un'Host dedicato

Usa il New-EC2Instance AWS Tools for Windows PowerShell comando e specifica l'affinità, la tenancy e l'host dell'istanza nel parametro di richiesta. `Placement`

Avvia le istanze Amazon EC2 in un gruppo di risorse host

Gli host dedicati sono inoltre integrati con. AWS License Manager Con License Manager, è possibile creare un gruppo di risorse host, ovvero una raccolta di Host dedicati gestiti come una singola entità. Quando si crea un gruppo di risorse host, si specificano le preferenze di gestione host, ad esempio l'allocazione automatica e il rilascio automatico, per gli Host dedicati. In questo modo è possibile avviare le istanze in Host dedicati senza allocare e gestire manualmente tali host. Per ulteriori informazioni, consulta la sezione relativa ai Host Resource Groups nella Guida per l'utente di AWS License Manager .

Quando si avvia un'istanza in un gruppo di risorse host che include un Host dedicato con capacità di istanze disponibile, Amazon EC2 avvia l'istanza su tale host. Se il gruppo di risorse host non include un host con capacità di istanze disponibile, Amazon EC2 alloca automaticamente un nuovo host nel gruppo di risorse host e quindi avvia l'istanza su tale host. Per ulteriori informazioni, consulta la sezione relativa ai gruppi di risorse host nella Guida per l'utente di AWS License Manager .

Requisiti e limiti

- È necessario associare una configurazione di licenza basata su core o socket all'AMI.
- Non è possibile utilizzare le AMI di SQL Server, SUSE o RHEL fornite da Amazon EC2 con Host dedicati.
- Non è possibile scegliere un host specifico scegliendo un ID host e non è possibile abilitare l'affinità di istanza quando si avvia un'istanza in un gruppo di risorse host.

È possibile avviare un'istanza in un gruppo di risorse host utilizzando i metodi descritti di seguito.

Console

Per avviare un'istanza in un gruppo di risorse host

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Istanze, Avvia istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI dall'elenco.

   > **Note**
   >
   > Le AMI di SQL Server, SUSE e RHEL fornite da Amazon EC2 non possono essere utilizzate con le occorrenze degli Host dedicati.

4. Nella sezione Tipo di istanza, seleziona il tipo di istanza da avviare.
5. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da associare all'istanza.
6. Nella sezione Avanzate, effettua le operazioni seguenti:

   a. Per Tenancy, scegli Dedicated Host (Host dedicato).

   b. Per Target host by (Host di destinazione per), seleziona Host resource group (Gruppo di risorse host).

   c. Per Tenancy host resource group (Gruppo di risorse host di tenancy), scegli il gruppo di risorse host in cui avviare l'istanza.

   d. Per Tenancy affinity (Affinità locazione), effettua una delle operazioni seguenti:

      - Seleziona Disattivata: l'istanza viene avviata sull'host specificato ma non è garantito che venga riavviata sullo stesso host dedicato se viene arrestata.
      - Seleziona l'ID host dedicato: se viene arrestata, l'istanza viene sempre riavviata su questo host specifico.

   Per ulteriori informazioni sull'affinità, consulta Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host.

7. Configura le opzioni rimanenti dell'istanza in base alla necessità. Per ulteriori informazioni, consulta Avvio di un'istanza utilizzando parametri definiti.
8. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Per avviare un'istanza in un gruppo di risorse host

Utilizzate il AWS CLI comando run-instances e, nel parametro `Placement` request, omettete l'opzione Tenancy e specificate l'ARN del gruppo di risorse host.

PowerShell

Per avviare un'istanza in un gruppo di risorse host

Utilizzate il New-EC2Instance AWS Tools for Windows PowerShell comando e, nel parametro `Placement` request, omettete l'opzione Tenancy e specificate l'ARN del gruppo di risorse host.

Modifica l'impostazione di posizionamento automatico per un host dedicato Amazon EC2 esistente

Puoi modificare le impostazioni di posizionamento automatico di un host dedicato dopo averlo assegnato al tuo AWS account, utilizzando uno dei seguenti metodi.

Console

Per modificare il posizionamento automatico di un Host dedicato

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Selezionare un host e scegliere Actions (Operazioni), Modify host (Modifica host).
4. In instance auto-placement (auto-posizionamento istanza), scegliere Enable (Abilita) per abilitare l'auto-posizionamento oppure deselezionare Enable (Abilita) per disabilitare l'auto-posizionamento. Per ulteriori informazioni, consulta Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host.
5. Seleziona Salva.

AWS CLI

Per modificare il posizionamento automatico di un Host dedicato

Utilizzate il comando modify-hosts AWS CLI . Gli esempi seguenti abilitano l'auto-posizionamento per l'Host dedicato specificato.

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

PowerShell

Per modificare il posizionamento automatico di un Host dedicato

Usa il comando. Edit-EC2Host AWS Tools for Windows PowerShell Gli esempi seguenti abilitano l'auto-posizionamento per l'Host dedicato specificato.

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

Modifica i tipi di istanza supportati per un host dedicato Amazon EC2 esistente

Puoi modificare un Host dedicato per cambiare i tipi di istanza supportati. Se attualmente supporta un singolo tipo di istanza, puoi modificarlo per supportare più tipi di istanza all'interno di tale famiglia di istanze. Analogamente, se attualmente supporta più tipi di istanza, puoi modificarlo per supportare solo un tipo di istanza specifico.

Per modificare un Host dedicato per supportare più tipi di istanza, occorre innanzitutto interrompere tutte le istanze in esecuzione sull'host. Il completamento di questa modifica richiede circa 10 minuti. L'Host dedicato passa allo stato `pending` mentre è in corso la modifica. Non è possibile avviare istanze interrotte o lanciare nuove istanze sull'Host dedicato mentre si trova nello stato `pending`.

Per modificare un Host dedicato che supporta più tipi di istanza per supportare solo un tipo di istanza singolo, l'host non deve avere istanze in esecuzione o il tipo delle istanze in esecuzione deve essere supportato dall'host. Ad esempio, per modificare un host che supporta più tipi di istanza nella famiglia di istanze `m5` per supportare solo istanze `m5.large`, non devono esserci istanze in esecuzione sull'Host dedicato o quelle in esecuzione devono essere solo istanze `m5.large`.

Se assegni un host per un tipo di istanza virtualizzata, successivamente non potrai modificare il tipo di istanza in `.metal`. Ad esempio, se assegni un host per il tipo di istanza `m5.large`, non puoi modificare il tipo di istanza in `m5.metal`. Allo stesso modo, se assegni un host per un tipo di istanza `.metal`, successivamente non potrai modificare il tipo di istanza in un'istanza virtualizzata. Ad esempio, se assegni un host per il tipo di istanza `m5.metal`, non puoi modificare il tipo di istanza in `m5.large`.

È possibile modificare i tipi di istanza supportati utilizzando uno dei metodi descritti di seguito.

Console

Per modificare i tipi di istanza supportati per un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Dedicated Host (Host dedicato).
3. Selezionare l'Host dedicato da modificare e scegliere Actions (Operazioni), Modify host (Modifica host).
4. In base alla configurazione corrente dell'Host dedicato, eseguire una delle operazioni riportate di seguito:

   - Se l'Host dedicato attualmente supporta un tipo di istanza specifico, l'opzione Support multiple instance types (Supporto per più tipi di istanza) non è abilitata e Instance type (Tipo di istanza) elenca il tipo di istanza supportato. Per modificare l'host per supportare più tipi nella famiglia di istanze corrente, per Support multiple instance types (Supporto per più tipi di istanza), selezionare Enable (Abilita).

     Prima di modificare un host per supportare più tipi di istanza, è necessario innanzitutto interrompere tutte le istanze in esecuzione su di esso.
   - Se l'Host dedicato attualmente supporta più tipi di istanza in una famiglia di istanze, l'opzione Enabled (Abilitato) è selezionata per Support multiple instance types (Supporto per più tipi di istanza). Per modificare l'host per supportare un tipo di istanza specifico, per Support multiple instance types (Supporto per più tipi di istanza), deselezionare Enable (Abilita), quindi per Instance type (Tipo di istanza), selezionare il tipo di istanza da supportare.

     Non è possibile modificare la famiglia di istanze supportata da Host dedicato.
5. Seleziona Salva.

AWS CLI

Per modificare i tipi di istanza supportati per un Host dedicato

Usa il comando modify-hosts AWS CLI .

Il comando seguente consente di modificare un Host dedicato per supportare più tipi di istanza all'interno della famiglia di istanze `m5`.

```
aws ec2 modify-hosts --instance-family m5 --host-ids h-012a3456b7890cdef
```

Il comando seguente consente di modificare un Host dedicato per supportare solo istanze `m5.xlarge`.

```
aws ec2 modify-hosts --instance-type m5.xlarge --instance-family --host-
ids h-012a3456b7890cdef
```

PowerShell

Per modificare i tipi di istanza supportati per un Host dedicato

Usa il comando. Edit-EC2Host AWS Tools for Windows PowerShell

Il comando seguente consente di modificare un Host dedicato per supportare più tipi di istanza all'interno della famiglia di istanze `m5`.

```
PS C:\> Edit-EC2Host --InstanceFamily m5 --HostId h-012a3456b7890cdef
```

Il comando seguente consente di modificare un Host dedicato per supportare solo istanze `m5.xlarge`.

```
PS C:\> Edit-EC2Host --InstanceType m5.xlarge --HostId h-012a3456b7890cdef
```

Modifica la tenancy e l'affinità dell'host dedicato Amazon EC2 per un'istanza Amazon EC2

Puoi modificare la tenancy di un'istanza dopo averla avviata. Puoi anche modificare l'affinità della tua istanza per indirizzarla a un host specifico o consentirne l'avvio su qualsiasi host dedicato disponibile con attributi corrispondenti nel tuo account. Per modificare la tenancy o l'affinità dell'istanza, lo stato dell'istanza deve essere `stopped`.

I dettagli del sistema operativo dell'istanza e l'eventuale installazione di SQL Server influiscono sulle conversioni supportate. Per ulteriori informazioni sui percorsi di conversione di tenancy disponibili per la tua istanza, consulta Conversione di tenancy nella Guida per l'utente di License Manager.

> **Note**
>
> Per le istanze T3, è necessario avviare l'istanza su un host dedicato per utilizzare una tenancy di `host`. Per le istanze T3, non è possibile modificare la tenancy da `host` a `dedicated` o `default`. Se si prova ad apportare una di queste modifiche di tenancy non supportate, verrà visualizzato il codice di errore `InvalidRequest`.

È possibile modificare la tenancy e l'affinità di un'istanza utilizzando i metodi descritti di seguito.

Console

Per modificare la tenancy o l'affinità dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Instances (Istanze) e selezionare l'istanza da modificare.
3. Scegli Instance state (Stato istanza), Stop (Arresta).
4. Con l'istanza selezionata, scegli Operazioni, Impostazioni istanza, Modifica posizionamento delle istanze.
5. Nella pagina Modifica il posizionamento dell'istanza, configura quanto segue:
   - Tenancy — Scegliere una delle opzioni indicate di seguito.
     - Run a dedicated hardware instance (Esegui un'istanza hardware dedicata) — Avvia l'istanza sotto forma di Istanza dedicata. Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.
     - Launch the instance on a Host dedicato (Avvia istanza su un host dedicato) — Avvia l'istanza su un Host dedicato con l'affinità configurabile.
   - Affinity (Affinità) — Scegliere una delle opzioni indicate di seguito.
     - This instance can run on any one of my hosts (Questa istanza può essere eseguita su uno qualsiasi dei miei host) – L'istanza viene avviata su qualsiasi Host dedicato disponibile nell'account che supporti il relativo tipo di istanza.
     - This instance can only run on the selected host (Questa istanza può essere eseguita solo sull'host selezionato) – L'istanza può essere eseguita solo sull'Host dedicato selezionato per l'opzione Target Host (Host target).

- Target Host (Host target) — Selezionare l'Host dedicato su cui deve essere eseguita l'istanza. Se nell'elenco non è presente alcun host target, è possibile che l'account non includa degli Host dedicati compatibili disponibili.

Per ulteriori informazioni, consulta Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host.

6. Seleziona Salva.

AWS CLI

Per modificare la tenancy o l'affinità dell'istanza

Utilizzate il modify-instance-placement AWS CLI comando. Gli esempi seguenti illustrano la modifica dell'affinità dell'istanza specificata da `default` in `host` e l'impostazione dell'Host dedicato con cui l'istanza ha affinità.

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host
 --tenancy host --host-id h-012a3456b7890cdef
```

PowerShell

Per modificare la tenancy o l'affinità dell'istanza

Usa il Edit-EC2InstancePlacement AWS Tools for Windows PowerShell comando. Gli esempi seguenti illustrano la modifica dell'affinità dell'istanza specificata da `default` in `host` e l'impostazione dell'Host dedicato con cui l'istanza ha affinità.

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -
Tenancy host -HostId h-012a3456b7890cdef
```

Rilascia un host dedicato Amazon EC2

Se non hai più bisogno di un host dedicato, puoi interrompere le istanze in esecuzione sull'host, indirizzarle all'avvio su un host diverso e quindi rilasciare l'host.

Prima di poter rilasciare l'host, è necessario arrestare tutte le istanze in esecuzione sull'Host dedicato. È possibile eseguire la migrazione di queste istanze su altre occorrenze degli Host dedicati

nel tuo account in modo da consentirti di continuare a utilizzarle. Queste fasi sono valide solo per le occorrenze degli Host dedicati on-demand.

È possibile rilasciare un Host dedicato utilizzando i seguenti metodi.

Console

Per rilasciare un Host dedicato

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Nella pagina Host dedicati, selezionare il Host dedicato da rilasciare.
4. Scegliere Actions (Operazioni), Release host (Rilascia host).
5. Scegliere Release (Rilascia).

AWS CLI

Per rilasciare un Host dedicato

Usa il comando release-hosts AWS CLI .

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

Per rilasciare un Host dedicato

Usa il comando. Remove-EC2Hosts AWS Tools for Windows PowerShell

```
PS C:\> Remove-EC2Hosts -HostId h-012a3456b7890cdef
```

Dopo aver rilasciato un Host dedicato, non potrai riutilizzare lo stesso host o ID host, né ti verranno addebitati i relativi costi nella fatturazione del servizio on-demand. Lo stato dell'Host dedicato dedicato viene cambiato in `released` e su tale host non sarà più possibile avviare istanze.

> **Note**
>
> Nel caso di Host dedicati rilasciati di recente, potrebbe essere necessario un po' di tempo prima che vengano esclusi dal conteggio del limite. Durante questo periodo, potresti

riscontrare errori di tipo `LimitExceeded` quando cerchi di allocare nuove occorrenze degli Host dedicati. Se questo è il caso, prova ad allocare nuovi host dopo pochi minuti.

Le istanze precedentemente arrestate continuano a essere disponibili per l'uso e sono elencate nella pagina Instances (Istanze). Relativamente alla tenancy, tali istanze conservano l'impostazione `host`.

Acquista prenotazioni per host dedicati per ricevere sconti sulla fatturazione

Le prenotazioni per host dedicati offrono uno sconto fino al 70 percento rispetto ai prezzi degli host dedicati su richiesta. È necessario disporre di host dedicati attivi allocati nel proprio account prima di poter acquistare prenotazioni per host dedicati. Per ulteriori informazioni, consulta Dedicated Host Reservations.

Puoi acquistare prenotazioni per host dedicati utilizzando i seguenti metodi:

Console

Per acquistare le prenotazioni

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Host dedicati, Prenotazioni di host dedicati, Purchase (Acquista) Prenotazioni di host dedicati.
3. Nella schermata Trova offerte, procedi come segue:
   a. Per la famiglia di istanze, seleziona la famiglia di istanze dell'Host dedicato per la quale acquistare la Prenotazione Host Dedicato.
   b. Per l'opzione di pagamento, seleziona e configura l'opzione di pagamento preferita.
4. Seleziona Successivo.
5. Seleziona gli host dedicati a cui associare la prenotazione di host dedicati, quindi scegli Avanti.
6. (Facoltativo) Assegna tag alla prenotazione dell'host dedicato.
7. Controlla il tuo ordine e scegli Acquista.

AWS CLI

Per acquistare le prenotazioni

1. Usa il describe-host-reservation-offerings AWS CLI comando per elencare le offerte disponibili che soddisfano le tue esigenze. Nel seguente esempio sono elencate le offerte che supportano le istanze appartenenti alla famiglia di istanze `m4` e il cui termine è un anno.

   > **Note**
   >
   > Il termine è specificato in secondi. Un anno pertanto corrisponde a 31.536.000 secondi, mentre tre anni corrispondono a 94.608.000.

   ```
   aws ec2 describe-host-reservation-offerings --filter Name=instance-family,Values=m4 --max-duration 31536000
   ```

   Il comando restituisce l'elenco di offerte corrispondenti ai criteri impostati. Annotare il valore `offeringId` dell'offerta da acquistare.

2. Usa il purchase-host-reservation AWS CLI comando per acquistare l'offerta e fornisci quanto `offeringId` indicato nel passaggio precedente. L'esempio seguente acquista la prenotazione specificata e la associa a un Host dedicato specifico già allocato nell' AWS account e applica un tag con una chiave `purpose` e un valore di. `production`

   ```
   aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --host-id-set h-013abcd2a00cbd123 --tag-specifications 'ResourceType=host-reservation,Tags={Key=purpose,Value=production}'
   ```

PowerShell

Per acquistare le prenotazioni

1. Utilizzate il Get-EC2HostReservationOffering AWS Tools for Windows PowerShell comando per elencare le offerte disponibili che soddisfano le vostre esigenze. Negli esempi seguenti sono elencate le offerte che supportano le istanze appartenenti alla famiglia di istanze `m4` e il cui termine è un anno.

> **Note**
>
> Il termine è specificato in secondi. Un anno pertanto corrisponde a 31.536.000 secondi, mentre tre anni corrispondono a 94.608.000.

```
PS C:\> $filter = @{Name="instance-family"; Value="m4"}
```

```
PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
```

Il comando restituisce l'elenco di offerte corrispondenti ai criteri impostati. Annotare il valore `offeringId` dell'offerta da acquistare.

2. Usa il New-EC2HostReservation AWS Tools for Windows PowerShell comando per acquistare l'offerta e fornisci quanto `offeringId` indicato nel passaggio precedente. L'esempio seguente acquista la prenotazione specificata e la associa a un host dedicato specifico che è già allocato nell' AWS account.

```
PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -
HostIdSet h-013abcd2a00cbd123
```

Condivisione di host dedicati Amazon EC2 su più account

La condivisione di host dedicati consente ai proprietari di host dedicati di condividere i propri host dedicati con altri AWS account o all'interno di un' AWS organizzazione. Ciò consente di creare e gestire host dedicati centralmente e di condividere l'host dedicato su più AWS account o all'interno AWS dell'organizzazione.

In questo modello, l' AWS account proprietario dell'Host dedicato (proprietario) lo condivide con altri AWS account (consumatori). I consumatori possono avviare istanze negli Host dedicati condivisi con loro così come le avvierebbero negli Host dedicati che allocano nel proprio account. Il proprietario è responsabile della gestione dell'Host dedicato e delle istanze avviate in esso. I proprietari non possono modificare le istanze avviate dai consumatori negli Host dedicati condivisi. I consumatori sono responsabili della gestione delle istanze che avviano negli Host dedicati condivisi con loro. I consumatori non possono visualizzare o modificare le istanze appartenenti ad altri consumatori o al proprietario dell'Host dedicato e non possono modificarle gli Host dedicati condivisi con loro.

Il proprietario di un Host dedicato può condividere un Host dedicato con:

- AWS Account specifici all'interno o all'esterno dell' AWS organizzazione
- Un'unità organizzativa all'interno della sua AWS organizzazione
- La sua intera AWS organizzazione

Indice

Prerequisiti per la condivisione di Host dedicati

- Per condividere un host dedicato, devi possederlo nel tuo AWS account. Non puoi condividere un Host dedicato che è stato condiviso con te.
- Per condividere un Host dedicato con la tua AWS organizzazione o un'unità organizzativa AWS della tua organizzazione, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilitare la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .

Limitazioni per la condivisione di Host dedicato

Non è possibile condividere Host dedicati che sono stati allocati per i seguenti tipi di istanza: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`.

Servizi correlati

AWS Resource Access Manager

La condivisione dell'Host dedicato si integra con AWS Resource Access Manager (AWS RAM). AWS RAM è un servizio che ti consente di condividere AWS le tue risorse con qualsiasi AWS account o tramite AWS Organizations. Con AWS RAM, condividi le risorse di tua proprietà creando una condivisione di risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori possono essere singoli AWS account, unità organizzative o un'intera organizzazione AWS Organizations.

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Condivisione tra zone di disponibilità

Per garantire che le risorse vengano distribuite tra le zone di disponibilità di una regione, mappiamo in modo indipendente le zone di disponibilità ai nomi per ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la zona `us-east-1a` di disponibilità del tuo AWS account potrebbe non avere la stessa posizione `us-east-1a` di un altro AWS account.

Per individuare la posizione dell'Host dedicati relativamente ai tuoi account, devi utilizzare l'ID della zona di disponibilità. L'ID della zona di disponibilità è un identificatore univoco e coerente per una zona di disponibilità per tutti gli AWS account. Ad esempio, `use1-az1` è un ID di zona di disponibilità per la regione `us-east-1` e identifica la stessa posizione in ogni account AWS .

Per visualizzare gli ID delle zone di disponibilità nel tuo account

1. Apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram.
2. Gli ID delle zone di disponibilità per la regione corrente sono visualizzati nel pannello Your AZ ID (Il tuo ID zona di disponibilità) sul lato destro dello schermo.

Autorizzazioni di Host dedicato condivisi

Autorizzazioni per i proprietari

I proprietari sono responsabili della gestione dei propri Host dedicati condivisi e delle istanze che avviano su di essi. I proprietari possono vedere tutte le istanze in esecuzione sull'Host dedicato condiviso, incluse quelle avviate dai consumatori. Non possono però eseguire alcuna operazione sulle istanze in esecuzione che sono state avviate dai consumatori.

Autorizzazioni per i consumatori

I consumatori sono responsabili della gestione delle istanze che avviano su un Host dedicato condiviso con loro. Non possono modificare l'Host dedicato condiviso in nessun modo e non possono visualizzare o modificare le istanze appartenenti ad altri consumatori o al proprietario dell'Host dedicato.

Fatturazione e misurazione

Non sono previsti costi aggiuntivi per la condivisione di Host dedicati.

Ai proprietari vengono addebitati gli Host dedicati che condividono. Ai consumatori non viene addebitato alcun costo per le istanze che avviano sugli Host dedicati condivisi.

Le Prenotazioni di host dedicati continuano a fornire sconti di fatturazione per gli Host dedicati condivisi. Solo i proprietari di Host dedicato possono acquistare Prenotazioni di host dedicati per gli Host dedicati condivisi che possiedono.

Limiti di Host dedicato

Gli Host dedicati condivisi vengono conteggiati solo ai fini dei limiti di Host dedicati del proprietario. I limiti di Host dedicati dei consumatori non sono influenzati dagli Host dedicati che sono stati condivisi con loro. Allo stesso modo, le istanze che i consumatori avviano sugli Host dedicati condivisi non vengono conteggiate ai fini dei loro limiti di istanze.

Ripristino host e condivisione di Host dedicato

Il ripristino host recupera le istanze avviate dal proprietario dell'Host dedicato e dai consumatori con cui è stato condiviso. L'Host dedicato sostitutivo viene allocato all'account del proprietario. Viene aggiunto alle stesse condivisioni di risorse dell'Host dedicato originale e viene condiviso con gli stessi consumatori.

Per ulteriori informazioni, consulta Ripristino dell'host dedicato Amazon EC2.

Condividi un host dedicato Amazon EC2 tra più account AWS

Quando un proprietario condivide un Host dedicato, consente ai consumatori di avviare istanze sull'host. I consumatori possono avviare sull'host condiviso il numero di istanze consentito dalla capacità disponibile.

> **Important**
>
> L'utente deve assicurarsi di disporre dei diritti di licenza appropriati per condividere qualsiasi licenza BYOL sugli Host dedicati.

Se condividi un Host dedicato con il posizionamento automatico abilitato, tieni presente quanto segue perché potrebbe portare a un utilizzo indesiderato di Host dedicato:

- Se i consumatori avviano istanze con tenancy Host dedicato e non hanno capacità su un Host dedicato che possiedono nel loro account, l'istanza viene avviata automaticamente sull'Host dedicato condiviso.

Per condividere un Host dedicato, devi aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che ti consente di condividere le tue risorse tra AWS account. Un condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise. Puoi aggiungere l'Host dedicato a una risorsa esistente oppure a una nuova condivisione di risorse.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso all'host dedicato condiviso. In caso contrario, i consumatori ricevono l'invito a partecipare alla condivisione di risorse e, dopo averlo accettato, ottengono l'accesso all'Host dedicato condiviso.

> **Note**
>
> Dopo la condivisione di un Host dedicato, possono essere necessari alcuni minuti perché i consumatori possano accedervi.

È possibile condividere una proprietà Host dedicato utilizzando uno dei metodi descritti di seguito.

Amazon EC2 console

Per condividere un Host dedicato di cui sei proprietario tramite la console Amazon EC2

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Scegliere Host dedicato per condividere e scegliere Azioni, Condividi prenotazione.

4. Selezionare la condivisione di risorse a cui aggiungere Host dedicato e scegliere Condividi host.

   Prima dell'accesso all'host condiviso possono essere necessari alcuni minuti.

AWS RAM console

Per condividere un host dedicato di tua proprietà utilizzando la AWS RAM console

Consulta Creazione di una condivisione di risorse in Guida per l'utente di AWS RAM .

AWS CLI

Per condividere un host dedicato di tua proprietà utilizzando il AWS CLI

Utilizza il comando create-resource-share.

Annulla la condivisione di un host dedicato condiviso con altri account AWS

Il proprietario dell'Host dedicato può annullare la condivisione di un Host dedicato condiviso in qualsiasi momento. Quando annulli la condivisione di un Host dedicato condiviso, si applicano le regole seguenti:

- I consumatori con cui l'Host dedicato è stato condiviso non possono più avviare nuove istanze su di esso.
- Le istanze di proprietà dei consumatori che erano in esecuzione sull'Host dedicato al momento dell'annullamento della condivisione continuano a essere eseguite ma sono destinate al ritiro. I consumatori ricevono notifiche di ritiro per le istanze e hanno due settimane di tempo per intervenire. Se però l'Host dedicato viene condiviso nuovamente con il consumatore entro il termine di preavviso del ritiro, i ritiri delle istanze vengono annullati.

Per annullare la condivisione di un Host dedicato condiviso di cui sei proprietario, devi rimuoverlo dalla condivisione di risorse. Puoi farlo usando i seguenti metodi:

Amazon EC2 console

Per annullare la condivisione di un Host dedicato condiviso di cui sei proprietario utilizzando la console Amazon EC2

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Scegliere la Host dedicato per la quale annullare la condivisione e scegliere la scheda Condivisione.
4. La scheda Condivisione elenca le condivisioni di risorse a cui Host dedicato è stato aggiunto. Selezionare la condivisione di risorse da cui eliminare Host dedicato e selezionare Elimina dalla condivisione di risorse.

AWS RAM console

Come annullare la condivisione di un Host dedicato condiviso di cui sei proprietario tramite la console AWS RAM

Consulta Aggiornamento di una condivisione di risorse in Guida per l'utente di AWS RAM .

Command line

Per annullare la condivisione di un Host dedicato condiviso di tua proprietà utilizzando il AWS CLI

Utilizza il comando disassociate-resource-share.

Visualizza gli host dedicati Amazon EC2 condivisi nel tuo account AWS

Puoi visualizzare l'Host dedicato che condividi con altri account e gli Host dedicati che sono condivisi con te. Se possiedi l'host dedicato, puoi vedere tutte le istanze in esecuzione sull'host, comprese le istanze lanciate dai consumatori. Se l'host dedicato è condiviso con te, puoi vedere solo le istanze che hai lanciato sull'host condiviso e non quelle lanciate da altri consumatori.

Proprietari e consumatori possono identificare Host dedicati condivise utilizzando uno dei seguenti metodi.

Amazon EC2 console

Per identificare un Host dedicato condiviso tramite la console Amazon EC2

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati). La schermata elenca gli Host dedicati di cui sei proprietario e gli Host dedicati che sono condivisi con te. Nella colonna Owner (Proprietario) è indicato l'ID dell'account AWS del proprietario dell'Host dedicato. Per visualizzare le istanze in esecuzione sugli host, seleziona la scheda Istanze.

Command line

Per identificare un host dedicato condiviso utilizzando il AWS CLI

Usa il comando describe-hosts. Il comando restituisce gli Host dedicati di cui sei proprietario e gli Host dedicati che sono condivisi con te.

Host dedicati Amazon EC2 su AWS Outposts

AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura, i servizi, le API e gli strumenti alle vostre sedi. Fornendo l'accesso locale all'infrastruttura AWS gestita, AWS Outposts consente di creare ed eseguire applicazioni in locale utilizzando le stesse interfacce di programmazione AWS delle regioni, utilizzando al contempo risorse di elaborazione e archiviazione locali per esigenze di elaborazione e dati locali a bassa latenza.

Un Outpost è un pool di capacità di AWS elaborazione e archiviazione distribuito presso la sede di un cliente. AWS gestisce, monitora e gestisce questa capacità come parte di una regione. AWS

Puoi allocare host dedicati sugli outpost che hai nel tuo account. In questo modo è più facile portare le licenze software e i carichi di lavoro esistenti che richiedono un server fisico dedicato su AWS Outposts. Puoi anche indirizzare risorse hardware specifiche su un Outpost per ridurre al minimo la latenza tra i tuoi carichi di lavoro.

Gli host dedicati consentono di utilizzare le licenze software idonee su Amazon EC2, in modo da ottenere la flessibilità e l'efficacia in termini di costi dell'utilizzo delle proprie licenze. Anche altre licenze software associate a macchine virtuali, socket o core fisici possono essere utilizzate su host dedicati, in base alle condizioni di licenza. Sebbene gli outpost siano sempre stati ambienti single-tenant idonei per i carichi di lavoro BYOL, gli host dedicati consentono di limitare le licenze necessarie a un singolo host anziché all'intera implementazione degli outpost.

Inoltre, l'utilizzo di host dedicati su un outpost offre una maggiore flessibilità nella distribuzione del tipo di istanza e un controllo più granulare sul posizionamento delle istanze. Si può puntare a un host specifico per il lancio di un'istanza e usare l'affinità di host per garantire che l'istanza venga sempre eseguita su quell'host, oppure si può usare il posizionamento automatico per lanciare un'istanza su qualsiasi host disponibile che abbia configurazioni corrispondenti e capacità disponibile.

Indice

- Considerazioni
- Alloca un host dedicato Amazon EC2 su AWS Outposts

Prerequisiti

Devi avere un Outpost installato nel tuo sito. Per ulteriori informazioni, consulta Creazione di un Outpost e ordinazione della capacità Outpost nella Guida per l'utente di AWS Outposts .

Funzionalità supportate

- Sono supportate le seguenti famiglie di istanze: `C5`, `M5`, `R5`, `C5d`, `M5d`, `R5d`, `G4dn` e `i3en`.
- Gli host dedicati sugli outpost possono essere configurati per supportare più dimensioni di istanza. Il supporto per più dimensioni di istanza è disponibile per le seguenti famiglie di istanze: `C5`, `M5`, `R5`, `C5d`, `M5d` e `R5d`. Per ulteriori informazioni, consulta Configurazioni della capacità delle istanze di Amazon EC2 Dedicated Host.
- Gli host dedicati sugli outpost supportano il posizionamento automatico e il lancio di istanze mirate. Per ulteriori informazioni, consulta Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host.
- Gli host dedicati sugli outpost supportano l'affinità degli host. Per ulteriori informazioni, consulta Posizionamento automatico dell'host dedicato Amazon EC2 e affinità degli host.
- Gli host dedicati su Outposts supportano la condivisione con. AWS RAM Per ulteriori informazioni, consulta Condivisione di host dedicati Amazon EC2 su più account.

Considerazioni

- Le prenotazioni di host dedicati non sono supportate sugli outpost.
- Ospitano gruppi di risorse e non AWS License Manager sono supportati su Outposts.
- Gli host dedicati sugli outpost non supportano istanze T3 espandibili.
- Gli host dedicati sugli outpost non supportano il ripristino dell'host.
- Il ripristino automatico semplificato non è supportato per le istanze con tenancy Host dedicato su Outposts.

Alloca un host dedicato Amazon EC2 su AWS Outposts

Puoi allocare e utilizzare gli host dedicati sugli outpost nello stesso modo in cui faresti con gli host dedicati in una regione AWS .

Prerequisiti

Creare una sottorete nell'Outpost. Per ulteriori informazioni, consulta Creazione di una sottorete nella Guida per l'utente di AWS Outposts .

Per allocare un host dedicato su un Outpost, utilizza uno dei metodi descritti di seguito:

AWS Outposts console

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Nel riquadro di navigazione, scegli Outpost. Seleziona l'outpost e scegli Actions (Operazioni), Allocate Dedicated Host (Alloca host dedicato).
3. Configura l'host dedicato secondo necessità. Per ulteriori informazioni, consulta Assegna un host dedicato Amazon EC2 da utilizzare nel tuo account.

   > **Note**
   >
   > I campi Availability Zone (Zona di disponibilità) e Outpost ARN (ARN dell'Outpost) dovrebbero essere precompilati con la zona di disponibilità e l'ARN dell'Outpost selezionato.

4. Scegli Alloca.

Amazon EC2 console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Dedicated Hosts (Host dedicati), quindi Allocate Dedicated Host (Alloca host dedicato).
3. In Availability Zone (Zona di disponibilità), seleziona la zona di disponibilità associata all'Outpost.
4. In Outpost ARN (ARN dell'Outpost), inserisci l'ARN dell'Outpost.
5. Per scegliere come target risorse hardware specifiche sull'Outpost, per Scegli risorse hardware specifiche sull'Outpost seleziona Abilita. Per ogni risorsa hardware da utilizzare come target, scegli Aggiungi ID risorsa, quindi inserisci l'ID della risorsa hardware.

> **Note**
>
> Il valore specificato per Quantità deve essere uguale al numero di ID degli asset specificati. Ad esempio, se specifichi 3 ID di asset, anche Quantità deve essere 3.

6. Configura le impostazioni rimanenti dell'host dedicato secondo necessità. Per ulteriori informazioni, consulta Assegna un host dedicato Amazon EC2 da utilizzare nel tuo account.
7. Scegli Alloca.

AWS CLI

Utilizzate il comando allocate-hosts AWS CLI . In `--availability-zone`, specifica la zona di disponibilità associata all'Outpost. In `--outpost-arn`, specifica l'ARN dell'Outpost. Facoltativamente, per `--asset-ids`, specifica gli ID delle risorse hardware dell'Outpost da scegliere come target.

```
aws ec2 allocate-hosts --availability-zone "us-east-1a" --outpost-arn
 "arn:aws:outposts:us-east-1a:111122223333:outpost/op-4fe3dc21baEXAMPLE" --asset-
ids asset_id --instance-family "m5" --auto-placement "off" --quantity 1
```

Per avviare un'istanza su un host dedicato su un Outpost

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati). Seleziona l'host dedicato che hai allocato nel passaggio precedente e scegli Actions (Operazioni), Launch instance onto host (Avvia l'istanza sull'host).
3. Configura l'istanza secondo necessità e quindi avvia l'istanza. Per ulteriori informazioni, consulta Avvia istanze Amazon EC2 su un host dedicato Amazon EC2.

Ripristino dell'host dedicato Amazon EC2

Il ripristino automatico dell'host dedicato riavvia le istanze su un nuovo host sostitutivo, se sull'host dedicato vengono rilevate delle condizioni problematiche. Il ripristino host riduce la necessità di intervento manuale e il carico operativo in caso di errore imprevisto dell'host dedicato relativamente a eventi di sistema o connettività di rete. Altri problemi relativi all'host dedicato richiederanno un intervento manuale da cui eseguire il ripristino.

Indice

Come funziona l'host dedicato Amazon EC2

Gli host dedicati e il processo di recupero dei gruppi di risorse host utilizzano i controlli dell'integrità a livello di host per valutare la disponibilità degli host dedicati e per rilevare errori di sistema sottostanti. Il tipo di errore dell'host dedicato determina se è possibile il ripristino automatico dell'host dedicato. Esempi di problemi che causano il mancato superamento dei controlli dello stato di integrità a livello di host includono:

- Perdita di connettività di rete
- Perdita di alimentazione elettrica del sistema
- Problemi hardware e software sull'host fisico

> **Important**
>
> Il ripristino automatico dell'host dedicato non si verifica quando l'host è programmato per il ritiro.

Ripristino automatico dell'host dedicato

Quando viene rilevato un guasto all'alimentazione del sistema o alla connettività di rete sull'host dedicato, viene avviato il ripristino automatico dell'host dedicato e Amazon EC2 alloca automaticamente un host dedicato sostitutivo nella stessa zona di disponibilità dell'host dedicato originale. L'Host dedicato sostitutivo riceve un nuovo ID host ma mantiene gli stessi attributi dell'Host dedicato originale, inclusi:

- Zona di disponibilità
- Tipo di istanza
- Tag
- Impostazioni di posizionamento automatico
- Prenotazione

Una volta allocato l'host dedicato sostitutivo, su tale host vengono ripristinate le istanze. Le istanze ripristinate mantengono gli stessi attributi delle istanze originali, inclusi:

- ID istanza
- Indirizzi IP privati
- Indirizzi IP elastici
- Allegati dei volumi EBS
- Tutti i metadati delle istanze

Inoltre, l'integrazione integrata con AWS License Manager automatizza il monitoraggio e la gestione delle licenze.

> **Note**
>
> AWS L'integrazione con License Manager è supportata solo nelle regioni in cui è disponibile AWS License Manager.

Se le istanze hanno una relazione di affinità host con l'Host dedicato danneggiato, le istanze ripristinate stabiliscono un'affinità host con l'Host dedicato sostitutivo.

Una volta che tutte le istanze sono state ripristinate sull'Host dedicato sostitutivo, l'Host dedicato danneggiato viene rilasciato e l'Host dedicato sostitutivo diventa disponibile per l'utilizzo.

Quando viene avviato il ripristino dell'host, il proprietario AWS dell'account riceve una notifica via e-mail e tramite un AWS Health Dashboard evento. Al completamento del ripristino viene dell'host inviata una seconda notifica.

Se si utilizza AWS License Manager per tenere traccia delle licenze, AWS License Manager alloca nuove licenze per l'Host dedicato sostitutivo in base ai limiti di configurazione della licenza. Se la configurazione della licenza prevede limiti rigidi che verranno violati a seguito del ripristino dell'host, il

processo di ripristino non è consentito e riceverai una notifica dell'errore di ripristino dell'host tramite una notifica Amazon SNS (se le impostazioni di notifica sono state configurate per License AWS Manager). Se la configurazione delle licenze presenta limiti software che verranno superati come conseguenza del ripristino host, il ripristino viene consentito e ricevi una notifica Amazon SNS relativa al superamento del limite. Per ulteriori informazioni, consultare Utilizzo delle configurazioni di licenza e Impostazioni in License Manager nella Guida per l'utente di AWS License Manager.

Stati del ripristino host

Quando viene rilevato un errore dell'Host dedicato, sull'Host dedicato danneggiato viene attivato lo stato `under-assessment` e su tutte le istanze viene attivato lo stato `impaired`. Non è possibile avviare istanze sull'Host dedicato danneggiato mentre si trova nello stato `under-assessment`.

Una volta allocato, sull'Host dedicato sostitutivo viene attivato lo stato `pending`. L'host rimane in questo stato fino al completamento del processo di ripristino host. Non è possibile avviare istanze sull'Host dedicato sostitutivo mentre si trova nello stato `pending`. Le istanze ripristinate sull'Host dedicato sostitutivo rimangono nello stato `impaired` durante il processo di ripristino.

Una volta completato il ripristino host, sull'Host dedicato sostitutivo viene attivato lo stato `available`e le istanze ripristinate tornato allo stato `running`. È possibile avviare istanze sull'Host dedicato sostitutivo dopo che è stato attivato lo stato `available`. L'Host dedicato danneggiato originale viene rilasciato definitivamente e viene attivato lo stato `released-permanent-failure`.

Se l'Host dedicato compromesso presenta istanze che non supportano il ripristino host, ad esempio le istanze con volumi supportati da instance store, l'Host dedicato non viene rilasciato. Viene invece contrassegnato per il ritiro e viene attivato lo stato `permanent-failure`.

Scenari senza il ripristino automatico dell'host dedicato

Il ripristino automatico dell'host dedicato non si verifica quando l'host è programmato per il ritiro. Riceverai una notifica di ritiro in occasione di un CloudWatch evento Amazon e l'indirizzo e-mail del proprietario dell' AWS account riceverà un messaggio relativo all'errore dell'host dedicato. AWS Health Dashboard Segui le procedure di correzione descritte nella notifica di ritiro entro il periodo di tempo specificato per ripristinare manualmente le istanze sull'host che desideri ritirare.

Le istanze arrestate non vengono ripristinate sull'Host dedicato sostitutivo. Se si prova ad avviare un'istanza arrestata destinata all'Host dedicato danneggiato, l'avvio non riesce. Consigliamo di modificare l'istanza arrestata specificando un Host dedicato di destinazione diverso oppure di avviarla su un Host dedicato disponibile con configurazioni corrispondenti abilitato per il posizionamento automatico.

Le istanze con archiviazione dell'istanza non vengono ripristinate sull'Host dedicato sostitutivo. Come misura di correzione, l'Host dedicato danneggiato viene contrassegnato per il ritiro e riceverai una notifica di ritiro una volta completato il ripristino host. Segui le procedure di correzione descritte nella notifica di ritiro entro il periodo di tempo specificato per ripristinare manualmente le istanze rimanenti sull'Host dedicato danneggiato.

Tipi di istanze supportati

Il ripristino dell'host è supportato per le seguenti famiglie di istanze: A1, C3, C4, C5, C5n, C6a, C6g, C6i, Inf1, G3, G5g, M3, M4, M5, M5n, M5zn, M6a, M6g, M6i, P2, P3, R3, R4, R5, R5b, R5n, R6g, R6i, T3, X1, X1e, X2ieZn, u-6tb1, u-9tb1, u-12tb1, u-18tb1 e u-24tb1.

Per ripristinare le istanze non supportate, consulta Ripristina manualmente le istanze che non sono supportate dal ripristino dell'host dedicato di Amazon EC2.

> **Note**
>
> Il ripristino automatico dell'host dedicato dei tipi di istanza metal supportati richiederà più tempo per rilevare e ripristinare i tipi di istanze non metal.

Prezzi

L'uso del ripristino host non prevede costi aggiuntivi, solo i normali costi dell'Host dedicato. Per maggiori informazioni, consulta Prezzi degli host dedicati di Amazon EC2.

Appena viene avviato il ripristino host, non riceverai più l'addebito per l'Host dedicato danneggiato. La fatturazione per l'host dedicato sostitutivo inizia solo dopo che viene attivato lo stato `available`.

Se l'addebito dell'Host dedicato danneggiato è stato effettuato in base alla tariffa on demand, questo criterio viene seguito anche per l'addebito dell'Host dedicato sostitutivo. Se l'Host dedicato danneggiato presenta un Prenotazioni di host dedicati attivo, questo viene trasferito nell'Host dedicato sostitutivo.

Abilita il ripristino dell'host dedicato Amazon EC2

È possibile abilitare il ripristino host in fase di allocazione dell'Host dedicato oppure successivamente.

Per ulteriori informazioni sull'abilitazione del ripristino host in fase di allocazione dell'Host dedicato, consulta Assegna un host dedicato Amazon EC2 da utilizzare nel tuo account.

Per abilitare il ripristino host dopo l'allocazione mediante la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Selezionare l'Host dedicato per cui abilitare il ripristino host, quindi scegliere Operazioni, Modify Host Recovery (Modifica ripristino host).
4. Per Host recovery (Ripristino host), scegliere Attiva, quindi Salva.

Per abilitare il ripristino dell'host dopo l'allocazione utilizzando AWS CLI

Utilizzare il comando modify-hosts e specificare il parametro `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery on --host-ids h-012a3456b7890cdef
```

Disattiva il ripristino dell'host dedicato Amazon EC2

È possibile disabilitare il ripristino host in qualsiasi momento dopo che l'Host dedicato è stato allocato.

Per disabilitare il ripristino host dopo l'allocazione mediante la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Selezionare l'Host dedicato per cui disabilitare il ripristino host, quindi scegliere Operazioni, Modify Host Recovery (Modifica ripristino host).
4. Per Host recovery (Ripristino host), scegliere Disattiva, quindi Salva.

Per disabilitare il ripristino dell'host dopo l'allocazione utilizzando AWS CLI

Utilizzare il comando modify-hosts e specificare il parametro `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery off --host-ids h-012a3456b7890cdef
```

Visualizza le impostazioni di ripristino dell'host per il tuo host dedicato Amazon EC2

È possibile visualizzare la configurazione del ripristino host per un Host dedicato in qualsiasi momento.

Per visualizzare la configurazione del ripristino host per un Host dedicato mediante la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Selezionare l'Host dedicato, quindi nella scheda Descrizione rivedere il campo Host Recovery (Ripristino host).

Come visualizzare la configurazione del ripristino host per un Host dedicato mediante la AWS CLI

Usa il comando describe-hosts.

```
$ aws ec2 describe-hosts --host-ids h-012a3456b7890cdef
```

L'elemento di risposta `HostRecovery` indica se il ripristino host è abilitato o disabilitato.

Ripristina manualmente le istanze che non sono supportate dal ripristino dell'host dedicato di Amazon EC2

Il ripristino host non supporta il ripristino delle istanze che utilizzano volumi di instance store. Segui le istruzioni riportate di seguito per ripristinare manualmente le istanze che potrebbero non essere ripristinate automaticamente.

> **Warning**
>
> Quando un'istanza viene arrestata, ibernata o terminata, i dati nei volumi di instance store vengono persi. Sono inclusi i volumi instance store collegati a un'istanza che ha un volume EBS come dispositivo root. Per proteggere i dati dei volumi di instance store, è opportuno creare una copia di backup nello archiviazione persistente prima che l'istanza venga arrestata o terminata.

Ripristino manuale delle istanze supportate da EBS

Per le istanze supportate da EBS che potrebbero non essere ripristinate automaticamente, consigliamo di arrestare e avviare manualmente le istanze per ripristinarle in un nuovo Host dedicato. Per ulteriori informazioni sull'arresto dell'istanza e sulle modifiche alla configurazione dell'istanza quando viene arrestata, consulta Arresta e avvia le istanze Amazon EC2.

Ripristino manuale delle istanze supportate da instance store

Per le istanze supportate da instance store che potrebbero non essere ripristinate automaticamente, consigliamo di effettuare quanto segue:

1. Avviare un'istanza sostitutiva su un nuovo Host dedicato dall'AMI più recente.
2. Migrare tutti i dati necessari nell'istanza sostituiva.
3. Terminare l'istanza originale nell'Host dedicato danneggiato.

Manutenzione dell'host per l'host dedicato Amazon EC2

Con la manutenzione dell'host, le istanze Amazon EC2 sull'host dedicato danneggiato vengono riavviate automaticamente su un host dedicato sostitutivo durante un evento di manutenzione programmata. Ciò aiuta a ridurre i tempi di inattività delle applicazioni e a scaricare su AWS il carico indifferenziato della manutenzione. La manutenzione degli host viene eseguita anche per la manutenzione pianificata e ordinaria di Amazon EC2.

La manutenzione degli host è supportata su tutte le nuove allocazioni di host dedicati effettuate tramite la console Amazon EC2. Per qualsiasi host dedicato presente nel tuo sistema Account AWS o per qualsiasi nuovo host dedicato allocato tramite AllocateHosts API, puoi configurare la manutenzione dell'host per gli host dedicati supportati. Per ulteriori informazioni, consulta the section called “Configura la manutenzione dell'host”.

Indice

Confronto tra manutenzione degli host e ripristino degli host

Nella tabella seguente vengono illustrate le differenze principali tra il ripristino degli host e la manutenzione degli host.

	Ripristino host	Manutenzione degli host
Accessibilità	Irraggiungibile	Raggiungibile
Stato	`under-assessment`	`permanent-failure`
Azione	Il ripristino è immediato	La manutenzione è programmata
Flessibilità di pianificazione	Non può essere riprogram mata	Non può essere riprogram mata
Gruppi di risorse host	Supportato	Non supportato

Per ulteriori informazioni sul ripristino degli host, consulta Ripristino degli host.

Tipi di istanze supportati

La manutenzione dell'host è supportata per le seguenti famiglie di istanze:

- Uso generico: `A1` | `M4` | `M5` | `M5a` | `M5n` | `M5zn` | `M6a` | `M6g` | `M6i` | `M6in` | `M7a` | `M7g` | `M7i` | `T3`
- Calcolo ottimizzato: `C4` | `C5` | `C5a` | `C5n` | `C6a` | `C6g` | `C6gn` | `C6i` | `C6in` | `C7g` | `C7gn` | `C7i`
- Ottimizzate per la memoria: `R4` | `R5` | `R5a` | `R5b` | `R5n` | `R6a` | `R6g` | `R6i` | `R6in` | `R7a` | `R7g` | `R7iz` | `u-12tb1` | `u-18tb1` | `u-24tb1` | `u-3tb1` | `u-6tb1` | `u-9tb1` | `X2iezn`
- Elaborazione accelerata: `G3` | `G5g` | `Inf1` | `P2` | `P3`

Limitazioni

- La manutenzione dell'host non è supportata in AWS Outposts, AWS Local Zones e AWS Wavelength Zones.
- La manutenzione degli host non può essere attivata o disattivata per gli host già inclusi in un gruppo di risorse host. Gli host aggiunti a un gruppo di risorse host mantengono le impostazioni di manutenzione degli host. Per ulteriori informazioni, consulta Gruppi di risorse host.
- La manutenzione degli host è supportata solo su tipi di istanze specifici. Per ulteriori informazioni, consulta the section called “Tipi di istanze supportati”.

Servizi correlati

Dedicated Host si integra con AWS License Manager: tiene traccia delle licenze negli host dedicati Amazon EC2 (supportato solo nelle regioni in cui è disponibile License Manager AWS). Per ulteriori informazioni, consultare la Guida per l'utente di AWS License Manager.

È necessario disporre di licenze sufficienti Account AWS per il nuovo host dedicato. Le licenze associate all'host degradato vengono rilasciate quando l'host viene rilasciato dopo il completamento dell'evento di manutenzione programmata.

Prezzi

L'uso della manutenzione degli host non prevede costi aggiuntivi, solo i normali costi dell'host dedicato. Per maggiori informazioni, consulta Prezzi degli host dedicati di Amazon EC2.

Appena viene avviata la manutenzione degli host, non riceverai più l'addebito per l'host dedicato degradato. La fatturazione per l'host dedicato sostitutivo inizia solo dopo che viene attivato lo stato `available`.

Se l'host dedicato danneggiato è stato fatturato utilizzando la tariffa on demand, anche l'host dedicato sostitutivo viene fatturato utilizzando la tariffa on demand. Se l'host dedicato degradato presenta una Prenotazione di host dedicati attiva, questo viene trasferito nel nuovo host dedicato.

Come funziona la manutenzione degli host per gli host dedicati Amazon EC2

Quando viene rilevato un degrado su un host dedicato, viene allocato un nuovo host dedicato. Il degrado può essere causato dal degrado dell'hardware sottostante o dal rilevamento di determinate condizioni problematiche. Le istanze sull'host dedicato danneggiato sono programmate per essere riavviate automaticamente sull'host dedicato sostitutivo.

L'host dedicato sostitutivo riceve un nuovo ID host ma mantiene gli stessi attributi dell'host dedicato originale. Questi attributi includono quanto segue.

- Impostazioni di posizionamento automatico
- Zona di disponibilità
- Prenotazione
- Affinità host
- Impostazioni di manutenzione degli host

- Impostazioni del ripristino degli host
- Tipo di istanza
- Tag

La manutenzione dell'host è disponibile in tutto Regioni AWS per tutti gli host dedicati supportati. Per ulteriori informazioni sugli host dedicati in cui la manutenzione degli host non è supportata, consulta the section called “Limitazioni”.

L'host dedicato degradato viene rilasciato dopo che tutte le istanze sono state riavviate su un nuovo host dedicato o interrotte. È possibile accedere alle istanze sull'host dedicato degradato prima dell'evento di manutenzione programmata, ma l'avvio di istanze sull'host dedicato degradato non è supportato.

È possibile utilizzare l'host dedicato sostitutivo per avviare nuove istanze sull'host prima dell'evento di manutenzione programmato. Tuttavia, una parte della capacità delle istanze sull'host sostitutivo è riservata alle istanze che devono essere migrate dall'host danneggiato. Non è possibile avviare nuove istanze in questa capacità riservata. Per ulteriori informazioni, consulta the section called “Istanze su host dedicati”.

Istanze su host dedicati

Amazon EC2 riserva automaticamente la capacità sull'host sostitutivo per le istanze che verranno migrate automaticamente dall'host danneggiato. Amazon EC2 non riserva la capacità sull'host sostitutivo per le istanze che non possono essere migrate automaticamente, ad esempio le istanze con volumi root dell'instance store. La capacità riservata non può essere utilizzata per avviare nuove istanze.

> **Note**
>
> La console Amazon EC2 mostra la capacità riservata come capacità utilizzata. Potrebbe sembrare che le istanze siano in esecuzione sia sull'host danneggiato che sull'host sostitutivo. Tuttavia, le istanze continueranno a funzionare solo sull'host danneggiato fino all'arresto o alla migrazione nella capacità riservata dell'host sostitutivo.

Se si arresta manualmente un'istanza sull'host danneggiato che può essere migrata automaticamente, la capacità riservata per quell'istanza sull'host sostitutivo viene rilasciata e diventa disponibile per l'uso.

Durante l'evento di manutenzione programmata, le istanze sull'host danneggiato vengono riavviate e migrate nella capacità riservata dell'host dedicato sostitutivo. Le istanze migrate mantengono gli stessi attributi di quelle sull'host danneggiato, inclusi i seguenti.

- Allegati dei volumi Amazon EBS
- Indirizzi IP elastici
- ID istanza
- Metadati delle istanze
- Indirizzo IP privato

È possibile interrompere e avviare un'istanza sull'host degradato in qualsiasi momento prima che venga avviato l'evento di manutenzione programmata. In questo modo, l'istanza viene riavviata su un altro host e non verrà sottoposta a manutenzione programmata. È necessario aggiornare l'affinità dell'host dell'istanza al nuovo host su cui si desidera riavviare l'istanza. Se si interrompono tutte le istanze sull'host danneggiato prima dell'inizio dell'evento di manutenzione, l'host danneggiato viene rilasciato e l'evento di manutenzione viene annullato. Per ulteriori informazioni, consulta Arresta e avvia le istanze Amazon EC2.

> **Note**
>
> I dati su qualsiasi volume dell'archivio locale non vengono conservati quando l'istanza viene arrestata e avviata.

Le istanze con un volume dell'archivio dell'istanza come dispositivo root vengono terminate dopo la data di terminazione specificata. Tutti i dati nei volumi dell'archivio dell'istanza vengono eliminati quando le istanze vengono terminate. Le istanze terminate vengono eliminate definitivamente e non possono essere riavviate. Per le istanze con volumi dell'archivio dell'istanza come dispositivo root, consigliamo di avviare istanze sostitutive su un host dedicato diverso utilizzando l'Amazon Machine Image più recente e di migrare tutti i dati disponibili nelle istanze sostitutive prima della data di terminazione specificata. Per ulteriori informazioni, consulta Azioni da intraprendere, ad esempio il ritiro.

Le istanze che non possono essere riavviate automaticamente vengono interrotte dopo la data specificata. È possibile avviare nuovamente queste istanze su un host diverso. Le istanze che utilizzano un volume Amazon EBS come dispositivo root continuano a utilizzare lo stesso volume Amazon EBS dopo essere state avviate su un nuovo host.

È possibile impostare l'ordine di riavvio dell'istanza riprogrammando l'ora di inizio del riavvio di un'istanza in https://console.aws.amazon.com/ec2/.

Evento di manutenzione

Al rilevamento del degrado, viene programmato un evento di manutenzione 14 giorni dopo, per riavviare le istanze su un nuovo host dedicato. Riceverai una notifica via e-mail con dettagli sull'host degradato, sull'evento di manutenzione programmato e sugli intervalli di tempo di manutenzione. Per ulteriori informazioni, consulta Visualizzazione degli eventi pianificati.

È possibile ripianificare l'evento di manutenzione per qualsiasi giorno fino a sette giorni dopo la data dell'evento pianificato. Per ulteriori informazioni sulla ripianificazione, consulta Ripianificare un evento pianificato.

Per il completamento dell'evento di manutenzione in genere sono necessari alcuni minuti. Nel raro caso in cui l'evento non vada a buon fine, riceverai una notifica via e-mail per espellere le istanze sull'host degradato entro un determinato periodo di tempo.

Stati di manutenzione degli host

Quando viene rilevato un degrado, l'host dedicato viene impostato su `permanent-failure`. Non è possibile avviare istanze su un host dedicato nello stato `permanent-failure`. Al termine dell'evento di manutenzione, l'host degradato viene rilasciato e messo nello stato `released, permanent-failure`.

Dopo aver rilevato un deterioramento su un host dedicato e prima di pianificare un evento di manutenzione, la manutenzione dell'host assegna automaticamente un host dedicato sostitutivo al tuo account. Questo host sostitutivo rimane in `pending` uno stato fino alla pianificazione di un evento di manutenzione. Dopo la pianificazione dell'evento di manutenzione, l'host dedicato sostitutivo si trasferisce nello `available` stato.

È possibile utilizzare l'host dedicato sostitutivo per avviare nuove istanze sull'host prima dell'evento di manutenzione pianificato. Tuttavia, una parte della capacità delle istanze sull'host sostitutivo è riservata alle istanze che devono essere migrate dall'host danneggiato. Non è possibile avviare nuove istanze in questa capacità riservata. Per ulteriori informazioni, consulta the section called “Istanze su host dedicati”.

Configurare l'impostazione di manutenzione dell'host per un host dedicato Amazon EC2

È possibile configurare la manutenzione dell'host per tutti gli host dedicati supportati tramite AWS Management Console o AWS CLI. Per ulteriori dettagli, consulta la tabella seguente.

AWS Management Console

Per abilitare la manutenzione dell'host per il tuo host dedicato utilizzando AWS Management Console.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Seleziona l'host dedicato > Operazioni > Modifica host.
4. Seleziona attiva nel campo Manutenzione dell'host.

Per disabilitare la manutenzione dell'host utilizzato dall'host dedicato tramite la AWS Management Console.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Seleziona l'host dedicato > Operazioni > Modifica host.
4. Seleziona disattiva nel campo Manutenzione dell'host.

Per visualizzare la configurazione del ripristino host per un Host dedicato mediante la AWS Management Console.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Seleziona l'host dedicato, quindi nella scheda Descrizione rivedi il campo Manutenzione host.

AWS CLI

Per abilitare o disabilitare la manutenzione dell'host utilizzato dal nuovo host dedicato durante l'allocazione tramite la AWS CLI.

Utilizza il comando allocate-hosts.

Attiva

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance on
```

Disabilita

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance off
```

Per abilitare o disabilitare la manutenzione dell'host utilizzato dall'host dedicato esistente tramite la AWS CLI.

Utilizza il comando modify-hosts.

Attiva

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance on --host-
ids h-0d123456bbf78910d
```

Disabilita

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance off --host-
ids h-0d123456bbf78910d
```

Per visualizzare la configurazione del ripristino host per un Host dedicato mediante la AWS CLI.

Usa il comando describe-hosts.

```
aws ec2 describe-hosts --region us-east-1 --host-ids h-0d123456bbf78910d
```

> **Note**
>
> Se disabiliti la manutenzione dell'host, ricevi una notifica e-mail per espellere l'host danneggiato e migrare manualmente le istanze su un altro host entro 28 giorni. Se hai prenotato un host dedicato, viene assegnato un host sostitutivo. Dopo 28 giorni, le istanze in esecuzione sull'host danneggiato vengono terminate e l'host viene rilasciato automaticamente.

Monitora lo stato dei tuoi host dedicati Amazon EC2

Amazon EC2 monitora costantemente lo stato degli Host dedicati. Gli aggiornamenti vengono comunicati sulla console Amazon EC2. È possibile visualizzare le informazioni su un Host dedicato utilizzando i seguenti metodi.

Console

Per visualizzare lo stato di un Host dedicato

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Individuare l'Host dedicato nell'elenco e controllare il relativo valore nella colonna State (Stato).

AWS CLI

Per visualizzare lo stato di un Host dedicato

Utilizzate il AWS CLI comando describe-hosts, quindi esaminate la `state` proprietà nell'`hostSet`elemento di risposta.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

Per visualizzare lo stato di un Host dedicato

Utilizzate il Get-EC2Host AWS Tools for Windows PowerShell comando e quindi esaminate la `state` proprietà nell'elemento di risposta. `hostSet`

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

Nella seguente tabella sono descritti i possibili stati di un Host dedicato.

Stato	Descrizione
`available`	AWS non ha rilevato alcun problema con l'host dedicato. Non è stata pianificata alcuna manutenzione né correzione. Le istanze possono essere avviate su questo host dedicato.
`released`	L'Host dedicato è stato rilasciato. L'ID host non è più in uso. Gli host rilasciati non possono essere riutilizzati.
`under-assessment`	AWS sta esaminando un possibile problema con l'host dedicato. Se è necessario intraprendere un'azione, riceverai una notifica tramite AWS Management Console o e-mail. Le istanze non possono essere avviate su occorrenze degli Host dedicato in questo stato.
`pending`	L'Host dedicato non può essere utilizzato per nuovi lanci di istanze. A questo scopo, deve essere modificato per supportare più tipi di istanza o deve essere in corso un ripristino host.
`permanent-failure`	È stato rilevato un errore irreversibile. Riceverai una notifica di espulsione tramite le istanze o e-mail. È possibile che l'esecuzione delle istanze continui. Se interrompi o chiudi tutte le istanze su un host dedicato con questo stato, AWS ritira l'host. AWS non riavvia le istanze in questo stato. Le istanze non possono essere avviate su occorrenze degli Host dedicati in questo stato.
`released-permanent-failure`	AWS rilascia permanentemente gli host dedicati che hanno avuto esito negativo e su cui non sono più presenti istanze in esecuzione. L'ID dell'Host dedicato non è più disponibile per l'utilizzo.

Tieni traccia delle modifiche alla configurazione dell'host dedicato di Amazon EC2 utilizzando AWS Config

È possibile utilizzarlo AWS Config per registrare le modifiche alla configurazione per gli host dedicati e per le istanze che vengono avviate, interrotte o terminate su di essi. Puoi quindi utilizzare le informazioni acquisite da AWS Config come origine dati per i report sulle licenze.

AWS Config registra singolarmente le informazioni di configurazione per gli host dedicati e le istanze e associa queste informazioni tramite relazioni. Sono disponibili tre condizioni per la generazione di report:

- AWS Config stato di registrazione: quando AWS Config è attiva, registra uno o più tipi di AWS risorse, che possono includere host dedicati e istanze dedicate. Per acquisire le informazioni richieste per i report sulle licenze, verifica che gli host e le istanze vengano registrate con i seguenti campi.
- Host recording status (Stato registrazione host) — Se questa opzione è impostata su Enabled (Abilitato), vengono registrate le informazioni sulla configurazione delle occorrenze degli Host dedicati.
- Instance recording status (Stato registrazione istanza) — Se questa opzione è impostata su Enabled (Abilitato), vengono registrate le informazioni sulla configurazione delle occorrenze degli Istanze dedicate.

Se una qualsiasi di queste tre condizioni è disabilitata, l'icona del pulsante Edit Config Recording (Modifica la registrazione di Config) è di colore rosso. Per sfruttare tutti i vantaggi di questo strumento assicurati che siano abilitati tutti e tre i metodi di registrazione. Dopo aver abilitato tutti e tre i metodi, l'icona sarà verde. Per modificare le impostazioni, scegli Edit Config Recording (Modifica la registrazione di Config). Verrai indirizzato alla AWS Config pagina di configurazione della AWS Config console, dove puoi configurare AWS Config e avviare la registrazione per i tuoi host, le istanze e altri tipi di risorse supportati. Per ulteriori informazioni, consulta Configurazione AWS Config tramite la console nella Guida per gli AWS Config sviluppatori.

> **Note**
>
> AWS Config registra le risorse dopo averle scoperte, operazione che potrebbe richiedere alcuni minuti.

Dopo aver AWS Config iniziato a registrare le modifiche alla configurazione degli host e delle istanze, è possibile ottenere la cronologia di configurazione di qualsiasi host allocato o rilasciato e di tutte le istanze avviate, interrotte o terminate. Ad esempio, in qualsiasi punto della cronologia della configurazione di un Host dedicato, puoi controllare il numero di istanze avviate su tale host, nonché il numero di socket e core sull'host. Per qualsiasi istanza puoi inoltre cercare l'ID della relativa Amazon Machine Image (AMI). Puoi utilizzare queste informazioni per generare report sulle licenze per il software collegato a server con licenza per socket o per core.

Puoi visualizzare la cronologia di configurazione in uno dei seguenti modi:

- Utilizzando la console. AWS Config Per ogni risorsa registrata, puoi visualizzare una pagina della timeline, che fornisce una cronologia dei dettagli di configurazione. Per visualizzare questa pagina, scegli l'icona grigia nella colonna Timeline configurazione della pagina Host dedicati. Per ulteriori informazioni, consulta Visualizzazione dei dettagli di configurazione nella AWS Config console nella Guida per gli AWS Config sviluppatori.
- Eseguendo AWS CLI i comandi. Innanzitutto, è possibile utilizzare il list-discovered-resourcescomando per ottenere un elenco di tutti gli host e le istanze. Quindi, puoi utilizzare il get-resource-config-historycomando per ottenere i dettagli di configurazione di un host o di un'istanza per un intervallo di tempo specifico. Per ulteriori informazioni, consulta l'argomento relativo alla visualizzazione dei dettagli di configurazione mediante la CLI nella Guida per lo sviluppatore di AWS Config .
- Utilizzando l' AWS Config API nelle tue applicazioni. Innanzitutto, puoi utilizzare l'ListDiscoveredResourcesazione per ottenere un elenco di tutti gli host e le istanze. Quindi, puoi utilizzare l'GetResourceConfigHistoryazione per ottenere i dettagli di configurazione di un host o di un'istanza per un intervallo di tempo specifico.

Ad esempio, per ottenere un elenco di tutti i tuoi host dedicati da AWS Config, esegui un comando CLI come il seguente.

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Per ottenere la cronologia di configurazione di un host dedicato da AWS Config, esegui un comando CLI come il seguente.

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --
resource-id i-1234567890abcdef0
```

Per gestire AWS Config le impostazioni utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella pagina Host dedicati (Host dedicati) scegliere Edit Config Recording (Modifica la registrazione di Config).
3. Nella AWS Config console, segui i passaggi indicati per attivare la registrazione. Per ulteriori informazioni, consulta Configurazione AWS Config tramite la console.

Per ulteriori informazioni, vedere Visualizzazione dei dettagli di configurazione nella AWS Config console.

Per attivare AWS Config utilizzando la riga di comando o l'API

- AWS CLI: visualizzazione dei dettagli di configurazione (AWS CLI) nella Guida per gli AWS Config sviluppatori.
- API Amazon EC2:. GetResourceConfigHistory

Istanze dedicate Amazon EC2

Per impostazione predefinita, le istanze EC2 vengono eseguite su hardware di tenancy condiviso. Ciò significa che più AWS account potrebbero condividere lo stesso hardware fisico.

Le istanze dedicate sono istanze EC2 eseguite su hardware dedicato a un singolo account. AWS Ciò significa che le istanze dedicate sono fisicamente isolate a livello di hardware host dalle istanze che appartengono ad altri Account AWS, anche se tali account sono collegati a un unico account di pagamento. Tuttavia, le istanze dedicate potrebbero condividere l'hardware con altre istanze delle stesse Account AWS che non sono istanze dedicate.

Le istanze dedicate non forniscono visibilità o controllo sul posizionamento delle istanze e non supportano l'affinità con gli host. Se si arresta e si avvia un'istanza dedicata, è possibile che non venga eseguita sullo stesso host. Allo stesso modo, non è possibile scegliere come target un host specifico su cui avviare o eseguire un'istanza. Inoltre, le istanze dedicate forniscono un supporto limitato per Bring Your Own License (BYOL).

Se hai bisogno di visibilità e controllo sul posizionamento delle istanze e di un supporto BYOL più completo, prendi in considerazione l'utilizzo di un host dedicato. Le istanze dedicate e gli host dedicati possono essere entrambi utilizzati per avviare istanze Amazon EC2 su server fisici dedicati. Non ci sono differenze di prestazioni, sicurezza o fisiche tra le Istanze dedicate e le istanze negli Host dedicati. Tuttavia, ci sono alcune differenze fondamentali tra loro. La tabella seguente evidenzia alcune differenze chiave tra istanze dedicate e host dedicati:

	Dedicated Host	Dedicated Instance
Server fisico dedicato	Server fisico con capacità di istanza completamente dedicata all'uso dell'utente.	Server fisico dedicato a un singolo account cliente.

	Dedicated Host	Dedicated Instance
Condivisione della capacità delle istanze	Può condividere la capacità dell'istanza con altri account.	Non supportato
Fatturazione	Fatturazione per host	Fatturazione per istanza
Visibilità di socket, core e ID host	Fornisce la visibilità del numero di socket e core fisici	Nessuna visibilità
Affinità a livello di host e istanza	Consente di distribuire in modo omogeneo le istanze sullo stesso server fisico nel tempo	Non supportato
Posiziona mento delle istanze interessate	Fornisce ulteriore visibilità e controllo sul posizionamento delle istanze su un server fisico	Non supportato
Ripristino automatico dell'istanza	Supportato. Per ulteriori informazioni, consulta Ripristino dell'host dedicato Amazon EC2.	Supportata
Modello di licenza Bring Your Own License (BYOL)	Supportato	Supporto parziale*
Prenotazioni della capacità	Non supportato	Supportata

* Le licenze Microsoft SQL Server con mobilità delle licenze tramite Software Assurance e Windows Virtual Desktop Access (VDA) possono essere utilizzate con l'istanza dedicata.

Per ulteriori informazioni sulle istanze dedicate, consulta la pagina Host dedicati di Amazon EC2.

Argomenti

Nozioni di base su Istanza dedicata

Un VPC può avere una tenancy di `default` o `dedicated`. Per impostazione predefinita, i tuoi VPC hanno una tenancy `default`, mentre le istanze avviate in un VPC di tenancy `default` hanno la tenancy `default`. Per avviare le istanze dedicate, procedi nel modo seguente:

- Crea un VPC con una tenancy di `dedicated` in modo che tutte le istanze del VPC vengano eseguite come istanze dedicate. Per ulteriori informazioni, consulta Avvia istanze dedicate in un VPC con tenancy predefinita.
- Crea un VPC con una tenancy di `default` e specifica manualmente una tenancy di `dedicated` per le istanze da eseguire come istanze dedicate. Per ulteriori informazioni, consulta Avvia istanze dedicate in un VPC con tenancy predefinita.

Funzionalità supportate

Le istanze dedicate supportano le seguenti funzionalità e integrazioni AWS di servizi:

Argomenti

Istanze riservate

Per riservare capacità per le istanze dedicate, è possibile acquistare istanze riservate dedicate o prenotazioni di capacità. Per ulteriori informazioni, consulta Istanze riservate e Prenotazione della capacità on demand.

Quando acquisti un'Istanza riservata dedicata, acquisti anche la capacità di avviare un'Istanza dedicata in un VPC a una tariffa di utilizzo molto ridotta; il costo di utilizzo si applica solo se avvii un'istanza con tenancy dedicata. Quando acquisti un'istanza riservata con una tenancy predefinita, si applica solo a un'istanza in esecuzione con la tenancy `default`; non si applicherà invece a un'istanza in esecuzione con la tenancy `dedicated`.

Non puoi modificare la tenancy di un'Istanza riservata dopo l'acquisto. Puoi tuttavia scambiare un'Istanza riservata modificabile con una nuova Istanza riservata modificabile con una tenancy diversa.

Scalabilità automatica

Per avviare le Istanze dedicate, è possibile utilizzare Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Avvio di istanze di Auto Scaling in un VPC nella Guida per l'utente di Amazon EC2 Auto Scaling.

Ripristino automatico

È possibile configurare il ripristino automatico per un'istanza dedicata se questa si danneggia a causa di un guasto hardware sottostante o di un problema che richiede la riparazione AWS . Per ulteriori informazioni, consulta Resilienza delle istanze.

Istanze spot dedicate

Puoi eseguire un'istanza spot dedicata specificando una tenancy `dedicated` quando crei una richiesta di istanza spot. Per ulteriori informazioni, consulta Specificare una tenancy per le Istanze spot.

Istanze a prestazioni espandibili

È possibile sfruttare i vantaggi dell'esecuzione su hardware istanza dedicata a tenancy singola con the section called “Istanze a prestazioni espandibili”. Le istanze dedicate T3 vengono lanciate in modalità illimitata per impostazione predefinita e forniscono un livello di base delle prestazioni della CPU con la possibilità di raggiungere un livello di CPU superiore quando richiesto dal carico di lavoro. Le prestazioni di base T3 e la capacità di ottimizzazione sono governate dai crediti CPU. A causa della natura espandibile dei tipi di istanza T3, si consiglia di monitorare il modo in cui le istanze T3

utilizzano le risorse della CPU dell'hardware dedicato per ottenere prestazioni ottimali. Le istanze dedicate T3 sono destinate a clienti con carichi di lavoro diversi che visualizzano un comportamento casuale della CPU, ma che idealmente hanno un utilizzo medio della CPU pari o inferiore a quello di base. Per ulteriori informazioni, consulta the section called “Concetti chiave”.

Amazon EC2 dispone di sistemi per identificare e correggere la variabilità delle prestazioni. Tuttavia, è ancora possibile sperimentare la variabilità a breve termine se si avviano più istanze dedicate T3 con modelli di utilizzo della CPU correlati. Per questi carichi di lavoro più complessi o correlati, si consiglia di utilizzare istanze dedicate M5 o M5a anziché istanze dedicate T3.

Limitazioni di Istanze dedicate

Quando utilizzi le istanze dedicate, tieni presente quanto indicato di seguito:

- Alcuni AWS servizi o le relative funzionalità non sono supportati da un VPC con la tenancy dell'istanza impostata su. `dedicated` Fai riferimento alla documentazione del relativo servizio per verificare se vi sono delle limitazioni.
- Alcuni tipi di istanza non possono essere avviati in un VPC se la tenancy delle istanze è impostata su `dedicated`. Per ulteriori informazioni sui tipi di istanza supportati, consulta Istanze dedicate di Amazon EC2.
- Quando avvii un'Istanza dedicata supportata da Amazon EBS, il volume EBS non viene eseguito sull'hardware con tenant singola.

Prezzi delle Istanze dedicate

I prezzi delle istanze dedicate sono diversi da quelli delle istanze on demand. Per ulteriori informazioni, consulta la pagina del prodotto Istanze dedicate di Amazon EC2.

Avvia istanze dedicate in un VPC con tenancy predefinita

Quando crei un VPC, puoi specificarne la tenancy delle istanze. Se avvii un'istanza in un VPC che ha una tenancy dell'istanza `dedicated`, l'istanza verrà sempre eseguita come istanza dedicata su un hardware a tua disposizione.

Per ulteriori informazioni sulla creazione di un VPC e sulla scelta delle opzioni di tenancy, consulta la sezione Creazione di un VPC nella Guida per l'utente di Amazon VPC.

Puoi avviare un'Istanza dedicata utilizzando la procedura guidata di avvio delle istanze di Amazon EC2.

Console

Per avviare un'Istanza dedicata in un VPC con tenancy predefinita tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Istanze, Avvia istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI dall'elenco.
4. Nella sezione Tipo di istanza, seleziona il tipo di istanza da avviare.

   > **Note**
   >
   > Verifica di selezionare un tipo di istanza supportato come Istanza dedicata. Per ulteriori informazioni, consulta Istanze dedicate di Amazon EC2.

5. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da associare all'istanza.
6. Nella sezione Advanced details (Dettagli avanzati), per Tenancy seleziona Dedicated (Dedicata).
7. Configura le opzioni rimanenti dell'istanza in base alla necessità. Per ulteriori informazioni, consulta Avvio di un'istanza utilizzando parametri definiti.
8. Scegliere Launch Instance (Avvia istanza).

Command line

Per impostare l'opzione della tenancy per un'istanza durante l'avvio tramite la riga di comando

- run-instances (AWS CLI)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Per ulteriori informazioni sull'avvio di un'istanza con tenancy `host`, consultare Avvia istanze Amazon EC2 su un host dedicato Amazon EC2.

Modifica la tenancy di un'istanza Amazon EC2

Puoi modificare la tenancy di un'istanza interrotta dopo averla avviata. Le modifiche apportate avranno effetto al successivo avvio dell'istanza.

I dettagli del sistema operativo dell'istanza e l'eventuale installazione di SQL Server influiscono sulle conversioni supportate. Per ulteriori informazioni sui percorsi di conversione di tenancy disponibili per la tua istanza, consulta Conversione di tenancy nella Guida per l'utente di License Manager.

> **Note**
>
> Per le istanze T3, è necessario avviare l'istanza su un host dedicato per utilizzare una tenancy di `host`. Non puoi modificare la tenancy da `host` a `dedicated` o `default`. Se si prova ad apportare una di queste modifiche di tenancy non supportate, verrà visualizzato il codice di errore `InvalidRequest`.

Console

Per modificare la tenancy di un'istanza utilizzando la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Instances (Istanze) e selezionare l'istanza.
3. Scegli Instance state (Stato istanza), quindi Stop instance (Arresta istanza) e Stop (Arresta).
4. Seleziona Actions (Operazioni), Instance settings (Impostazioni istanza), Modify instance placement (Modifica posizionamento delle istanze).
5. Nell'elenco Tenancy, specificare se eseguire l'istanza sull'hardware dedicato o su un Host dedicato. Seleziona Salva.

Command line

Per modificare il valore della tenancy di un'istanza utilizzando la riga di comando

- modify-instance-placement (AWS CLI)
- Edit-EC2InstancePlacement (AWS Tools for Windows PowerShell)

Modifica la locazione di un Amazon VPC

Puoi modificare la tenancy di un'istanza di un VPC da `dedicated` a `default` dopo averla creata. La modifica della tenancy delle istanze del VPC non influisce sulla tenancy di eventuali istanze esistenti nel VPC. Al successo avvio di un'istanza nel VPC, l'istanza avrà una tenancy `default`, a meno che durante l'avvio non specifichi un valore diverso.

> **Note**
>
> Non è possibile modificare la tenancy di istanza di un VPC da `default` a `dedicated` dopo la sua creazione.

Puoi modificare la tenancy dell'istanza di un VPC utilizzando solo AWS un SDK o AWS CLI l'API Amazon EC2.

Command line

Per modificare l'attributo di tenancy dell'istanza di un VPC utilizzando il AWS CLI

Usa il modify-vpc-tenancycomando e specifica l'ID del VPC e il valore di tenancy dell'istanza. L'unico valore supportato è `default`.

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

Prenotazioni della capacità

Prenotazioni della capacità ti permette di prenotare la capacità di elaborazione per le istanze Amazon EC2 in una zona di disponibilità specifica. Esistono due tipi di prenotazioni della capacità per casi d'uso differenti.

Tipi di prenotazioni della capacità

- Prenotazione della capacità on demand
- Blocchi di capacità per ML

Di seguito sono elencati alcuni casi d'uso comuni per le prenotazioni della capacità on demand:

- Eventi di dimensionamento: puoi creare prenotazioni della capacità on demand prima di eventi aziendali critici per assicurarti di poter dimensionare le risorse all'occorrenza.
- Requisiti normativi e ripristino di emergenza: utilizza le prenotazioni della capacità on demand per soddisfare i requisiti normativi in materia di alta disponibilità e riserva la capacità in una zona di disponibilità o regione diversa per il ripristino di emergenza.

Di seguito sono elencati alcuni casi d'uso comuni di Blocchi di capacità per ML:

- Addestramento e messa a punto dei modelli di machine learning (ML): ottieni un accesso ininterrotto alle istanze GPU che hai prenotato per completare l'addestramento e la messa a punto dei modelli di ML.
- Esperimenti e prototipi di ML: esegui esperimenti e crea prototipi che richiedono istanze GPU per brevi periodi.

Quando utilizzare la prenotazione della capacità on demand

Utilizza le prenotazioni della capacità on demand se hai requisiti di capacità rigorosi e stai eseguendo carichi di lavoro aziendali critici che richiedono la garanzia della capacità. Con le prenotazioni della capacità on demand, puoi sempre disporre dell'accesso alla capacità Amazon EC2 che hai prenotato per tutto il tempo necessario.

Quando utilizzare Blocchi di capacità per ML

Utilizza Blocchi di capacità per ML quando devi assicurarti di avere accesso ininterrotto alle istanze GPU per un periodo di tempo definito a partire da una data futura. I blocchi di capacità sono ideali per addestrare e perfezionare i modelli di ML, per brevi cicli di sperimentazione e per gestire i picchi temporanei della domanda di inferenza in futuro. Con Blocchi di capacità puoi assicurarti di avere accesso alle risorse GPU in una data specifica per eseguire i tuoi carichi di lavoro ML.

Prenotazione della capacità on demand

Prenotazioni di capacità on demand ti permette di prenotare la capacità di elaborazione per le istanze Amazon EC2 in una zona di disponibilità specifica per qualsiasi durata. Le prenotazioni della capacità riducono il rischio di non poter accedere alla capacità on-demand in caso di limitazioni di capacità. Se i tuoi requisiti di capacità sono rigorosi e stai eseguendo carichi di lavoro aziendali critici che richiedono un certo livello di garanzia della capacità a lungo o breve termine, ti consigliamo di creare una prenotazione della capacità per assicurarti di avere sempre accesso alla capacità di Amazon EC2 quando ne hai bisogno, per tutto il tempo necessario.

È possibile creare Prenotazioni della capacità in qualsiasi momento, senza impegnarsi per uno o tre anni. La capacità diventa disponibile e la fatturazione inizia non appena viene effettuato il provisioning della Prenotazione della capacità nel tuo account. Quando non hai più bisogno della garanzia di capacità, annulla la prenotazione della capacità per rilasciarla e interrompere i costi associati. Puoi anche utilizzare gli sconti di fatturazione offerti da Savings Plans e dalle istanze riservate regionali per ridurre il costo di una prenotazione della capacità.

Per creare una Prenotazione di capacità, specificare:

- La zona di disponibilità in cui prenotare la capacità.
- Il numero di istanze per cui si desidera riservare la capacità.
- Gli attributi dell'istanza, inclusi il tipo di istanza, la piattaforma, la zona di disponibilità e la tenancy

Prenotazioni di capacità può essere utilizzata solo dalle istanze che corrispondono agli attributi. Come impostazione predefinita, vengono automaticamente utilizzate eseguendo istanze che corrispondono agli attributi. Se non disponi di istanze in esecuzione che corrispondono agli attributi della Prenotazione di capacità, questa rimane inutilizzata finché non avvii un'istanza con attributi corrispondenti.

Indice

Differenze tra Prenotazioni di capacità, Istanze riservate e Savings Plans.

La tabella seguente evidenzia alcune differenze chiave tra Prenotazioni di capacità, Istanze riservate e Savings Plans:

	Prenotazioni di capacità	Istanze riservate zonali	Istanze riservate regionali	Savings Plans
Termine	Nessun impegno richiesto. Possono essere create e annullate in base alle esigenze.	Richiedono un impegno fisso di uno o tre anni		
Vantaggio capacità	Capacità riservata in una zona di disponibilità specifica.		Nessuna capacità riservata.	
Sconto di fatturazione	Nessuno sconto di fatturazione. †	Fornisce uno sconto di fatturazione.		
Limiti di istanze	Si applicano i limiti Istanza on demand per regione.	Il valore predefinito è 20 per zona di disponibilità. È possibile richiedere un aumento del limite.	Il valore predefinito è 20 per regione. È possibile richiedere un aumento del limite.	Nessun limite.

† È possibile combinare le prenotazioni di capacità con Savings Plans o le istanze riservate regionali per ricevere uno sconto.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Istanze riservate
- Guida per l'utente di Savings Plans

Piattaforme supportate

È necessario creare la Prenotazione di capacità con la piattaforma corretta per assicurarsi che corrisponda correttamente alle istanze. Le Prenotazioni di capacità supportano le seguenti piattaforme:

- Linux/Unix
- Linux con SQL Server Standard
- Linux con SQL Server Web
- Linux con SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- RHEL con SQL Server Standard
- RHEL con SQL Server Enterprise
- RHEL con SQL Server Web
- RHEL con HA
- RHEL con HA e SQL Server Standard
- RHEL con HA e SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows con SQL Server
- Windows con SQL Server Web
- Windows con SQL Server Standard
- Windows con SQL Server Enterprise

Quando si acquista un'Prenotazione di capacità, è necessario specificare la piattaforma corrispondente al sistema operativo dell'istanza.

- Per le distribuzioni SUSE Linux e RHEL, escluso BYOL, è necessario scegliere la piattaforma specifica. Ad esempio, la piattaforma SUSE Linux o Red Hat Enterprise Linux.
- Per tutte le altre distribuzioni Linux (tra cui Ubuntu), scegliere la piattaforma Linux/UNIX.
- Se si porta l'abbonamento RHEL esistente con formula BYOL, è necessario scegliere la piattaforma Linux/UNIX.
- Per Windows con SQL Standard, Windows con SQL Server Enterprise e Windows con SQL Server Web, è necessario scegliere la piattaforma specifica.
- Per tutte le altre versioni di Windows, ad eccezione di BYOL che non è supportato, scegliere la piattaforma Windows.

Quote

Il numero di istanze per le quali è possibile prenotare la capacità si basa sula quota di istanze on demand del proprio account. È possibile prenotare la capacità per tante istanze quante ne permette tale quota, meno il numero delle istanze in esecuzione.

Le quote si applicano solo alle istanze in esecuzione. Se l'istanza è in sospeso, interrotta o ibernata, non viene conteggiata ai fini della quota.

Limitazioni

Prima di creare le Prenotazioni di capacità, considera le seguenti limitazioni e restrizioni.

- Le Prenotazioni di capacità attive e inutilizzate contano per i limiti Istanza on demand.
- Le prenotazioni di capacità non sono trasferibili da un AWS account all'altro. Tuttavia, puoi condividere le prenotazioni di capacità con altri AWS account. Per ulteriori informazioni, consulta Utilizzo degli Prenotazioni di capacità condivisi.
- Gli sconti di fatturazione Istanza riservata zonali non si applicano a Prenotazioni di capacità.
- Le Prenotazioni di capacità non possono essere create in gruppi di collocazione cluster. I gruppi di collocazione di partizione non sono supportati.
- Prenotazioni di capacità non può essere utilizzato con Host dedicati. Prenotazioni della capacità non può essere utilizzato con Istanze dedicate.
- [Istanze Windows] Le prenotazioni di capacità non possono essere utilizzate con la licenza Bring Your Own License (BYOL).
- Prenotazioni di capacità non assicura che un'istanza ibernata possa riprendere dopo aver tentato di avviarla.

Prezzi e fatturazione di Prenotazione di capacità

Argomenti

- Prezzi
- Fatturazione
- Sconti di fatturazione
- Visualizzazione di una fattura

Prezzi

Le Prenotazioni della capacità vengono addebitate alla tariffa on-demand equivalente indipendentemente dal fatto che si stia o meno eseguendo istanze nella capacità riservata. Se non utilizzi la prenotazione, sarà indicata come prenotazione inutilizzata nella fattura Amazon EC2. Quando esegui un'istanza che corrisponde agli attributi di una prenotazione, paghi solamente per l'istanza e non per la prenotazione. Non sono previsti costi iniziali o costi aggiuntivi.

Ad esempio, se crei una Prenotazione di capacità per 20 istanze Linux `m4.large` e ne esegui 15 `m4.large` nella stessa zona di disponibilità, ti verrà addebitato il costo per 15 istanze attive e per 5 istanze non utilizzate nella prenotazione.

Alle prenotazioni della capacità, si applicano sconti di fatturazione per i Savings Plans e per le istanze riservate regionali. Per ulteriori informazioni, consulta Sconti di fatturazione.

Per ulteriori informazioni, consulta Amazon EC2 Prezzi di .

Fatturazione

La fatturazione viene avviata non appena viene effettuato il provisioning della Prenotazione della capacità nel tuo account e prosegue finché la Prenotazione della capacità rimane effettuata nel tuo account.

Le Prenotazioni di capacità sono fatturate a granularità per secondo. Questo significa che verrai addebitato per ore parziali Ad esempio, se una Prenotazione della capacità rimane con provisioning nell'account per 24 ore e 15 minuti, saranno fatturate 24.25 ore di prenotazione.

Gli esempi seguenti mostrano come viene fatturata una Prenotazione di capacità. La Prenotazione di capacità viene creata per un'istanza Linux `m4.large`, che ha una tariffa on demand di 0,10 USD per ora di utilizzo. In questo esempio, la Prenotazione della capacità è con provisioning nell'account per cinque ore. La Prenotazione di capacità non viene utilizzata per la prima ora, quindi viene fatturata per un'ora non utilizzata alla tariffa on demand standard del tipo di istanza `m4.large`. Dalle due alle cinque ore, la Prenotazione di capacità è occupata da un'istanza `m4.large`. Durante tale periodo, Prenotazione di capacità non accumula nessun costo e all'account viene addebitata l'istanza `m4.large` che la occupa. Alla sesta ora, la Prenotazione di capacità viene annullata e l'istanza `m4.large` viene eseguita normalmente al di fuori della capacità riservata. Per quell'ora, viene applicata la tariffa on demand del tipo di istanza `m4.large`.

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

Sconti di fatturazione

Gli sconti sulla fatturazione per Savings Plans e Regional Reserved Instances si applicano alle prenotazioni di capacità. AWS applica automaticamente questi sconti alle prenotazioni di capacità con attributi corrispondenti. Quando una istanza utilizza una Prenotazione di capacità, lo sconto viene applicato all'istanza. Gli sconti vengono applicati preferibilmente all'utilizzo delle istanze prima di utilizzare le Prenotazioni di capacità inutilizzate.

Gli sconti di fatturazione per le Istanze riservate zonali non si applicano alle Prenotazioni di capacità.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Istanze riservate
- Guida per l'utente di Savings Plans
- Opzioni di fatturazione e acquisto

Visualizzazione di una fattura

Puoi controllare gli addebiti e le commissioni relativi al tuo account sulla AWS Billing and Cost Management console.

- Il Dashboard (Pannello di controllo) mostra un riepilogo di spesa per l'account.
- Nella pagina Bills (Fatture), sotto Details (Dettagli), espandi la sezione Elastic Compute Cloud e la regione per ottenere le informazioni di fatturazione relative alle Prenotazioni di capacità.

Puoi visualizzare gli addebiti online o scarica un file CSV. Per ulteriori informazioni, consulta Voci prenotazione di capacità nella Guida per l'utente di AWS Billing and Cost Management .

Utilizzo di Prenotazioni di capacità

Per iniziare a usare le Prenotazioni di capacità, crea la prenotazione di capacità necessaria nella zona di disponibilità. Quindi, è possibile avviare istanze nella capacità riservata, visualizzarne la capacità di utilizzo in tempo reale e aumentarne o diminuirne la capacità in base alle esigenze.

Per impostazione predefinita, le prenotazioni di capacità associano automaticamente le nuove istanze e le istanze in esecuzione con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy). Questo significa che qualsiasi istanza con attributi corrispondenti viene eseguita automaticamente nella Prenotazione di capacità. Tuttavia, puoi anche utilizzare una Prenotazione di capacità per carichi di lavoro specifici. In questo modo puoi controllare in modo esplicito quali istanze possono essere eseguite in quella capacità riservata.

Puoi specificare il modo in cui termina la prenotazione. Si può scegliere di annullare manualmente la Prenotazione di capacità o di terminarla automaticamente in un momento specificato. Se specifichi un'ora di fine, la Prenotazione di capacità viene annullata entro un'ora a dall'ora specificata. Se ad esempio specifichi il 31 maggio 2019 alle 13:30:55, la Prenotazione di capacità terminerà tra le 13:30:55 e le 14:30:55 del 31 maggio 2019. Dopo il termine della prenotazione, non è più possibile puntare istanze alla Prenotazione di capacità. Le istanze in esecuzione nella capacità riservata continuano a essere eseguite senza interruzioni. Se le istanze che puntano a una Prenotazione di capacità vengono arrestate, non è possibile riavviarle finché non vengono rimosso le loro preferenze di target della Prenotazione di capacità o configurarle in modo che puntino a una Prenotazione di capacità diversa.

Indice

Creazione di una Prenotazione di capacità

Se la tua richiesta di creazione di una Prenotazione di capacità va a buon fine, la capacità è immediatamente disponibile. La capacità rimane prenotata per l'utilizzo finché Prenotazione di capacità è attiva ed è possibile avviarvi istanze in qualsiasi momento. Se la Prenotazione di capacità è aperta, le nuove istanze e le istanze esistenti che hanno attributi corrispondenti vengono eseguiti automaticamente nella capacità della Prenotazione di capacità. Se la Prenotazione della capacità è `targeted`, le istanze devono specificamente puntarla per l'esecuzione nella capacità riservata.

La richiesta di creare una Prenotazione di capacità ha esito negativo se una selle seguenti condizioni è true:

- Amazon EC2 non dispone di capacità sufficiente per soddisfare la richiesta. Prova in un momento successivo, prova una zona di disponibilità differente o prova una richiesta inferiore. Se l'applicazione è flessibile su più tipi di istanza e dimensioni, prova con attributi di istanza differenti.
- La quantità richiesta supera il limite Istanza on demand per la famiglia di istanze selezionata. Incrementare il limite Istanza on demand per la famiglia di istanze e riprovare. Per ulteriori informazioni, consulta Quote di istanze on demand.

Come creare una Prenotazione di capacità utilizzando la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Prenotazioni di capacità, quindi Create Prenotazione di capacità (Crea Prenotazione di capacità).
3. Nella pagina Crea una Prenotazione di capacità, configurare le impostazioni seguenti nella sezione Instance details (Dettagli istanza): Il tipo di istanza, la piattaforma, la zona di disponibilità e la tenenza delle istanze avviate devono corrispondere al tipo di istanza, alla piattaforma, alla zona di disponibilità e alla tenancy specificati qui, altrimenti la prenotazione di capacità non viene applicata. Ad esempio, se una Prenotazione di capacità aperta non corrisponde, l'avvio di un'istanza destinata esplicitamente a Prenotazione di capacità non riesce.

    a. Instance Type (Tipo di istanza) – Il tipo di istanza da avviare nella capacità riservata.

    b. Launch EBS-optimized instances (Avvia istanze ottimizzate per EBS) — Specificare se prenotare la capacità per istanze ottimizzate per EBS. Questa opzione è selezionata come impostazione predefinita per alcuni tipi di istanza. Per ulteriori informazioni, consulta the section called “Ottimizzazione di Amazon EBS”.

    c. Platform – Il sistema operativo per le istanze. Per ulteriori informazioni, consulta Piattaforme supportate.

    d. Availability Zone (Zona di disponibilità) – La zona di disponibilità nella quale prenotare la capacità.

    e. Tenancy – Specificare se eseguire un hardware condiviso (default) o un'istanza dedicata.

    f. (Opzionale)Gruppo di collocazione ARNL'ARN del gruppo di collocazione cluster in cui creare la prenotazione della capacità.

    Per ulteriori informazioni, consulta Le Prenotazioni della capacità in gruppi di collocazione cluster..

g. Quantity (Quantità) – Specificare il numero di istanze per le quali riservare la capacità. Se si specifica una quantità che supera il limite Istanza on demand rimanente per il tipo di istanza selezionato, la richiesta viene negata.

4. Configurare le seguenti impostazioni nella sezione Reservation details (Dettagli prenotazione):

   a. Reservation Ends (Fine prenotazione) — Selezionare una delle seguenti opzioni:

      - Manually (Manualmente) — Prenotare la capacità fino a quando viene annullata esplicitamente.
      - Specific time (Ora specifica) – Annulla la prenotazione della capacità automaticamente alla data e all'ora specificate.

   b. Instance eligibility (Idoneità istanza) — Selezionare una delle seguenti opzioni:

      - open — (Impostazione predefinita) La Capacity Reservation corrisponde a qualsiasi istanza con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy). Se si avvia un'istanza con gli attributi corrispondenti, viene posizionata nella capacità riservata automaticamente.
      - targetizzato: la Capacity Reservation accetta solo istanze con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e che hanno come target esplicito la prenotazione.

5. Selezionare Request reservation (Richiedi prenotazione).

Per creare una prenotazione di capacità utilizzando il AWS CLI

Utilizza il comando create-capacity-reservation. Per ulteriori informazioni, consulta Piattaforme supportate.

Il comando seguente crea una prenotazione di capacità che riserva la capacità per tre `m5.2xlarge` istanze che eseguono AMI Red Hat Enterprise Linux nella zona di `us-east-1a` disponibilità.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-platform Red
 Hat Enterprise Linux --availability-zone us-east-1a --instance-count 3
```

Il comando seguente crea una prenotazione di capacità che riserva la capacità per tre `m5.2xlarge` istanze che eseguono Windows con AMI SQL Server nella zona di disponibilità. `us-east-1a`

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-
platform Windows with SQL Server --availability-zone us-east-1a --instance-count 3
```

Avvio di istanze in una Prenotazione di capacità esistente

Quando si avvia un'istanza, è possibile specificare se avviare l'istanza in qualsiasi Prenotazione di capacità open, in una specifica Prenotazione di capacità o in un gruppo di Prenotazioni di capacità. È possibile avviare un'istanza solo in una riserva di capacità con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e una capacità sufficiente. In alternativa, è possibile configurare l'istanza in modo da evitare l'esecuzione in un Prenotazione di capacità, anche se si dispone di un Prenotazione di capacità open che ha attributi corrispondenti e capacità disponibile.

L'avvio di un'istanza in una Prenotazione di capacità ne riduce la capacità disponibile per il numero di istanze avviate. Ad esempio, se avvii tre istanze, la capacità disponibile della Prenotazione di capacità è ridotta di tre.

Come avviare istanze in una Prenotazione di capacità esistente utilizzando la console

1. Segui la procedura per avviare un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per specificare le impostazioni per il gruppo di collocamento e la prenotazione della capacità.
2. Espandi i dettagli avanzati ed esegui le seguenti operazioni:

   a. Per Gruppo di posizionamento, selezionate il gruppo di posizionamento del cluster in cui avviare l'istanza.

   b. Per Capacity Reservation (Prenotazione della capacità), scegliere una delle seguenti opzioni a seconda della configurazione della prenotazione della capacità:

      - Nessuno: impedisce l'avvio delle istanze in una riserva di capacità. Le istanze vengono eseguite in capacità on demand.
      - Apri: avvia le istanze in qualsiasi riserva di capacità che abbia attributi corrispondenti e una capacità sufficiente per il numero di istanze selezionate. Se non si dispone di una Prenotazione di capacità corrispondente con capacità sufficiente, l'istanza utilizza la capacità on demand.
      - Target by ID: avvia le istanze nella prenotazione di capacità selezionata. Se questa Prenotazione di capacità non dispone di capacità sufficiente per il numero di istanze selezionate, l'avvio dell'istanza non riesce.

- Target per gruppo: avvia le istanze in qualsiasi riserva di capacità con attributi e capacità disponibili corrispondenti nel gruppo di prenotazione di capacità selezionato. Se il gruppo selezionato non dispone di una Prenotazione di capacità con attributi corrispondenti e capacità disponibile, le istanze vengono avviate in Capacità on demand.

3. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Per avviare un'istanza in una prenotazione di capacità esistente utilizzando il AWS CLI

Utilizzare il comando run-instances e specificare il parametro `--capacity-reservation-specification`.

L'esempio seguente avvia un'istanza `t2.micro` in qualsiasi Prenotazione di capacità aperta che abbia attributi corrispondenti e capacità disponibile:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationPreference=open
```

L'esempio seguente avvia un'istanza `t2.micro` in una `targeted` Prenotazione di capacità:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

L'esempio seguente avvia un'istanza `t2.micro` in un gruppo Prenotazione di capacità:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1
 --instance-type t2.micro --key-name MyKeyPair --subnet-
id subnet-1234567890abcdef1 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Modifica di una Prenotazione di capacità

È possibile modificare gli attributi di una Prenotazione di capacità attiva dopo averla creata. Non è possibile modificare una Prenotazione di capacità dopo la sua scadenza o dopo averla esplicitamente annullata.

Quando modifichi una Prenotazione di capacità, puoi solo aumentare o diminuire la quantità e modificare il modo in cui è rilasciata. Non è possibile modificare il tipo di istanza, l'ottimizzazione per EBS, la piattaforma, la zona di disponibilità o l'idoneità dell'istanza di una prenotazione della capacità. Se devi modificare uno di questi attributi, ti consigliamo di annullare la prenotazione, quindi crearne una nuova con gli attributi richiesti.

Se si specifica una quantità nuova che supera il limite Istanza on demand rimanente per il tipo di istanza selezionato, l'aggiornamento avrà esito negativo.

Come modificare una richiesta Prenotazione di capacità utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Prenotazioni di capacità, selezionare la Prenotazione di capacità da modificare e selezionare Edit (Modifica).
3. Modificare le opzioni Quantity (Quantità) o Reservation ends (Fine prenotazione) in base alle esigenze e selezionare Save changes (Salva modifiche).

Per modificare una prenotazione di capacità utilizzando il AWS CLI

Utilizza il comando modify-capacity-reservation:

Ad esempio, il comando seguente modifica una Prenotazione di capacità per riservare la capacità per otto istanze.

```
aws ec2 modify-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0 --instance-count 8
```

Modificare le impostazioni della Prenotazione di capacità di un'istanza

Puoi modificare le impostazioni Prenotazione di capacità seguenti per un'istanza arrestata in qualsiasi momento:

- Inizia da qualsiasi prenotazione di capacità con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e capacità disponibile.
- Avviare l'istanza in una Prenotazione di capacità specifica.
- Avviare in qualsiasi prenotazione della capacità che abbia attributi corrispondenti e capacità disponibile in un gruppo di prenotazione della capacità
- Impedire l'avvio dell'istanza in una Prenotazione di capacità.

Come modificare le impostazioni Prenotazione di capacità di un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Instances (Istanze) e selezionare l'istanza da modificare. Arrestare l'istanza in errore, se non è già stata arrestata.
3. Scegli Azioni, Impostazioni dell'istanza, Modifica impostazioni di prenotazione della capacità.
4. Per Prenotazione di capacità, scegliere una delle seguenti opzioni:

   - Open (Apri) – Avvia l'istanza in una qualsiasi Prenotazione di capacità che abbia attributi corrispondenti e capacità sufficiente per il numero di istanze selezionate. Se non si dispone di una Prenotazione di capacità corrispondente con capacità sufficiente, l'istanza utilizza la capacità on demand.
   - None (Nessuno) – Impedisce l'avvio delle istanze in una Prenotazione di capacità. Le istanze vengono eseguite in capacità on demand.
   - Specify Capacity Reservation (Specifica prenotazione di capacità) – Avvia le istanze nella Prenotazione di capacità selezionata. Se questa Prenotazione di capacità non dispone di capacità sufficiente per il numero di istanze selezionate, l'avvio dell'istanza non riesce.
   - Specify Capacity Reservation group (Specifica gruppo Prenotazione capacità) – Avvia le istanze in qualsiasi Prenotazione di capacità con attributi corrispondenti e capacità disponibile nel gruppo di — selezionato. Se il gruppo selezionato non dispone di una Prenotazione di capacità con attributi corrispondenti e capacità disponibile, le istanze vengono avviate in Capacità on demand.

Per modificare le impostazioni di prenotazione della capacità di un'istanza utilizzando il AWS CLI

Utilizzate il comando modify-instance-capacity-reservation-attributes.

Ad esempio, il comando seguente modifica l'impostazione della Prenotazione di capacità di un'istanza in `open` o `none`.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationPreference=none|open
```

Ad esempio, il comando seguente modifica un'istanza per indirizzare una specifica Prenotazione di capacità.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

Ad esempio, il comando seguente modifica un'istanza per indirizzare un gruppo di Prenotazione di capacità specifico.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Visualizzazione di una Prenotazione di capacità

una Prenotazioni di capacità può trovarsi nei possibili stati elencati di seguito:

- `active` – La capacità è disponibile per l'uso.
- `expired`— – La Prenotazione di capacità è scaduta automaticamente alla data e ora specificate nella richiesta di prenotazione. La capacità riservata non è più disponibile per l'utilizzo.
- `cancelled`—La Prenotazione di capacità è stata annullata. La capacità riservata non è più disponibile per l'utilizzo.
- `pending`— – La richiesta Prenotazione di capacità è stata completata, ma il provisioning della capacità è ancora in corso.
- `failed`— – La richiesta Prenotazione di capacità ha avuto esito negativo. Una richiesta potrebbe non riuscire a causa di parametri della richiesta non validi, limitazioni di capacità o vincoli al limite di istanze. È possibile visualizzare una richiesta non riuscita per 60 minuti.

> **Note**
>
> A causa dell'eventuale modello di coerenza seguito dalle API di Amazon EC2, dopo aver creato una prenotazione di capacità, possono essere necessari fino a 5 minuti prima che la console e describe-capacity-reservationsla risposta indichino che la prenotazione di capacità è attiva. `active` Durante questo periodo, la risposta della console e di `describe-capacity-reservations` può indicare che la Prenotazione della capacità è nello stato `pending`. Tuttavia, la Prenotazione della capacità potrebbe essere già disponibile per l'uso ed è possibile tentare di avviare istanze al suo interno.

Come visualizzare la Prenotazioni di capacità utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Prenotazioni di capacità e selezionare una Prenotazione di capacità da visualizzare.
3. Selezionare View launched instances for this reservation (Visualizza le istanze avviate per questa prenotazione).

Per visualizzare le tue prenotazioni di capacità, utilizza il AWS CLI

Utilizza il comando describe-capacity-reservations:

Ad esempio, il comando seguente descrive tutte le Prenotazioni di capacità.

```
aws ec2 describe-capacity-reservations
```

Output di esempio:

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-group/
MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
```

```
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
        }
    ]
}
```

Annullamento di una Prenotazione di capacità

È possibile annullare una Prenotazione di capacità in qualsiasi momento, se non è più necessaria la capacità riservata. Quando annulli una Prenotazione di capacità, la capacità viene rilasciata immediatamente e non è più riservata per l'utilizzo.

È possibile annullare Prenotazioni di capacità e Prenotazioni di capacità vuote con istanze in esecuzione. Se annulli una prenotazione della capacità con istanze in esecuzione, le istanze continuano a essere eseguite normalmente al di fuori della prenotazione della capacità a tariffe per le istanze on demand standard o a una tariffa scontata, se disponi di un Savings Plan o di una Istanza riservata regionale corrispondente.

Dopo l'annullamento di una Prenotazione di capacità, le istanze che la puntano non possono più avviare. Modifica queste istanze in modo che puntino a una Prenotazione di capacità diversa, vengano avviate in una qualsiasi Prenotazione di capacità aperta con attributi corrispondenti e capacità sufficiente oppure evita di avviare in una Prenotazione di capacità. Per ulteriori informazioni, consulta Modificare le impostazioni della Prenotazione di capacità di un'istanza.

Come annullare una Prenotazione di capacità utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Prenotazioni di capacità e selezionare Prenotazione di capacità per annullare.
3. Selezionare Cancel reservation (Annulla prenotazione), Cancel reservation (Annulla prenotazione).

Per annullare una prenotazione di capacità utilizzando il AWS CLI

Utilizza il comando cancel-capacity-reservation:

Ad esempio, il comando seguente annulla una Prenotazione di capacità con un ID di `cr-1234567890abcdef0`.

```
aws ec2 cancel-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0
```

Utilizzo di Prenotazione di capacità con i gruppi

È possibile utilizzarla AWS Resource Groups per creare raccolte logiche di prenotazioni di capacità, chiamate gruppi di risorse. Un gruppo di risorse è un raggruppamento logico di AWS risorse che si trovano tutte nella stessa AWS regione. Per ulteriori informazioni sui gruppi di risorse, consultare Che cosa sono i gruppi di risorse? nella Guida per l'utente di AWS Resource Groups .

Puoi includere le prenotazioni di capacità che possiedi nel tuo account e le prenotazioni di capacità condivise con te da altri AWS account in un unico gruppo di risorse. Puoi anche includere prenotazioni di capacità con attributi diversi (tipo di istanza, piattaforma, zona di disponibilità e tenancy) in un unico gruppo di risorse.

Quando crei gruppi di risorse per le prenotazioni di capacità, puoi assegnare le istanze a un gruppo di prenotazioni di capacità anziché a una singola prenotazione. Le istanze destinate a un gruppo di prenotazioni di capacità corrispondono a qualsiasi prenotazione di capacità del gruppo che presenta attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e capacità disponibile. Se il gruppo non dispone di una Prenotazione di capacità con attributi corrispondenti e capacità disponibile, le istanze vengono eseguite utilizzando la capacità on demand. Se una corrispondenza Prenotazione di capacità viene aggiunta al gruppo di destinazione in una fase successiva, l'istanza viene automaticamente abbinata e spostata nella sua capacità riservata.

Per impedire l'uso non intenzionale di Prenotazioni di capacità in un gruppo, configurare le Prenotazioni di capacità nel gruppo per accettare solo le istanze che hanno come target esplicitamente la riserva di capacità. A tale scopo, impostare Instance eligibility (Idoneità istanza) su target (console precedente) o Solo istanze che specificano questa prenotazione (nuova console) durante la creazione di Prenotazione di capacità utilizzando la console Amazon EC2. Quando si utilizza il AWS CLI, specificare `--instance-match-criteria targeted` quando si crea la prenotazione di capacità. In questo modo è possibile eseguire nel gruppo solo le istanze che hanno come target esplicito il gruppo o una Prenotazione di capacità nel gruppo.

Se una Prenotazione di capacità nel gruppo viene annullata o scade mentre dispone di istanze in esecuzione, le istanze vengono spostate automaticamente in un'altra Prenotazione di capacità nel gruppo con attributi corrispondenti e capacità disponibile. Se nel gruppo non sono presenti

Prenotazioni di capacità rimanenti con attributi corrispondenti e capacità disponibile, le istanze vengono eseguite in capacità on demand. Se una Prenotazione di capacità corrispondente viene aggiunta al gruppo di destinazione in una fase successiva, l'istanza viene automaticamente spostata nella sua capacità riservata.

Argomenti

Creazione di un gruppo di prenotazione di capacità

Creazione di un gruppo per le prenotazioni di capacità

Utilizzate il comando create-group AWS CLI . Per `name`, fornire un nome descrittivo per il gruppo e, per `configuration`, specificare due parametri di richiesta `Type`:

- `AWS::EC2::CapacityReservationPool` per garantire che il gruppo di risorse possa essere mirato per i lanci di istanza
- `AWS::ResourceGroups::Generic` con `allowed-resource-types` impostato su `AWS::EC2::CapacityReservation` per garantire che il gruppo di risorse accetti solo prenotazioni capacità

Ad esempio, il seguente comando crea una tabella denominata `MyCRGroup`.

```
aws resource-groups create-group --name MyCRGroup --configuration
 '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Di seguito viene mostrato l'output di esempio.

```
{
    "GroupConfiguration": {
```

```
        "Status": "UPDATE_COMPLETE",
        "Configuration": [
            {
                "Type": "AWS::EC2::CapacityReservationPool"
            },
            {
                "Type": "AWS::ResourceGroups::Generic",
                "Parameters": [
                    {
                        "Values": [
                            "AWS::EC2::CapacityReservation"
                        ],
                        "Name": "allowed-resource-types"
                    }
                ]
            }
        ]
    },
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

Aggiunta di una prenotazione di capacità a un gruppo

Se aggiungi a un gruppo una prenotazione di capacità condivisa con te e tale prenotazione non è condivisa, essa viene automaticamente rimossa dal gruppo.

Per aggiungere Prenotazione di capacità a un gruppo

Utilizzare il comando AWS CLI group-resources. Per `group`, specificare il nome del gruppo a cui aggiungere le Prenotazioni di capacità, e per `resources`, specificare ARN di Prenotazioni di capacità da aggiungere. Per aggiungere più Prenotazioni di capacità, separare gli ARN con uno spazio. Per ottenere gli ARN delle prenotazioni di capacità da aggiungere, utilizzate il describe-capacity-reservations AWS CLI comando e specificate gli ID delle prenotazioni di capacità.

Ad esempio, il comando seguente aggiunge due Prenotazioni di capacità a un gruppo denominato `MyCRGroup`.

```
aws resource-groups group-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Di seguito viene mostrato l'output di esempio.

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

Visualizzazione delle prenotazioni di capacità in un gruppo

Per visualizzare l'oggetto Prenotazioni di capacità in un gruppo specifico

Usa il list-group-resources AWS CLI comando. Per `group`, specificare il nome del gruppo.

Ad esempio, il comando seguente elenca le Prenotazioni di capacità in un gruppo denominato `MyCRGroup`.

```
aws resource-groups list-group-resources --group MyCRGroup
```

Di seguito viene mostrato l'output di esempio.

```
{
    "QueryErrors": [],
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
```

```
    ]
}
```

> **Note**
>
> L'output del comando include le prenotazioni di capacità di cui sei proprietario e le prenotazioni di capacità condivise con te.

Visualizzazione dei gruppi ai quali appartiene una prenotazione di capacità

AWS CLI

Visualizzazione dei gruppi ai quali è stata aggiunta una prenotazione di capacità specifica

Usa il AWS CLI comando get-groups-for-capacity-reservation.

Ad esempio, il comando seguente elenca i gruppi ai quali Prenotazione di capacità `cr-1234567890abcdef1` è stato aggiunto.

```
aws ec2 get-groups-for-capacity-reservation --capacity-reservation-
id cr-1234567890abcdef1
```

Di seguito viene mostrato l'output di esempio.

```
{
    "CapacityReservationGroups": [
        {
            "OwnerId": "123456789012",
            "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/
MyCRGroup"
        }
    ]
}
```

> **Note**
>
> Se specifichi una prenotazione di capacità condivisa con te, il comando restituisce solo i gruppi di prenotazioni di capacità di tua proprietà.

Amazon EC2 console

Visualizzazione dei gruppi ai quali è stata aggiunta una prenotazione di capacità specifica

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Prenotazioni di capacità, selezionare la Prenotazione di capacità da visualizzare, quindi scegliere View (Visualizza).

   I gruppi a cui la Prenotazione di capacità è stata aggiunta sono elencati nella scheda Groups (Gruppi).

> **Note**
>
> Se scegli una prenotazione di capacità condivisa con te, la console visualizza solo i gruppi di prenotazioni di capacità di tua proprietà.

Rimozione di una prenotazione di capacità da un gruppo

Per rimuovere una Prenotazione di capacità da un gruppo

Utilizzare il comando AWS CLI ungroup-resources. Per `group`, specificare l'ARN del gruppo da cui rimuovere l'Prenotazione di capacità e per `resources` specificare gli ARN delle Prenotazioni di capacità da rimuovere. Per rimuovere più Prenotazioni di capacità, separare gli ARN con uno spazio.

Nell'esempio seguente vengono rimosse due Prenotazioni di capacità da un gruppo denominato `MyCRGroup`.

```
aws resource-groups ungroup-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Di seguito viene mostrato l'output di esempio.

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
```

```
    ]
}
```

Eliminazione di un gruppo di prenotazione di capacità

Per eliminare un gruppo

Utilizzate il comando delete-group. AWS CLI Per `group`, fornire il nome del gruppo da eliminare.

Ad esempio, il comando seguente elimina un gruppo denominato `MyCRGroup`.

```
aws resource-groups delete-group --group MyCRGroup
```

Di seguito viene mostrato l'output di esempio.

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

Le Prenotazioni della capacità in gruppi di collocazione cluster.

È possibile creare prenotazioni della capacità in un gruppo di collocazione cluster per prenotare la capacità di elaborazione Amazon EC2 per i propri carichi di lavoro. I gruppi di collocazione dei cluster offrono il vantaggio di una bassa latenza di rete e di un elevato throughput di rete.

La creazione di una prenotazione della capacità in un gruppo di collazione cluster garantisce l'accesso alla capacità di calcolo nei gruppi di collocazione del cluster quando necessario, per tutto il tempo necessario. Questo è ideale per prenotare capacità per carichi di lavoro HPC (High Performance) che richiedono un dimensionamento di elaborazione. Consente di dimensionare il cluster garantendo al contempo che la capacità rimanga disponibile per l'utilizzo in modo da poter scalare il backup quando necessario.

Argomenti

- Limitazioni
- Utilizzo di prenotazioni della capacità nei gruppi di collocazione cluster

Limitazioni

Tenere presente quanto segue quando si creano Prenotazioni della capacità nei gruppi di collocazione cluster:

- Se una prenotazione di capacità esistente non fa parte di un gruppo di collocamento, non è possibile modificare la prenotazione di capacità per riservare la capacità in un gruppo di collocamento. Per prenotare la capacità in un gruppo di collocazione, è necessario creare la Prenotazione della capacità nel gruppo di collocazione.
- Dopo aver creato una prenotazione della capacità in un gruppo di collocazione, non è possibile modificarla per prenotare la capacità al di fuori del gruppo di collocazione.
- È possibile aumentare la capacità riservata in un gruppo di collocazione modificando una prenotazione della capacità esistente nel gruppo di collocazione o creando prenotazioni della capacità aggiuntive nel gruppo di collocazione. Tuttavia, si aumentano le possibilità di ottenere un errore di capacità insufficiente.
- Non è possibile condividere prenotazioni della capacità create in un gruppo di collocazione cluster.
- Non puoi eliminare un gruppo di collocazione cluster con prenotazioni della capacità `active`. Devi annullare tutte le prenotazioni della capacità nel gruppo di collocazione cluster prima di poterlo eliminare.

Utilizzo di prenotazioni della capacità nei gruppi di collocazione cluster

Per iniziare a utilizzare le Prenotazioni della capacità con i gruppi di collocazione cluster, attenersi alla seguente procedura.

> **Note**
>
> Se si desidera creare una prenotazione della capacità in un gruppo di collocazione cluster esistente, saltare il passaggio 1. Quindi, per i passaggi 2 e 3, specificare l'ARN del gruppo di collocazione cluster esistente. Per informazioni su come trovare l'ARN del gruppo di collocamento del cluster esistente, vedere. Visualizzate le informazioni sul gruppo di collocamento

Argomenti

- Fase 1: (facoltativo) creazione di un gruppo di collocazione cluster da utilizzare con una prenotazione della capacità

- Fase 2: creazione di una prenotazione della capacità in un gruppo di collocazione cluster
- Fase 3: avvio di istanze in un gruppo di collocazione cluster

Fase 1: (facoltativo) creazione di un gruppo di collocazione cluster da utilizzare con una prenotazione della capacità

Eseguire questo passaggio solo se è necessario creare un nuovo gruppo di collocazione cluster. Per utilizzare un gruppo di collocazione cluster esistente, saltare questo passaggio e quindi per i passaggi 2 e 3, utilizzare l'ARN di quel gruppo di collocazione cluster. Per informazioni su come trovare l'ARN del gruppo di collocamento del cluster esistente, vedere. Visualizzate le informazioni sul gruppo di collocamento

È possibile creare un gruppo di collocazione cluster utilizzando uno dei metodi descritti di seguito.

Console

Per creare un gruppo di collocazione cluster tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Placement Groups (Gruppi di collocazione), quindi Create Placement Group (Crea gruppo di collocazione).
3. Per Name (Nome), specificare un nome descrittivo per il gruppo di collocazione.
4. Per Placement Strategy (Strategia di collocazione), scegliere Cluster.
5. Seleziona Crea gruppo.
6. Nella tabella Gruppi di posizionamento, nella colonna Group ARN, annota l'ARN del gruppo di posizionamento del cluster che hai creato. Ti servirà per la fase successiva.

AWS CLI

Per creare un gruppo di posizionamento del cluster utilizzando il AWS CLI

Utilizza il comando create-placement-group. Per `--group-name`Name (Nome), specificare un nome descrittivo per il gruppo di collocazione, e per `--strategy`, specificare `cluster`.

Nell'esempio seguente viene creato un gruppo di collocazione denominato `MyPG` che utilizza la strategia di collocazione `cluster`.

```
aws ec2 create-placement-group \
```

```
    --group-name MyPG \
    --strategy cluster
```

Prendere nota del gruppo di collocazione ARN restituito nell'output del comando, perché sarà necessario per il passaggio successivo.

Fase 2: creazione di una prenotazione della capacità in un gruppo di collocazione cluster

È possibile creare una prenotazione della capacità in un gruppo di collocazione cluster nello stesso modo in cui si crea qualsiasi prenotazione della capacità. Tuttavia, è necessario specificare anche l'ARN del gruppo di collocazione cluster in cui creare la prenotazione della capacità. Per ulteriori informazioni, consulta Creazione di una Prenotazione di capacità.

Considerazioni

- Il gruppo di collocazione cluster specificato deve trovarsi nello stato `available`. Se il gruppo di collocazione cluster è nello stato `pending`, `deleting`, o `deleted`, la richiesta avrà esito negativo.
- La prenotazione della capacità e il gruppo di collocazione cluster devono essere nella stessa zona di disponibilità. Se la richiesta di creazione della prenotazione di capacità specifica una zona di disponibilità diversa da quella del gruppo di collocazione cluster, la richiesta avrà esito negativo.
- È possibile creare prenotazioni della capacità solo per i tipi di esempio supportati dai gruppi di collocazione cluster. Se si specifica un tipo di istanza non supportato, la richiesta avrà un esito negativo. Per ulteriori informazioni, consulta Regole e limitazioni del gruppo di collocazione cluster.
- Se si crea un prenotazione della capacità `open` in un gruppo di collocazione cluster e esistono istanze in esecuzione esistenti con attributi corrispondenti (gruppo di collocazione ARN, tipo di istanza, zona di disponibilità, piattaforma e tenancy), tali istanze vengono eseguite automaticamente nella prenotazione della capacità.
- La richiesta di creare una Prenotazione di capacità ha esito negativo se una selle seguenti condizioni è true:
  - Amazon EC2 non dispone di capacità sufficiente per soddisfare la richiesta. Provare in un momento successivo, provare una zona di disponibilità differente o provare una capacità inferiore. Se l'applicazione è flessibile su più tipi di istanza e dimensioni, provare con attributi di istanza differenti.
  - La quantità richiesta supera il limite Istanza on demand per la famiglia di istanze selezionata. Incrementare il limite Istanza on demand per la famiglia di istanze e riprovare. Per ulteriori informazioni, consulta Quote di istanze on demand.

È possibile creare un gruppo di collocazione cluster utilizzando uno dei metodi descritti di seguito.

Console

Come creare una Prenotazione di capacità utilizzando la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Prenotazioni della capacità, quindi Create Prenotazione di capacità (Crea Prenotazione di capacità).
3. Nella pagina Crea una prenotazione di capacità, specifica il tipo di istanza, la piattaforma, la zona di disponibilità, la tenancy, la quantità e la data di fine, in base alle esigenze.
4. Per Gruppo di collocamento, selezionare l'ARN del gruppo di collocamento del cluster in cui creare la prenotazione di capacità.
5. Scegli Create (Crea).

Per ulteriori informazioni, consulta Creazione di una Prenotazione di capacità.

AWS CLI

Per creare una prenotazione di capacità utilizzando il AWS CLI

Utilizza il comando create-capacity-reservation. In `--placement-group-arn`, specificare l'ARN del gruppo di collocazione cluster in cui creare la prenotazione della capacità.

```
$ aws ec2 create-capacity-reservation \
    --instance-type instance_type \
    --instance-platform platform \
    --availability-zone az \
    --instance-count quantity \
    --placement-group-arn placement_group_ARN
```

Per ulteriori informazioni, consulta Creazione di una Prenotazione di capacità.

Fase 3: avvio di istanze in un gruppo di collocazione cluster

Si avvia un'istanza in una prenotazione della capacità in un gruppo di collocazione cluster nello stesso modo in cui si avvia un'istanza in qualsiasi prenotazione della capacità. Tuttavia, è necessario specificare anche l'ARN del gruppo di collocazione cluster in cui si avvia l'istanza. Per ulteriori informazioni, consulta Creazione di una Prenotazione di capacità.

Considerazioni

- Se la prenotazione della capacità è `open`, non è necessario specificare la prenotazione della capacità nella richiesta di avvio dell'istanza. Se l'istanza ha attributi (gruppo di collocazione ARN, tipo di istanza, zona di disponibilità, piattaforma e tenancy) che corrispondono a un prenotazione della capacità in un specifico gruppo di collocazione, l'istanza viene eseguita automaticamente nella prenotazione della capacità.
- Se la prenotazione della capacità accetta solo avvii di istanze con destinazione, è necessario specificare la prenotazione della capacità di destinazione oltre al gruppo di collocazione cluster nella richiesta.
- Se la prenotazione della capacità è in un gruppo di prenotazione della capacità, è necessario specificare la prenotazione della capacità di destinazione oltre al gruppo di collocazione cluster nella richiesta. Per ulteriori informazioni, consulta Utilizzo di Prenotazione di capacità con i gruppi.

È possibile avviare un'istanza in una prenotazione della capacità in un gruppo di collocazione cluster utilizzando uno dei metodi descritti di seguito.

Console

Come avviare istanze in una Prenotazione di capacità esistente utilizzando la console

1. Segui la procedura per avviare un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per specificare le impostazioni per il gruppo di collocamento e la prenotazione della capacità.
2. Espandi i dettagli avanzati ed esegui le seguenti operazioni:

   a. Per Gruppo di posizionamento, selezionate il gruppo di posizionamento del cluster in cui avviare l'istanza.

   b. Per Capacity Reservation (Prenotazione della capacità), scegliere una delle seguenti opzioni a seconda della configurazione della prenotazione della capacità:

      - Apri: consente di avviare le istanze in qualsiasi riserva `open` di capacità nel gruppo di posizionamento del cluster che abbia attributi corrispondenti e una capacità sufficiente.
      - Target by ID: per avviare le istanze in una Capacity Reservation che accetta solo lanci di istanze mirati.
      - Target per gruppo: per avviare le istanze in qualsiasi riserva di capacità con attributi e capacità disponibili corrispondenti nel gruppo di prenotazione di capacità selezionato.

3. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Per ulteriori informazioni, consultare Avvio di istanze in una Prenotazione di capacità esistente.

AWS CLI

Per avviare le istanze in una prenotazione di capacità esistente utilizzando il AWS CLI

Utilizzare il comando run-instances. Se è necessario indirizzare una prenotazione della capacità specifica o un gruppo di prenotazione della capacità specifico, specificare il parametro `--capacity-reservation-specification`. Per `--placement`, specificare il parametro `GroupName` e quindi specificare il nome del gruppo di collocazione creato nelle fasi precedenti.

Il seguente comando avvia un'istanza in una prenotazione della capacità `targeted` in un gruppo di collocazione cluster.

```
$ aws ec2 run-instances \
    --image-id ami_id \
    --count quantity \
    --instance-type instance_type \
    --key-name key_pair_name \
    --subnet-id subnetid \
    --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
    --placement "GroupName=cluster_placement_group_name"
```

Per ulteriori informazioni, consulta Avvio di istanze in una Prenotazione di capacità esistente.

Prenotazioni della capacità in zone locali

Una zona locale è un'estensione di una AWS regione geograficamente vicina agli utenti. Le risorse create in una Local Zone possono servire gli utenti locali con comunicazioni a latenza molto bassa. Per ulteriori informazioni, consulta AWS Local Zones.

È possibile estendere un VPC dalla sua AWS regione principale a una zona locale creando una nuova sottorete in quella zona locale. Quando si crea una sottorete in una Local Zone, il VPC viene esteso anche a tale Local Zone. La sottorete nella Local Zone funziona allo stesso modo delle altre sottoreti nel VPC.

Utilizzando le Local Zones, è possibile collocare Prenotazioni di capacità in più posizioni più vicine agli utenti. È possibile creare e utilizzare Prenotazioni di capacità in Local Zones nello stesso modo in cui si crea e si utilizza Prenotazioni di capacità nelle normali zone di disponibilità. Si applicano le stesse caratteristiche e il comportamento di corrispondenza delle istanze. Per ulteriori informazioni sui modelli di determinazione dei prezzi supportati nelle Local Zones, consultare Domande frequenti sulle Local Zones AWS.

Considerazioni

Non è possibile utilizzare gruppi Prenotazione di capacità in una Local Zone.

Utilizzo di un Prenotazione di capacità in una Local Zone

1. Abilita la zona locale per l'uso nel tuo AWS account. Per ulteriori informazioni, consulta Adesione alle Local Zones.
2. Creare una prenotazione di capacità nella Local Zone. Per Availability Zone (Zona di disponibilità), scegli la Local Zone. La zona locale è rappresentata da un codice AWS regionale seguito da un identificatore che indica la posizione, ad esempio`us-west-2-lax-1a`. Per ulteriori informazioni, consulta Creazione di una Prenotazione di capacità.
3. Creare una sottorete nella Local Zone. Per Availability Zone (Zona di disponibilità), scegli la Local Zone. Per ulteriori informazioni, consulta Creazione di una sottorete nel VPC nella Guida per l'utente di Amazon VPC.
4. Avvia un'istanza. Per Subnet (Sottorete), scegliere la sottorete nella Local Zone (ad esempio `subnet-123abc | us-west-2-lax-1a`), e per Capacity Reservation (Prenotazione di capacità), scegliere la specifica (`open` o la destinazione per ID) necessaria per la Prenotazione di capacità creata nella Local Zone. Per ulteriori informazioni, consulta Avvio di istanze in una Prenotazione di capacità esistente.

Prenotazioni della capacità nelle zone Wavelength

AWS Wavelength consente agli sviluppatori di creare applicazioni che offrono latenze molto basse a dispositivi mobili e utenti finali. Wavelength distribuisce servizi di calcolo e storage standard di AWS all'edge delle reti 5G dei provider all'avanguardia nei servizi di telecomunicazione. Puoi estendere un Amazon Virtual Private Cloud (VPC) a una o più zone Wavelength. Puoi quindi utilizzare AWS risorse come le istanze Amazon EC2 per eseguire applicazioni che richiedono una latenza estremamente bassa e una connessione ai AWS servizi della regione. Per maggiori informazioni, consultare Zone AWS Wavelength.

Quando si creano Prenotazioni di capacità on demand, è possibile scegliere la zona Wavelength e avviare istanze in una Prenotazione di capacità in una zona Wavelength specificando la sottorete associata a tale zona Wavelength. Una zona Wavelength è rappresentata da un codice regione AWS seguito da un identificatore che indica la posizione, ad esempio `us-east-1-wl1-bos-wlz-1`.

Le zone Wavelength non sono disponibili in tutte le regioni. Per informazioni sulle regioni che supportano le zone Wavelength, consulta Zone Wavelength disponibili nella Guida per gli sviluppatori di AWS Wavelength .

Considerazioni

Non è possibile utilizzare gruppi Prenotazione di capacità in una zona Wavelength.

Utilizzo di un Prenotazione di capacità in una zona Wavelength

1. Abilita la Wavelength Zone per utilizzarla nel tuo account. AWS Per ulteriori informazioni, consulta the section called “Abilitazione delle zone Wavelength”.
2. Creare una Prenotazione di capacità nella zona Wavelength. Per Zona di disponibilità, scegli Wavelength. Il Wavelength è rappresentato da AWS un codice regionale seguito da un identificatore che indica la posizione, ad esempio. `us-east-1-wl1-bos-wlz-1` Per ulteriori informazioni, consulta Creazione di una Prenotazione di capacità.
3. Crea una sottorete nella zona Wavelength. Per Zona di disponibilità, scegli la zona Wavelength. Per ulteriori informazioni, consulta Creazione di una sottorete nel VPC nella Guida per l'utente di Amazon VPC.
4. Avvia un'istanza. Per Subnet (Sottorete), scegliere la sottorete nella zona Wavelength (ad esempio `subnet-123abc | us-east-1-wl1-bos-wlz-1`), e per Prenotazione di capacità, scegliere la specifica (`open` o la destinazione per ID) necessaria per la Prenotazione di capacità creata nella Wavelength. Per ulteriori informazioni, consulta Avvio di istanze in una Prenotazione di capacità esistente.

Prenotazioni di capacità su AWS Outposts

AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura, i servizi, le API e gli strumenti alle sedi dei clienti. Fornendo l'accesso locale all'infrastruttura AWS gestita, AWS Outposts consente ai clienti di creare ed eseguire applicazioni in locale utilizzando le stesse interfacce di programmazione AWS delle regioni, utilizzando al contempo risorse di elaborazione e archiviazione locali per esigenze di elaborazione dati locali e latenza inferiori.

Un Outpost è un pool di capacità di AWS elaborazione e archiviazione distribuito presso la sede di un cliente. AWS gestisce, monitora e gestisce questa capacità come parte di una regione. AWS

È possibile creare Prenotazioni di capacità sugli Outpost creati nel tuo account. Questo ti permette di riservare capacità di calcolo su un Outpost presso il tuo sito. È possibile creare e utilizzare Prenotazioni di capacità negli Outpost nello stesso modo in cui si crea e si utilizzano le Prenotazioni di capacità nelle normali zone di disponibilità. Si applicano le stesse caratteristiche e il comportamento di corrispondenza delle istanze.

Puoi anche condividere le prenotazioni di capacità su Outposts con altri AWS account all'interno della tua organizzazione utilizzando. AWS Resource Access Manager Per informazioni sulla condivisione delle prenotazioni di capacità, consulta Utilizzo degli Prenotazioni di capacità condivisi.

Prerequisito

Devi avere un Outpost installato presso il tuo sito. Per ulteriori informazioni, consulta Creazione di un Outpost e ordinazione della capacità Outpost nella Guida per l'utente di AWS Outposts .

Considerazioni

- Non è possibile utilizzare gruppi Prenotazione di capacità in un Outpost.

Per utilizzare una Prenotazione di capacità in un Outpost

1. Creare una sottorete nell'Outpost. Per ulteriori informazioni, consulta Creazione di una sottorete nella Guida per l'utente di AWS Outposts .
2. Creare una prenotazione di capacità nell'Outpost.
   a. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
   b. Nel pannello di navigazione, selezionare Outposts e quindi Actions (Operazioni), Create Capacity Reservation (Crea prenotazione di capacità).
   c. Configurare la Prenotazione di capacità in base alle esigenze, quindi scegliere Create (Crea). Per ulteriori informazioni, consulta Creazione di una Prenotazione di capacità.

      > **Note**
      >
      > Il menu a discesa Instance Type (Tipo di istanza) elenca solo i tipi di istanza supportati dall'Outpost selezionato, mentre Availability zone (Zona di disponibilità) elenca solo la zona di disponibilità a cui è associato l'Outpost selezionato.

3. Avviare un'istanza in una Prenotazione di capacità Per Subnet (Sottorete), selezionare la sottorete creata alla fase 1 e per Capacity Reservation (Prenotazione di capacità) selezionare la Prenotazione di capacità creata alla fase 2. Per ulteriori informazioni, consulta Avvio di un'istanza sull'Outpost nella Guida per l'utente di AWS Outposts .

Utilizzo degli Prenotazioni di capacità condivisi

La condivisione della capacità di prenotazione consente ai proprietari di una prenotazione di capacità di condividere la propria capacità riservata con altri AWS account o all'interno di un' AWS organizzazione. Ciò consente di creare e gestire le prenotazioni di capacità centralmente e di condividere la capacità riservata tra più AWS account o all'interno AWS dell'organizzazione.

In questo modello, l' AWS account proprietario della Capacity Reservation (proprietario) la condivide con altri AWS account (consumatori). I consumatori possono avviare le istanze in Prenotazioni di capacità condivise con loro nello steso modo in cui le avvierebbero in Prenotazioni di capacità di cui sono proprietari nel proprio account. Il proprietario Prenotazione di capacità è responsabile della gestione di Prenotazione di capacità e delle istanze avviate in esso. I proprietari non possono modificare le istanze che i consumatori avviano in Prenotazioni di capacità che hanno condiviso. I consumatori sono responsabili della gestione delle istanze che avviano in Prenotazioni di capacità condivisi con loro. I consumatori non possono visualizzare o modificare le istanze di proprietà di altri consumatori o del proprietario Prenotazione di capacità.

Un proprietario Prenotazione di capacità può condividere Prenotazione di capacità con:

- AWS Account specifici all'interno o all'esterno dell' AWS organizzazione
- Un'unità organizzativa all'interno della sua AWS organizzazione
- La sua intera AWS organizzazione

Indice

- Visualizzazione dell'utilizzo condiviso della Prenotazione di capacità
- Autorizzazioni di Prenotazione di capacità condivise
- Fatturazione e misurazione
- Limiti di istanze

Prerequisiti per la condivisione di Prenotazioni di capacità

- Per condividere una prenotazione di capacità, devi averla nel tuo AWS account. Non è possibile condividere un Prenotazione di capacità che è stato condiviso con te.
- È possibile condividere solo Prenotazioni di capacità per istanze con tenancy condivise. Non è possibile condividere Prenotazioni di capacità per istanze dedicate a tenancy singola.
- La condivisione della capacità di prenotazione non è disponibile per AWS i nuovi account o per AWS gli account con una cronologia di fatturazione limitata.
- Per condividere una prenotazione di capacità con la propria AWS organizzazione o un'unità organizzativa AWS all'interno dell'organizzazione, è necessario abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilita la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .

Servizi correlati

La condivisione di Capacity Reservation si integra con AWS Resource Access Manager (AWS RAM). AWS RAM è un servizio che ti consente di condividere AWS le tue risorse con qualsiasi AWS account o tramite AWS Organizations. Con AWS RAM, condividi le risorse di tua proprietà creando una condivisione di risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori possono essere singoli AWS account, unità organizzative o un'intera organizzazione AWS Organizations.

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Condivisione tra zone di disponibilità

Per garantire che le risorse vengano distribuite tra le zone di disponibilità di una regione, mappiamo in modo indipendente le zone di disponibilità ai nomi per ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la zona `us-east-1a` di disponibilità del tuo AWS account potrebbe non avere la stessa posizione `us-east-1a` di un altro AWS account.

Per individuare la posizione di Prenotazioni di capacità relativamente ai tuoi account, devi utilizzare l'ID della zona di disponibilità (ISD AZ). L'ID AZ è un identificatore univoco e coerente per una zona di disponibilità per tutti gli AWS account. Ad esempio, `use1-az1` è un ID AZ per la `us-east-1` regione ed è la stessa posizione in ogni AWS account.

Per visualizzare gli ID AZ per le zone di disponibilità nell'account

1. Apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram.
2. Gli ID AZ per la regione attuale vengono visualizzati nel pannello Il tuo ID AZ sul lato destro dello schermo.

Condivisione di una Prenotazione di capacità

Quando condividi una prenotazione di capacità che possiedi con altri AWS account, consenti loro di avviare istanze nella tua capacità riservata. Se condividi una Prenotazione di capacità aperta, tieni a mente quanto segue, poiché potrebbe portare a un utilizzo indesiderato di Prenotazione di capacità:

- Se i consumatori hanno istanze in esecuzione che corrispondono agli attributi di Prenotazione di capacità, il parametro `CapacityReservationPreference` impostato su `open` e non sono ancora in esecuzione nella capacità riservata, utilizzano automaticamente la Prenotazione di capacità condivisa.
- Se i consumatori avviano istanze con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e hanno il `CapacityReservationPreference` parametro impostato su`open`, si avviano automaticamente nella riserva di capacità condivisa.

Per condividere Prenotazione di capacità, devi aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che ti consente di condividere le tue risorse tra AWS account. Un condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise. Quando condividi Prenotazione di capacità tramite la console Amazon EC2, l'aggiungi a una condivisione risorse esistente. Per aggiungere la Prenotazione di capacità a una nuova condivisione di risorse, devi creare la condivisione di risorse utilizzando la console AWS RAM.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene concesso l'accesso alla riserva di capacità condivisa se i requisiti per la condivisione sono soddisfatti. Se la Prenotazione della capacità è condivisa con account esterni, i consumatori ricevono un invito a unirsi alla condivisione di risorse e viene loro concesso l'accesso alla Prenotazione di capacità condivisa una volta accettato l'invito.

> **Important**
>
> Prima di avviare le istanze in una prenotazione di capacità condivisa con te, verifica di avere accesso alla prenotazione di capacità condivisa visualizzandola nella console o descrivendola utilizzando il comando. describe-capacity-reservations AWS CLI Se riesci a visualizzare la prenotazione di capacità condivisa nella console o a descriverla utilizzando il AWS CLI, è disponibile all'uso e puoi avviare istanze al suo interno. Se tenti di avviare istanze nella Prenotazione della capacità e non questa è accessibile a causa di un errore di condivisione, le istanze verranno avviate in capacità on demand.

Puoi condividere la Prenotazione della capacità di cui sei proprietario tramite la console Amazon EC2, la console AWS RAM o AWS CLI.

Per condividere Prenotazione di capacità di cui sei proprietario utilizzando la console Amazon EC2.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Scegliere Prenotazione di capacità per condividere e scegliere Azioni, Condividi prenotazione.
4. Selezionare la condivisione di risorse a cui aggiungere Prenotazione di capacità e scegliere Condividi Prenotazione di capacità.

   Prima dell'accesso a Prenotazione di capacità condiviso possono essere necessari alcuni minuti.

Per condividere una prenotazione di capacità di tua proprietà utilizzando la console AWS RAM

Consulta Creazione di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per condividere una prenotazione di capacità di tua proprietà utilizzando il AWS CLI

Utilizza il comando create-resource-share.

Interrompere la condivisione di una Prenotazione di capacità

Il proprietario Prenotazione di capacità può interrompere la condivisione di una Prenotazione di capacità in qualsiasi momento. Si applicano le regole seguenti:

- Le istanze di proprietà dei consumatori in esecuzione nella capacità condivisa nel momento in cui la condivisione viene annullata continuano a essere eseguite normalmente al di fuori della capacità

prenotata e la capacità viene ripristinata a Prenotazione di capacità soggetta a disponibilità della capacità Amazon EC2.

- I consumatori con cui è stato condiviso Prenotazione di capacità non possono più avviare nuove istanze nella capacità prenotata.

Per interrompere la condivisione di una Prenotazione di capacità di un utente, è necessario rimuoverla dalla condivisione risorse. È possibile effettuare tale operazione mediante la console Amazon EC2, la console AWS RAM o la AWS CLI.

Per interrompere la condivisione di una Prenotazione di capacità di un utente tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Selezionare la Prenotazione di capacità e scegliere la scheda Condivisione.
4. La scheda Condivisione elenca le condivisioni di risorse a cui Prenotazione di capacità è stato aggiunto. Selezionare la condivisione di risorse da cui eliminare Prenotazione di capacità e selezionare Elimina dalla condivisione di risorse.

Per interrompere la condivisione di una prenotazione di capacità di tua proprietà utilizzando la AWS RAM console

Consulta Aggiornamento di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per interrompere la condivisione di una prenotazione di capacità di cui sei proprietario, utilizza il AWS CLI

Utilizza il comando disassociate-resource-share.

Identificazione e visualizzazione di una Prenotazione di capacità

> **Important**
>
> Prima di avviare le istanze in una Prenotazione della capacità condivisa con te, verifica di avervi accesso visualizzandola nella console o descrivendola utilizzando la AWS CLI. Se riesci a visualizzare la prenotazione di capacità condivisa nella console o a descriverla utilizzando il AWS CLI, è disponibile all'uso e puoi avviare istanze al suo interno. Se tenti di

avviare istanze nella Prenotazione della capacità e questa non è accessibile a causa di un errore di condivisione, l'istanza verrà avviata in capacità on demand.

Proprietari e consumatori possono identificare e visualizzare Prenotazioni di capacità condivise tramite la console Amazon EC2 e la AWS CLI.

Per individuare un Prenotazione di capacità condiviso tramite la console Amazon EC2.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati). La schermata elenca i Prenotazioni di capacità di cui sei proprietario e i Prenotazioni di capacità che sono condivisi con te. La colonna Proprietario mostra l'ID dell' AWS account del proprietario della Capacity Reservation. `(me)`accanto all'ID AWS dell'account indica che sei il proprietario.

Per identificare una prenotazione di capacità condivisa utilizzando il AWS CLI

Utilizza il comando describe-capacity-reservations. Il comando restituisce le prenotazioni di capacità di cui sei proprietario e le prenotazioni di capacità condivise con te. `OwnerId`mostra l'ID dell' AWS account del proprietario della Capacity Reservation.

Visualizzazione dell'utilizzo condiviso della Prenotazione di capacità

Il proprietario della Prenotazione della capacità condivisa può visualizzarne l'uso in qualsiasi momento tramite la console Amazon EC2 e AWS CLI.

Per visualizzare l'utilizzo Prenotazione di capacità tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Selezionare Prenotazione di capacità per il quale visualizzare l'utilizzo e scegliere la scheda Utilizzo.

   La colonna ID account AWS mostra gli ID degli account dei consumatori che attualmente utilizzano la Prenotazione di capacità. La colonna Istanze avviate mostra il numero di istanze che ogni consumatore ha attualmente in esecuzione nella capacità prenotata.

Per visualizzare l'utilizzo di Capacity Reservation utilizzando il AWS CLI

Usare il get-capacity-reservation-usagecomando. `AccountId`mostra l'ID dell'account che utilizza la prenotazione della capacità. `UsedInstanceCount`mostra il numero di istanze che il consumatore ha attualmente in esecuzione nella capacità riservata.

Autorizzazioni di Prenotazione di capacità condivise

Autorizzazioni per i proprietari

I proprietari sono responsabili della gestione e dell'annullamento dei loro Prenotazioni di capacità condivisi. I proprietari non possono modificare le istanze in esecuzione nel Prenotazione di capacità condiviso di proprietà di altri account. I proprietari sono comunque responsabili della gestione delle istanze che avviano nel Prenotazione di capacità condiviso.

Autorizzazioni per i consumatori

I consumatori sono responsabili della gestione delle istanze in esecuzione nell'Prenotazione di capacità condiviso. I consumatori non possono modificare l'Prenotazione di capacità condiviso in nessun modo e non possono visualizzare o modificare le istanze di proprietà di altri consumatori o del proprietario di Prenotazione di capacità.

Fatturazione e misurazione

Non sono previsti costi aggiuntivi per la condivisione di Prenotazioni di capacità.

Al proprietario di Prenotazione di capacità vengono fatturate le istanze eseguite all'interno di Prenotazione di capacità e la capacità prenotata non utilizzata. I consumatori sono fatturati in base alle istanze che eseguono all'interno dell'Prenotazione di capacità condiviso.

Se il titolare della prenotazione della capacità appartiene a un account pagante diverso e la prenotazione della capacità è coperta da un'istanza riservata regionale o da un Savings Plan, al proprietario della prenotazione della capacità continuerà a essere fatturata l'istanza riservata regionale o il Savings Plan. In questi casi, il proprietario della prenotazione della capacità paga l'istanza regionale riservata o il Savings Plan e ai consumer vengono fatturati i costi delle istanze eseguite nella prenotazione di capacità condivisa.

Limiti di istanze

Tutti i conteggi di utilizzo Prenotazione di capacità che contribuiscono ai limiti Istanza on demand del proprietario di Prenotazione di capacità. di ripetizione che riesce:

- Capacità prenotata non utilizzata
- Utilizzo da parte delle istanze possedute dal proprietario Prenotazione di capacità

- Utilizzo da parte delle istanze possedute dai consumatori

Istanze inviate nella capacità condivisa dai consumatori contribuiscono al raggiungimento del limite Istanza on demand del proprietario Prenotazione di capacità. I limiti delle istanze dei consumatori sono una somma dei limiti Istanza on demand e della capacità disponibile nel Prenotazioni di capacità condiviso a cui hanno accesso.

Parco istanze prenotazione della capacità

Un Parco istanze di prenotazione della capacità on demand è un gruppo di prenotazione della capacità.

Una richiesta di parco istanze di prenotazione della capacità contiene tutte le informazioni di configurazione necessarie per avviare un parco istanze di prenotazione della capacità. Utilizzando una singola richiesta, puoi prenotare grandi quantità di capacità Amazon EC2 per il tuo carico di lavoro su più tipi di istanze, fino a una capacità di destinazione specificata.

Dopo aver creato un parco istanze di prenotazione della capacità, potrai gestire collettivamente le prenotazione della capacità nel parco istanze, modificandolo o annullandolo.

Argomenti

Come funzionano i parchi istanze di prenotazione della capacità

Quando crei un parco istanze di prenotazione della capacità, questo tenta di creare prenotazioni della capacità individuali per soddisfare la capacità target totale specificata nella richiesta del parco istanze.

Il numero di istanze per cui il parco istanze prenota la capacità dipende dalla capacità target totale e dai pesi del tipo di istanza specificati. Il tipo di istanza per il quale prenota la capacità dipende dalla strategia di allocazione e dalla priorità del tipo di istanza utilizzate.

Se non c'è capacità sufficiente al momento della creazione del parco istanze e questo non è in grado di soddisfare immediatamente la capacità target totale, il parco istanze tenta di creare asincronicamente le prenotazioni della capacità, finché non avrà prenotato la quantità di capacità richiesta.

Quando il parco istanze avrà raggiunto la sua capacità target totale, tenterà di mantenerla. Se una prenotazione della capacità nel parco istanze viene annullata, questo creerà automaticamente una o più prenotazioni della capacità, a seconda della configurazione del parco istanze, per sostituire la capacità persa e mantenere la capacità target totale.

Le prenotazioni della capacità nel parco istanze non possono essere gestite individualmente. Devono essere gestite collettivamente, modificando il parco istanze. Quando modifichi un parco istanze, le prenotazioni della capacità in esso contenute vengono automaticamente aggiornate per riflettere le modifiche.

Attualmente, i parchi istanze di prenotazione della capacità supportano i criteri `open` di corrispondenza delle istanze e tutte le prenotazioni della capacità avviate da un parco istanze utilizzano automaticamente questi criteri di corrispondenza. In base a questi criteri, le nuove istanze e le istanze esistenti con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) vengono eseguite automaticamente nelle prenotazioni di capacità create da un parco veicoli. I parchi istanze di prenotazione della capacità non supportano i criteri di corrispondenza delle istanze `target`.

Considerazioni

Quando utilizzi i parchi istanze di prenotazione della capacità, tieni presente quanto segue:

- Una flotta di prenotazioni di capacità può essere creata, modificata, visualizzata e annullata utilizzando l'API and. AWS CLI AWS
- Le prenotazioni della capacità in un parco istanze non possono essere gestite individualmente. Devono essere gestite collettivamente, modificando o annullando il parco istanze.
- Un parco istanze di prenotazione della capacità non può estendersi in tutte le Regioni.
- Un parco istanze di prenotazione della capacità non può estendersi su più zone di disponibilità.
- Le prenotazioni di capacità create da una flotta di prenotazioni di capacità vengono automaticamente etichettate con il seguente tag AWS generato:
  - Chiave - `aws:ec2-capacity-reservation-fleet`
  - Valore - *`fleet_id`*

È possibile utilizzare questo tag per identificare le prenotazioni della capacità create da un parco istanze di prenotazione della capacità.

Prezzi

Non sono previsti costi aggiuntivi, per l'utilizzo di parchi istanze di prenotazione della capacità. Ti verranno fatturate le singole prenotazioni della capacità create dai parchi istanze di prenotazioni della capacità. Per ulteriori informazioni sulla fatturazione delle prenotazioni della capacità, consulta Prezzi e fatturazione di Prenotazione di capacità.

Concetti sui parchi istanze di prenotazione della capacità

In questo argomento vengono descritti alcuni dei concetti dei parchi istanze di prenotazione della capacità.

Argomenti

- Capacità target totale
- Strategia di allocazione
- Peso del tipo di istanza
- Priorità del tipo di istanza

Capacità target totale

LaCapacità target totale definisce la quantità totale della capacità di calcolo prenotata dal parco istanze di prenotazione della capacità. Specifichi la capacità target totale quando crei il parco istanze di prenotazione della capacità. Dopo la creazione del parco istanze, Amazon EC2 crea automaticamente le prenotazioni della capacità per prenotare la capacità fino al target totale.

Il numero di istanze per cui il parco istanze di prenotazione della capacità prenota la capacità è determinato dalla capacità target totale e dal peso del tipo di istanza specificato per ciascun tipo di istanza nel parco di prenotazione della capacità (`total target capacity/instance type weight=number of instances`).

È possibile assegnare una capacità target totale in base alle unità significative per il carico di lavoro. Ad esempio, se il carico di lavoro richiede un certo numero di vCPU, puoi assegnare la capacità target totale in base al numero di vCPU richieste. Se il carico di lavoro richiede vCPU `2048`, specifica una capacità target totale di `2048` e quindi assegna i pesi del tipo di istanza in base al numero di

vCPU fornite dai tipi di istanza nel parco istanze. Per vedere un esempio, consulta Peso del tipo di istanza.

Strategia di allocazione

La strategia di allocazione del parco istanze di prenotazione della capacità stabilisce il modo in cui questo soddisfa la richiesta di capacità riservata dalle specifiche del tipo di istanza nella configurazione del parco istanze di prenotazione della capacità.

Attualmente, è supportata solo la strategia di allocazione `prioritized`. Con questa strategia, il parco istanze di prenotazione della capacità crea prenotazioni utilizzando le priorità assegnate a ciascuna delle specifiche del tipo di istanza nella configurazione sua configurazione. I valori di priorità inferiori indicano una priorità più elevata per l'uso. Ad esempio, supponiamo di creare un parco istanze di prenotazione della capacità che utilizza i seguenti tipi e priorità di istanza:

- `m4.16xlarge`: priorità = 1
- `m5.16xlarge`: priorità = 3
- `m5.24xlarge`: priorità = 2

Come prima cosa, il parco istanze tenta di creare prenotazioni di capacità per `m4.16xlarge`. Se Amazon EC2 non ha sufficiente capacità `m4.16xlarge`, il parco istanze tenta di creare prenotazioni di capacità per `m5.24xlarge`. Se Amazon EC2 non ha sufficiente capacità `m5.24xlarge`, il parco istanze tenta di creare prenotazioni di capacità per `m5.16xlarge`.

Peso del tipo di istanza

Il peso del tipo di istanza è un peso assegnato a ciascun tipo di istanza nel parco istanze di prenotazione della capacità. Il peso determina quante unità di capacità ciascuna istanza di quel tipo specifico conta verso la capacità target totale del parco istanze.

È possibile assegnare pesi in base a unità significative per il carico di lavoro. Ad esempio, se il carico di lavoro richiede un certo numero di vCPU, è possibile assegnare pesi in base al numero di vCPU fornite da ciascun tipo di istanza nel parco istanze di prenotazione della capacità. In questo caso, se crei un parco istanze di capacità utilizzando `m4.16xlarge` e `m5.24xlarge`, assegnerai pesi corrispondenti al numero di vCPU per ciascuna istanza come segue:

- `m4.16xlarge` — 64 vCPU, peso = 64 unità
- `m5.24xlarge` — 96 vCPU, peso = 96 unità

Il peso del tipo di istanza determina il numero di istanze per cui il parco istanze di prenotazione della capacità prenota quest'ultima. Ad esempio, se un parco istanze di prenotazione della capacità con una capacità target totale di 384 unità utilizza i tipi di istanza e i pesi nell'esempio precedente, il parco istanze potrebbe prenotare capacità per 6 istanze `m4.16xlarge` (384 capacità target totale/peso di 64 tipi di istanze = 6 istanze), oppure 4 istanze `m5.24xlarge`(384/96 = 4).

Se non assegni i pesi del tipo di istanza o se assegni un peso del tipo di istanza di 1, la capacità target totale si baserà esclusivamente sul conteggio delle istanze. Ad esempio, se un parco istanze di prenotazione della capacità con una capacità target totale di 384unità utilizza i tipi di istanza nell'esempio precedente, ma omette i pesi o specifica un peso di 1 per entrambi i tipi di istanza, il parco istanze potrebbe prenotare capacità per 384 istanze `m4.16xlarge` o per 384 istanze `m5.24xlarge`.

Priorità del tipo di istanza

La priorità del tipo di istanza è un valore che assegni ai tipi di istanza nel parco istanze. Le priorità vengono utilizzate per determinare quali tipi di istanza specificati per il parco istanze devono essere assegnati per l'uso.

I valori di priorità inferiori indicano una priorità più elevata per l'uso.

Utilizzo del parco istanze di prenotazione della capacità

Argomenti

Prima di iniziare

Prima di creare un parco istanze di prenotazione della capacità:

1. Determina la quantità di capacità di calcolo necessaria per il carico di lavoro.

2. Decidi i tipi di istanza e le zone di disponibilità che desideri utilizzare.
3. Assegna a ciascun tipo di istanza una priorità in base alle tue esigenze e preferenze. Per ulteriori informazioni, consulta Priorità del tipo di istanza.
4. Crea un sistema di ponderazione della capacità che abbia senso per il tuo carico di lavoro. Assegna un peso a ciascun tipo di istanza e determina la capacità target totale. Per ulteriori informazioni, consulta Peso del tipo di istanza e Capacità target totale.
5. Stabilisci se hai bisogno della prenotazione della capacità a tempo indeterminato o solo per uno specifico periodo di tempo.

Stati del parco istanze di prenotazione della capacità

Un parco istanze di prenotazione della capacità può avere uno dei seguenti stati:

- `submitted`: la richiesta del parco istanze di prenotazione della capacità è stata inviata e Amazon EC2 si sta preparando a creare le prenotazioni della capacità.
- `modifying`: il parco istanze di prenotazione della capacità è in fase di modifica. Il parco istanze rimane in questo stato fino al completamento della modifica.
- `active`: il parco istanze di prenotazione della capacità ha soddisfatto la capacità target totale e sta tentando di mantenerla. Il parco istanze rimane in questo stato finché non viene modificato o eliminato.
- `partially_fulfilled`: il parco istanze di prenotazione della capacità soddisfa parzialmente la capacità target totale. La capacità Amazon EC2 non è sufficiente per soddisfare la capacità target totale. Il parco istanze cerca di soddisfare in modo asincrono la sua capacità target totale.
- `expiring`: il parco istanze di prenotazione della capacità ha raggiunto la data di fine ed è in fase di scadenza. Una o più delle sue prenotazioni di capacità potrebbero essere ancora attive.
- `expired`: il parco istanze di prenotazione della capacità ha raggiunto la data di fine. Il parco istanze e le sue prenotazioni di capacità sono scaduti. Il parco istanze non può creare nuove prenotazioni di capacità.
- `cancelling`: il parco istanze di prenotazione della capacità sta per essere annullato. Una o più delle sue prenotazioni di capacità potrebbero essere ancora attive.
- `cancelled`: il parco istanze di prenotazione della capacità è stato eliminato manualmente. Il parco istanze e le sue prenotazioni di capacità vengono eliminati e il parco istanze non può creare nuove prenotazioni di capacità.
- `failed`: il parco istanze di prenotazione della capacità non è riuscito a prenotare la capacità per i tipi di istanza specificati.

Creazione di un parco istanze di prenotazione della capacità

Quando crei un parco istanze di prenotazione della capacità, questo crea automaticamente le prenotazioni di capacità per i tipi di istanza specificati nella richiesta del parco istanze, fino a raggiungere la capacità target totale specificata. Il numero di istanze per le quali il parco istanze di prenotazione della capacità prenota quest'ultima dipende dalla capacità target totale e dai pesi del tipo di istanza specificati nella richiesta. Per ulteriori informazioni, consulta Peso del tipo di istanza e Capacità target totale.

Quando crei il parco istanze, devi specificare i tipi di istanza da utilizzare e una priorità per ciascuno di questi tipi di istanza. Per ulteriori informazioni, consulta Strategia di allocazione e Priorità del tipo di istanza.

> **Note**
>
> Il ruolo AWSServiceRoleForEC2CapacityReservationFleetcollegato al servizio viene creato automaticamente nel tuo account la prima volta che crei una flotta di prenotazioni di capacità. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per il parco istanze di prenotazione della capacità.

Attualmente, i parchi istanze di prenotazione della capacità supportano solo i criteri `open` di corrispondenza delle istanze.

È possibile creare un parco istanze di prenotazione della capacità solo utilizzando la riga di comando.

Creazione di un parco istanze di prenotazione della capacità

Usa il comando. create-capacity-reservation-fleet AWS CLI

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity capacity_units \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy dedicated|default \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

Di seguito sono riportati i contenuti di `instanceTypeSpecification.json`.

```
[
```

```
    {
        "InstanceType": "instance_type",
        "InstancePlatform":"platform",
        "Weight": instance_type_weight,
        "AvailabilityZone":"availability_zone",
        "AvailabilityZoneId" : "az_id",
        "EbsOptimized": true|false,
        "Priority" : instance_type_priority
    }
]
```

Output previsto.

```
{
    "Status": "status",
    "TotalFulfilledCapacity": fulfilled_capacity,
    "CapacityReservationFleetId": "cr_fleet_id",
    "TotalTargetCapacity": capacity_units
}
```

Esempio

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 24 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-12-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

`instanceTypeSpecification.json`

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

Output di esempio:

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

Visualizzazione di un parco istanze di prenotazione della capacità

È possibile visualizzare le informazioni di configurazione e le capacità per un parco istanze di prenotazione della capacità in qualsiasi momento. La visualizzazione di un parco istanze fornisce anche dettagli sulle singole prenotazioni di capacità all'interno del parco istanze stesso.

È possibile visualizzare un parco istanze di prenotazione della capacità solo tramite la riga di comando.

Come visualizzare un parco istanze di prenotazione della capacità

Usa il describe-capacity-reservation-fleets AWS CLI comando.

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Output previsto

```
{
    "CapacityReservationFleets": [
        {
            "Status": "status",
            "EndDate": "yyyy-mm-ddThh:mm:ss.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "cr_fleet_id",
            "Tenancy": "dedicated|default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr1_id",
                    "AvailabilityZone": "cr1_availability_zone",
                    "FulfilledCapacity": cr1_used_capacity,
                    "Weight": cr1_instance_type_weight,
```

```
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr1_platform",
                    "TotalInstanceCount": cr1_number of instances,
                    "Priority": cr1_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr1_instance_type"
                },
    {
                    "CapacityReservationId": "cr2_id",
                    "AvailabilityZone": "cr2_availability_zone",
                    "FulfilledCapacity": cr2_used_capacity,
                    "Weight": cr2_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr2_platform",
                    "TotalInstanceCount": cr2_number of instances,
                    "Priority": cr2_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr2_instance_type"
                },
            ],
            "TotalTargetCapacity": total_target_capacity,
            "TotalFulfilledCapacity": total_target_capacity,
            "CreateTime": "yyyy-mm-ddThh:mm:ss.000Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

Esempio

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Output di esempio

```
{
    "CapacityReservationFleets": [
        {
            "Status": "active",
            "EndDate": "2021-12-31T23:59:59.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "crf-abcdef01234567890",
```

```
            "Tenancy": "default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr-1234567890abcdef0",
                    "AvailabilityZone": "us-east-1a",
                    "FulfilledCapacity": 5.0,
                    "Weight": 1.0,
                    "CreateDate": "2021-07-02T08:34:33.398Z",
                    "InstancePlatform": "Linux/UNIX",
                    "TotalInstanceCount": 5,
                    "Priority": 1,
                    "EbsOptimized": true,
                    "InstanceType": "m5.xlarge"
                }
            ],
            "TotalTargetCapacity": 5,
            "TotalFulfilledCapacity": 5.0,
            "CreateTime": "2021-07-02T08:34:33.397Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

Modifica di un parco istanze di prenotazione della capacità

È possibile modificare la capacità target totale e la data di un parco istanze di prenotazione della capacità in qualsiasi momento. Quando modifichi la capacità target totale di un parco istanze di prenotazione della capacità, questo crea automaticamente nuove prenotazioni di capacità o modifica o annulla le prenotazioni di capacità esistenti nel parco istanze per soddisfare la nuova capacità target totale. Quando modifichi la data di fine del parco istanze, le date di fine per tutte le singole prenotazioni di capacità vengono aggiornate di conseguenza.

Dopo aver modificato un parco istanze, il suo stato passa a `modifying`. Non è possibile tentare ulteriori modifiche a un parco istanze mentre si trova nello stato `modifying`.

Non è possibile modificare la tenancy, la zona di disponibilità, i tipi di istanza, le piattaforme di istanza, le priorità o i pesi utilizzati da un parco istanze di prenotazione della capacità. Se devi modificare uno di questi parametri, potrebbe essere necessario che tu annulli il parco istanze esistente e crearne uno nuovo con i parametri richiesti.

È possibile modificare un parco istanze di prenotazione delle capacità solo utilizzando la riga di comando.

Come modificare un parco istanze di prenotazione delle capacità

Usa il modify-capacity-reservation-fleet AWS CLI comando.

> **Note**
>
> Non è possibile specificare `--end-date` e `--remove-end-date` nello stesso comando.

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id cr_fleet_ids \
--total-target-capacity capacity_units \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--remove-end-date
```

Output previsto

```
{
    "Return": true
}
```

Esempio: modifica della capacità target totale

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--total-target-capacity 160
```

Esempio: modifica della data di fine

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--end-date 2021-07-04T23:59:59.000Z
```

Esempio: rimozione della data di fine

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--remove-end-date
```

Output di esempio

```
{
    "Return": true
}
```

Annullamento di un parco istanze di prenotazione della capacità

Quando non hai più bisogno di un parco istanze di prenotazione della capacità e della capacità questa prenota, puoi annullarla. Quando annulli un parco istanze, il suo stato cambia in `cancelled` e non può più creare nuove prenotazioni di capacità. Inoltre, tutte le singole prenotazioni di capacità nel parco istanze vengono annullate e le istanze precedentemente in esecuzione nella capacità riservata continuano a funzionare normalmente in capacità condivisa.

È possibile annullare un parco istanze di prenotazione della capacità solo utilizzando la riga di comando.

Come annullare un parco istanze di prenotazione della capacità

Usa il cancel-capacity-reservation-fleet AWS CLI comando.

```
aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Output previsto

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_1"
        },
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_2"
        }
    ],
    "FailedFleetCancellations": [
        {
         "CapacityReservationFleetId": "cr_fleet_id_3",
         "CancelCapacityReservationFleetError": [
             {
```

```
                "Code": "code",
                      "Message": "message"
            }
           ]
      }
     ]
}
```

Esempio: annullamento riuscito

```
aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Output di esempio

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

Esempio di configurazione di un parco istanze di prenotazione della capacità

Argomenti

- Esempio 1: capacità riservata basata su vCPU

Esempio 1: capacità riservata basata su vCPU

Nell'esempio seguente viene creata un parco istanze di prenotazione della capacità che utilizza due tipi di istanza: `m5.4xlarge` e `m5.12xlarge`.

Utilizza un sistema di ponderazione basato sul numero di vCPU fornito dai tipi di istanza specificati. La capacità target totale è di `480` vCPU. `m5.4xlarge` fornisce 16 vCPU e ottiene un peso di 16, mentre `m5.12xlarge` fornisce 48 vCPU e ottiene un peso di 48. Questo sistema di ponderazione configura il parco istanze di prenotazione della capacità in modo da prenotare la capacità per 30 istanze `m5.4xlarge` (480/16=30) o per 10 istanze `m5.12xlarge` (480/48=10).

Il parco istanze è configurato per dare priorità alla capacità `m5.12xlarge` e ottiene la priorità di `1`, mentre `m5.4xlarge`ottiene una priorità inferiore di `2`. Ciò significa che la flotta cercherà di riservare prima la capacità `m5.12xlarge` e farà il tentativo di prenotare `m5.4xlarge` solo se Amazon EC2 non disporrà di sufficiente capacità `m5.12xlarge`.

Il parco istanze prenota la capacità per `Windows` istanze e la prenotazione scade automaticamente il `October 31, 2021` alle `23:59:59` UTC.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 480 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-10-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

Di seguito sono riportati i contenuti di `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 2
    },
    {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
        "Weight": 48,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
 }
]
```

Utilizzo di ruoli collegati ai servizi per il parco istanze di prenotazione della capacità

On-Demand Capacity Reservation Fleet utilizza AWS Identity and Access Management ruoli collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente l

parco istanze di prenotazione della capacità. I ruoli collegati ai servizi sono predefiniti da Capacity Reservation Fleet e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione del parco istanze di prenotazione della capacità, poiché ti permette di evitare di aggiungere manualmente le autorizzazioni necessarie. Il parco istanze di prenotazione della capacità definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo il parco istanze di prenotazione della capacità potrà assumere i suoi ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse del parco istanze di prenotazione della capacità, poiché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Autorizzazioni dei ruoli collegati ai servizi per il parco istanze di prenotazione della capacità

Capacity Reservation Fleet utilizza il ruolo collegato AWSServiceRoleForEC2CapacityReservationFleetai servizi denominato per creare, descrivere, modificare e annullare le prenotazioni di capacità precedentemente create da una flotta di prenotazioni di capacità, per tuo conto.

Il ruolo AWSServiceRoleForEC2CapacityReservationFleet collegato al servizio prevede che la seguente entità assuma il ruolo:. `capacity-reservation-fleet.amazonaws.com`

Il ruolo utilizza la AWSEC2CapacityReservationFleetRolePolicypolitica, che include le seguenti autorizzazioni:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateCapacityReservation",
                "ec2:CancelCapacityReservation",
                "ec2:ModifyCapacityReservation"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:CapacityReservationFleet": "arn:aws:ec2:*:*:capacity-
reservation-fleet/crf-*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateCapacityReservation"
                }
            }
        }
    ]
}
```

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per il parco istanze di prenotazione della capacità

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei una flotta di prenotazioni di capacità utilizzando il `create-capacity-reservation-fleet` AWS CLI comando o l'`CreateCapacityReservationFleet`API, il ruolo collegato al servizio viene creato automaticamente per te.

Se si elimina questo ruolo collegato ai servizi e quindi deve essere creato di nuovo, è possibile utilizzare lo stesso processo per ricreare il ruolo nell'account. Quando crei un parco istanze di prenotazione della capacità, questo crea nuovamente il ruolo collegato ai servizi per tuo conto.

Modifica di un ruolo collegato ai servizi per il parco istanze di prenotazione della capacità

Capacity Reservation Fleet non consente di modificare il ruolo collegato al AWSServiceRoleForEC2CapacityReservationFleet servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per il parco istanze di prenotazione della capacità

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi, prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio parco istanze di prenotazione della capacità utilizza tale ruolo quando provi a eliminare le risorse, è possibile che l'eliminazione abbia esito negativo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare il ruolo collegato al servizio AWSServiceRoleForEC2CapacityReservationFleet

1. Utilizza il `delete-capacity-reservation-fleet` AWS CLI comando o l'`DeleteCapacityReservationFleet`API per eliminare le flotte di prenotazione della capacità dal tuo account.
2. Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForEC2CapacityReservationFleet servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi del parco istanze di prenotazione della capacità

Il parco istanze di prenotazione della capacità supporta l'utilizzo di ruoli collegati ai servizi in tutte le Regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta AWS Regioni ed endpoint di .

Monitoraggio delle prenotazioni di capacità

È possibile utilizzare le seguenti funzionalità per monitorare le prenotazioni di capacità:

Argomenti

- Monitora le prenotazioni di capacità utilizzando le metriche CloudWatch
- Monitora le prenotazioni di capacità utilizzando EventBridge
- Notifiche di utilizzo

Monitora le prenotazioni di capacità utilizzando le metriche CloudWatch

Con le CloudWatch metriche, puoi monitorare in modo efficiente le tue prenotazioni di capacità e identificare la capacità inutilizzata impostando CloudWatch allarmi per avvisarti quando vengono raggiunte le soglie di utilizzo. Questo può aiutare a mantenere un volume Prenotazione di capacità costante e ottenere un livello di utilizzo più elevato.

On-Demand Capacity Reservations invia dati metrici ogni cinque minuti. CloudWatch I parametri non sono supportati per Prenotazioni di capacità che sono attivi per meno di cinque minuti.

Per ulteriori informazioni sulla visualizzazione dei parametri nella CloudWatch console, consulta Using Amazon CloudWatch Metrics. Per ulteriori informazioni sulla creazione di allarmi, consulta Creazione di CloudWatch allarmi Amazon.

Indice

- Parametri di utilizzo Prenotazione di capacità
- Dimensioni dei parametri Prenotazione di capacità
- Visualizza i CloudWatch parametri per le prenotazioni di capacità

Parametri di utilizzo Prenotazione di capacità

Lo spazio dei nomi `AWS/EC2CapacityReservations` include le seguenti metriche di utilizzo che è possibile utilizzare per monitorare e mantenere la capacità su richiesta entro le soglie specificate per la prenotazione.

Parametro	Descrizione
`UsedInstanceCount`	Numero di istanze attualmente in uso. Unità: numero
`AvailableInstanceCount`	Numero di istanze disponibili. Unità: numero
`TotalInstanceCount`	Numero totale di istanze riservate. Unità: numero
`InstanceUtilization`	Percentuale di istanze di capacità riservata attualmente in uso. Unità: percentuale

Dimensioni dei parametri Prenotazione di capacità

È possibile utilizzare le seguenti dimensioni per perfezionare i parametri elencati nella tabella precedente.

Dimensione	Descrizione
`CapacityReservationId`	Questa dimensione univoca a livello globale filtra i dati richiesti solo per la prenotazione di capacità identificata.

Visualizza i CloudWatch parametri per le prenotazioni di capacità

I parametri sono raggruppati in primo luogo in base allo spazio dei nomi del servizio e in secondo luogo in base alle dimensioni supportate. È possibile utilizzare le procedure seguenti per visualizzare i parametri per Prenotazioni di capacità.

Per visualizzare i parametri di prenotazione della capacità utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Se necessario, modificare la regione. Dalla barra di navigazione, selezionare la regione dove si trova Prenotazione di capacità. Per ulteriori informazioni, consultare Regioni ed endpoint.
3. Nel riquadro di navigazione, seleziona Parametri.
4. Per Tutti i parametri, scegliere Prenotazione capacità EC2.
5. Scegliere la dimensione dei parametri Per impegno capacità. I parametri saranno raggruppati per `CapacityReservationId`.
6. Per ordinare i parametri, utilizza l'intestazione della colonna. Per creare il grafico di un parametro, seleziona la casella di controllo accanto al parametro.

Come visualizzare i parametri della Prenotazione della capacità (AWS CLI)

Utilizza il comando list-metrics seguente:

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Monitora le prenotazioni di capacità utilizzando EventBridge

AWS Health invia eventi ad Amazon EventBridge quando una prenotazione di capacità nel tuo account è inferiore al 20% di utilizzo in determinati periodi. Con EventBridge, puoi stabilire regole che attivano azioni programmatiche in risposta a tali eventi. Ad esempio, è possibile creare una regola che annulla automaticamente una prenotazione di capacità quando il suo utilizzo è inferiore al 20% in un periodo di 7 giorni.

Gli eventi in EventBridge sono rappresentati come oggetti JSON. I campi univoci per l'evento sono contenuti nella sezione "detail" dell'oggetto JSON. Il campo "event" contiene il nome dell'evento. Il campo "result" contiene lo stato completato dell'operazione che ha attivato l'evento. Per ulteriori informazioni, consulta i modelli di EventBridge eventi di Amazon nella Amazon EventBridge User Guide.

Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Questa funzionalità non è supportata in AWS GovCloud (US).

Indice

- Crea una EventBridge regola

Eventi

AWS Health invia i seguenti eventi quando l'utilizzo della capacità per una prenotazione di capacità è inferiore al 20 percento.

Eventi

- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION
- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION

Di seguito è riportato un esempio di evento generato quando l'utilizzo della capacità di una prenotazione di capacità appena creata è inferiore al 20% in un periodo di 24 ore.

```
{
    "version": "0",
    "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-10T12:03:38Z",
    "region": "ap-south-1",
    "resources": [
        "cr-01234567890abcdef"
    ],
    "detail": {
        "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
        "eventTypeCategory": "accountNotification",
        "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }
```

```
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef"
            }
        ]
    }
    }
```

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

Di seguito è riportato un esempio di evento generato quando l'utilizzo della capacità di una o più prenotazioni di capacità è inferiore al 20% in un periodo di 7 giorni.

```
{
    "version": "0", "id":"7439d42b-3c7f-ad50-6a88-25e2a70977e2",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-07T06:06:01Z",
    "region": "us-east-1",
    "resources": [
        "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
        "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
        "eventTypeCategory": "accountNotification",
        "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
```

```
            {
                "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/
UNIX | 0.0%"
            },
            {
                "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/
UNIX | 0.0%"
            }
        ]
    }
}
```

Crea una EventBridge regola

Per ricevere notifiche e-mail quando l'utilizzo di Capacity Reservation scende al di sotto del 20%, crea un argomento Amazon SNS, quindi crea EventBridge una regola per l'`AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION`evento.

Creazione dell'argomento Amazon SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel riquadro di navigazione scegliere Argomenti, quindi Crea nuovo argomento.
3. Per Tipo, scegliere Standard.
4. Per Nome argomento, inserisci un nome per il nuovo argomento.
5. Scegli Create topic (Crea argomento).
6. Scegli Crea sottoscrizione.
7. Per Protocollo scegli E-mail, mentre per Endpoint inserisci l'indirizzo e-mail che deve ricevere le notifiche.
8. Scegli Crea sottoscrizione.
9. L'indirizzo e-mail inserito sopra riceverà un messaggio e-mail con l'oggetto seguente: `AWS Notification - Subscription Confirmation`. Segui le istruzioni per confermare la tu sottoscrizione.

Per creare la regola EventBridge

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel riquadro di navigazione scegli Rules (Regole), quindi Create rule (Crea regola).

3. Per Nome, inserisci un nome per la nuova regola.
4. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
5. Seleziona Successivo.
6. Per Modello di eventi, procedi come segue:
    a. Per Origine evento, scegli Servizi AWS .
    b. Per Servizio AWS , scegli AWS Health.
    c. Per Tipo di evento, scegli Notifica di sottoutilizzo prenotazione di capacità on demand EC2.
7. Seleziona Successivo.
8. Per Destinazione 1, esegui queste operazioni:
    a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).
    b. Per Select a target (Seleziona un target), scegli SNS topic (Argomento SNS).
    c. Per Argomento, scegli l'argomento che hai creato in precedenza.
9. Scegli Avanti, quindi scegli di nuovo Avanti.
10. Scegli Crea regola.

Notifiche di utilizzo

AWS Health invia le seguenti e-mail e AWS Health Dashboard notifiche quando l'utilizzo della capacità per Capacity Reservations nel tuo account scende al di sotto del 20 percento.

- Notifiche individuali per ogni prenotazione di capacità appena creata il cui utilizzo è stato inferiore al 20% nelle ultime 24 ore.
- Una notifica riepilogativa per tutte le prenotazioni di capacità il cui utilizzo è stato inferiore al 20% negli ultimi 7 giorni.

Le notifiche e le AWS Health Dashboard notifiche e-mail vengono inviate all'indirizzo e-mail associato all' AWS account proprietario delle prenotazioni di capacità. Le notifiche includono le seguenti informazioni:

- ID della prenotazione di capacità.
- La zona di disponibilità della prenotazione di capacità.
- Il tasso medio di utilizzo della prenotazione di capacità.

- Il tipo di istanza e la piattaforma (sistema operativo) della prenotazione di capacità.

Inoltre, quando l'utilizzo della capacità per una prenotazione di capacità nell'account scende al di sotto del 20% in un periodo di 24 e 7 giorni, AWS Health invia eventi a. EventBridge Con EventBridge, puoi creare regole che attivano azioni automatiche, come l'invio di notifiche e-mail o l'attivazione di AWS Lambda funzioni, in risposta a tali eventi. Per ulteriori informazioni, consulta Monitora le prenotazioni di capacità utilizzando EventBridge.

Blocchi di capacità per ML

Blocchi di capacità per ML ti consente di prenotare istanze GPU molto richieste in date future per supportare i tuoi carichi di lavoro di machine learning (ML) di breve durata. Le istanze eseguite all'interno di un Capacity Block vengono automaticamente posizionate vicine tra loro all'interno di Amazon UltraClusters EC2, per reti a bassa latenza, su scala petabit e non bloccanti.

Con Blocchi di capacità puoi vedere quando la capacità dell'istanza GPU sarà disponibile nelle date future e pianificare l'avvio di un blocco di capacità di modo che inizi nel momento più adatto alle tue esigenze. Quando prenoti un blocco di capacità, ottieni una garanzia di capacità prevedibile per le istanze GPU pagando solo per il tempo necessario. Ti consigliamo di ricorrere ai blocchi di capacità quando hai bisogno di GPU per supportare i tuoi carichi di lavoro ML per giorni o settimane alla volta e non vuoi pagare una prenotazione mentre le tue istanze GPU non sono in uso.

Di seguito sono elencati alcuni casi d'uso comuni dei blocchi di capacità.

- Addestramento e messa a punto dei modelli di ML: ottieni un accesso ininterrotto alle istanze GPU che hai prenotato per completare l'addestramento e la messa a punto dei modelli di ML.
- Esperimenti e prototipi di ML: esegui esperimenti e crea prototipi che richiedono istanze GPU per brevi periodi.

I Capacity Blocks sono attualmente disponibili per istanze e istanze. `p5.48xlarge` `p4d.24xlarge` Le `p5.48xlarge` istanze sono disponibili nelle regioni Stati Uniti orientali (Ohio) e Stati Uniti orientali (Virginia settentrionale). Le `p4d.24xlarge` istanze sono disponibili nelle regioni Stati Uniti orientali (Ohio) e Stati Uniti occidentali (Oregon). Puoi prenotare un blocco di capacità con un orario di inizio della prenotazione fino a otto settimane nel futuro.

Puoi utilizzare i Capacity Blocks per prenotare istanze `p5` e `p4d` istanze con le seguenti opzioni di durata e quantità di istanze.

- Durata delle prenotazioni in incrementi di 1 giorno fino a un massimo di 14 giorni
- Opzioni di quantità di istanze della prenotazione: 1, 2, 4, 8, 16, 32 o 64 istanze

Per prenotare un Capacity Block, devi innanzitutto specificare le tue esigenze di capacità, tra cui il tipo di istanza, il numero di istanze, la quantità di tempo, la prima data di inizio e l'ultima data di fine di cui hai bisogno. Quindi, puoi visualizzare un'offerta per un blocco di capacità disponibile che soddisfa le tue specifiche. L'offerta per il blocco di capacità include dettagli come l'ora di inizio, la zona di disponibilità e il prezzo di prenotazione. Il prezzo di un'offerta per un blocco di capacità dipende dalla domanda e dall'offerta disponibili al momento della trasmissione dell'offerta. Dopo la prenotazione, il prezzo di un blocco di capacità non cambia. Per ulteriori informazioni, consulta Prezzi e fatturazione di Blocchi di capacità.

Quando acquisti un'offerta per un blocco di capacità, la prenotazione viene creata per la data e il numero di istanze che hai selezionato. Quando inizia la prenotazione del blocco di capacità, puoi scegliere come destinazione gli avvii delle istanze specificando l'ID di prenotazione nelle richieste di avvio.

Puoi utilizzare tutte le istanze prenotate fino a 30 minuti prima dell'orario di fine del blocco di capacità. A 30 minuti dalla fine della prenotazione del blocco di capacità, iniziamo a terminare tutte le istanze in esecuzione nel blocco di capacità. Utilizziamo questo lasso di tempo per ripulire le istanze prima di consegnare il blocco di capacità al cliente successivo. Gli ultimi 30 minuti della prenotazione non sono inclusi nel prezzo del blocco di capacità. Emettiamo un evento fino a EventBridge 10 minuti prima dell'inizio del processo di terminazione. Per ulteriori informazioni, consulta Monitora i blocchi di capacità con EventBridge.

Argomenti

Piattaforme supportate

Capacity Blocks for ML attualmente supporta istanze `p5.48xlarge` e `p4d.24xlarge` istanze con tenancy predefinita. Quando si utilizza il AWS Management Console per acquistare un Capacity Block, l'opzione di piattaforma predefinita è Linux/UNIX. Quando si utilizza AWS Command Line Interface (AWS CLI) o AWS SDK si acquista un Capacity Block, sono disponibili le seguenti opzioni di piattaforma:

- Linux/Unix
- Red Hat Enterprise Linux
- RHEL con HA
- SUSE Linux
- Ubuntu Pro

Considerazioni

Prima di utilizzare i blocchi di capacità, considera i seguenti dettagli e limitazioni.

- I blocchi di capacità iniziano e terminano alle 11:30 UTC (tempo coordinato universale).
- Il processo di terminazione per le istanze in esecuzione in un blocco di capacità inizia alle 11:00 UTC (tempo coordinato universale) dell'ultimo giorno della prenotazione.
- I blocchi di capacità possono essere prenotati con un orario di inizio fino a 8 settimane nel futuro.
- Non sono ammesse modifiche o cancellazioni dei blocchi di capacità.
- I Capacity Block non possono essere condivisi tra AWS account o all'interno AWS dell'organizzazione.
- I blocchi di capacità non possono essere utilizzati in un gruppo di prenotazione della capacità.
- Il numero totale di istanze che possono essere prenotate in Capacity Blocks in tutti gli account AWS dell'organizzazione non può superare le 64 istanze in una data particolare.
- Per utilizzare un blocco di capacità, le istanze devono avere come destinazione specifica l'ID di prenotazione.
- Le istanze in un blocco di capacità non vengono conteggiate ai fini dei limiti delle istanze on demand.
- Per le istanze P5 che utilizzano un'AMI personalizzata, assicurati di disporre del software e della configurazione necessari per EFA.

- I Capacity Blocks attualmente non possono essere utilizzati con gruppi di nodi gestiti di Amazon EKS oKarpenter. Per ulteriori informazioni su come creare un gruppo di nodi autogestito di Amazon EKS, consulta Capacity Blocks for ML nella Guida per l'utente di Amazon EKS.

Risorse correlate

Dopo aver creato un Capacity Block, puoi fare quanto segue con il Capacity Block:

- Avvia le istanze nel Capacity Block. Per ulteriori informazioni, consulta Avvio delle istanze nei blocchi di capacità.
- Crea un gruppo Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Use Capacity Blocks per carichi di lavoro di machine learning nella Guida per l'utente di Amazon EC2 Auto Scaling.

  > **Note**
  >
  > Se utilizzi Amazon EC2 Auto Scaling o Amazon EKS, puoi pianificare la scalabilità in modo che venga eseguita all'inizio della prenotazione Capacity Block. Grazie alla scalabilità pianificata, gestisce AWS automaticamente i nuovi tentativi al posto tuo, quindi non devi preoccuparti di implementare la logica dei tentativi per gestire gli errori transitori.

- AWS ParallelCluster Migliora i flussi di lavoro ML con. Per ulteriori informazioni, consulta Enhancing ML workflow with AWS ParallelCluster e Amazon EC2 Capacity Blocks for ML.

Per ulteriori informazioni su AWS ParallelCluster, consulta What is. AWS ParallelCluster

Prezzi e fatturazione di Blocchi di capacità

Argomenti

- Prezzi
- Fatturazione

Prezzi

Con Blocchi di capacità per ML di Amazon EC2, il pagamento avviene in base alle prenotazioni. Il prezzo di un blocco di capacità dipende dalla domanda e dall'offerta di blocchi di capacità disponibili al momento dell'acquisto. Puoi visualizzare il prezzo di un'offerta per un blocco di capacità

prima di prenotarlo. Il prezzo del blocco di capacità viene addebitato in anticipo al momento della prenotazione. Quando cerchi un blocco di capacità in un intervallo di date, ti proponiamo l'offerta per il blocco di capacità con il prezzo più basso disponibile. Dopo la prenotazione, il prezzo di un blocco di capacità non cambia.

Quando utilizzi un blocco di capacità, paghi per il sistema operativo che utilizzi quando le istanze sono in esecuzione. Per ulteriori informazioni sui prezzi dei sistemi operativi, consulta la pagina dei prezzi di Amazon EC2 Capacity Blocks for ML.

Fatturazione

Il prezzo di un'offerta per un blocco di capacità viene addebitato in anticipo. Il pagamento viene fatturato sul tuo account AWS entro 12 ore dall'acquisto di un blocco di capacità. Durante l'elaborazione del pagamento, la risorsa di prenotazione del blocco di capacità rimane nello stato `payment-pending`. Se il pagamento non può essere elaborato entro 12 ore, il blocco di capacità viene rilasciato e lo stato della prenotazione diventa `payment-failed`.

Dopo la corretta elaborazione del pagamento, lo stato delle risorse del blocco di capacità passa da `payment-pending` a `scheduled`. Riceverai una fattura che riflette il pagamento anticipato una tantum. Nella fattura, puoi associare l'importo pagato all'ID di prenotazione del blocco di capacità.

Quando inizia la prenotazione del blocco di capacità, la fatturazione viene effettuata solo in base al sistema operativo utilizzato mentre le istanze sono in esecuzione nella prenotazione. Puoi visualizzare l'utilizzo e gli addebiti associati nella fattura alla ricorrenza dall'attivazione del servizio per il mese di utilizzo nel tuo AWS Cost and Usage Report.

> **Note**
>
> Gli sconti Savings Plans e per le istanze riservate non si applicano ai blocchi di capacità.

Visualizzazione di una fattura

Puoi visualizzare la fattura nella AWS Billing and Cost Management console. Il pagamento anticipato per il blocco di capacità viene visualizzato nel mese in cui hai acquistato la prenotazione.

Dopo l'inizio della prenotazione, la fattura riporta righe separate per il tempo di prenotazione in blocco utilizzato e quello inutilizzato. Puoi utilizzare queste voci per controllare quanto tempo della prenotazione è stato utilizzato. Nella riga verrà visualizzato solo il costo di utilizzo per il tempo

impiegato, se utilizzi un sistema operativo premium. Per ulteriori informazioni, consulta Prezzi. Il tempo inutilizzato non comporta costi supplementari.

Per ulteriori informazioni, consulta Visualizzazione della fattura nella Guida per l'utente di AWS Billing and Cost Management .

Se il blocco di capacità inizia in un mese diverso da quello in cui hai acquistato la prenotazione, il prezzo corrisposto in anticipo e l'utilizzo della prenotazione vengono visualizzati in mesi di fatturazione distinti. Nel tuo AWS Cost and Usage Report, l'ID di prenotazione Capacity Block è elencato nella voce Reservation/ReservationARN della tua tariffa iniziale e il LineItem/ResourceID nella tua fattura anniversario, in modo da poter associare l'utilizzo al prezzo iniziale corrispondente.

Utilizzo dei blocchi di capacità

Per iniziare a utilizzare i blocchi di capacità, devi prima trovare e acquistare un blocco di capacità disponibile che corrisponda alle tue esigenze di dimensione, durata e tempistica di prenotazione. Quindi, quando inizia la prenotazione, puoi utilizzare il blocco di capacità avviando istanze che hanno come destinazione l'ID della prenotazione. Trenta minuti prima della scadenza della prenotazione, iniziamo a terminare tutte le istanze ancora in esecuzione nel blocco di capacità.

I blocchi di capacità vengono forniti come prenotazioni della capacità `targeted` in un'unica zona di disponibilità. Per eseguire istanze in un blocco di capacità, è necessario specificare l'ID di prenotazione all'avvio delle istanze. Se interrompi le istanze di tua iniziativa e il blocco di capacità scade, non puoi riavviarle finché non scegli come destinazione un altro blocco di capacità nello stato `active`.

Per impostazione predefinita, i blocchi di capacità offrono connettività di rete a bassa latenza e ad alta velocità di trasmissione effettiva tra le istanze all'interno del blocco di capacità; di conseguenza, se si sceglie di utilizzare un blocco di capacità, non è necessario ricorrere a un gruppo di collocazione cluster.

Argomenti

- Prerequisiti
- Ricerca e acquisto di blocchi di capacità
- Avvio delle istanze nei blocchi di capacità
- Visualizzazione dei blocchi di capacità

Prerequisiti

È necessario utilizzare il tipo Regione AWS di istanza corrispondente che si desidera utilizzare. Per ulteriori informazioni, consulta Regioni.

I blocchi di capacità con `p5.48xlarge` istanze sono disponibili di seguito Regioni AWS.

Nome Regione	Codice regione
Stati Uniti orientali (Ohio)	us-east-2
US East (N. Virginia)	us-east-1

I blocchi di capacità con `p4d.24xlarge` istanze sono disponibili di seguito. Regioni AWS

Nome Regione	Codice regione
Stati Uniti orientali (Ohio)	us-east-2
US West (Oregon)	us-west-2

> **Note**
>
> Le dimensioni dei blocchi di capacità pari a 64 istanze non sono supportate per tutti i tipi di istanze. Regioni AWS

Ricerca e acquisto di blocchi di capacità

Per prenotare un blocco di capacità, devi prima trovare un periodo di tempo in cui la capacità è disponibile che soddisfi le tue esigenze. Per trovare un blocco di capacità disponibile per la prenotazione, è necessario specificare alcuni valori.

- Il numero di istanze necessarie
- Il periodo di tempo per il quale ti occorrono le istanze
- L'intervallo di date per le quali ti occorre la prenotazione

Per cercare un'offerta per un blocco di capacità disponibile, devi specificare la durata della prenotazione e il numero di istanze. È necessario selezionare una delle opzioni seguenti.

- Per durata della prenotazione: fino a 14 giorni con incrementi di 1 giorno
- Ad esempio, il numero di istanze è 1, 2, 4, 8, 16, 32 o 64 istanze

Se è disponibile un blocco di capacità che corrisponde alle tue specifiche, restituiamo i dettagli di una sola offerta per un blocco di capacità. I dettagli dell'offerta includono l'ora di inizio della prenotazione, la zona di disponibilità per la prenotazione e il prezzo della prenotazione. Per ulteriori informazioni, consulta Prezzi.

Puoi acquistare l'offerta per il blocco di capacità che ti viene mostrata oppure modificare i criteri di ricerca per visualizzare le altre opzioni disponibili. Non esiste una scadenza predefinita per l'offerta, tuttavia le offerte sono assegnate secondo l'ordine di conferma delle richieste.

Quando acquisti un'offerta per un blocco di capacità, ricevi una risposta immediata che conferma che il tuo blocco di capacità è stato prenotato. Dopo la conferma, nel tuo account verrà visualizzata una nuova prenotazione della capacità con un tipo di prenotazione `capacity-block` e un valore `start-date` impostato sull'ora di inizio dell'offerta che hai acquistato. La tua prenotazione di un blocco di capacità viene creata con uno stato di `payment-pending`. Dopo la corretta elaborazione del pagamento anticipato, lo stato della prenotazione diventa `scheduled`. Per ulteriori informazioni, consulta Fatturazione.

Per trovare e acquistare un blocco di capacità, è possibile utilizzare uno dei seguenti metodi.

Console

Ricerca e acquisto di un blocco di capacità utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore dello schermo, seleziona un Regione AWS. Questa scelta è importante perché le dimensioni dei blocchi di capacità di 64 istanze non sono supportate per tutti i tipi di istanze in tutte le regioni.
3. Nel riquadro di navigazione, scegli Prenotazioni della capacità, Acquista blocchi di capacità.
4. In Attributi di capacità, puoi definire i parametri di ricerca del blocco di capacità. Per impostazione predefinita, la piattaforma è Linux. Se desideri selezionare un sistema operativo diverso, utilizza la AWS CLI. Per ulteriori informazioni, consulta Piattaforme supportate.
5. In Capacità totale, seleziona il numero di istanze che desideri prenotare.

6. In Durata, inserisci il numero di giorni per cui è necessaria la prenotazione.
7. In Intervallo di date per la ricerca dei blocchi di capacità, inserisci la prima data di inizio possibile e l'ultima data di fine accettabile per la tua prenotazione.
8. Scegli Cerca blocchi di capacità.
9. Se è disponibile un blocco di capacità che soddisfa le tue specifiche, vedrai un'offerta nella sezione Blocchi di capacità consigliati. Se sono presenti più offerte che soddisfano le tue specifiche, viene mostrata l'offerta per il blocco di capacità con il prezzo più basso disponibile. Per visualizzare altre offerte per blocchi di capacità, modifica gli input di ricerca e scegli nuovamente Cerca blocchi di capacità.
10. Quando trovi un'offerta per un blocco di capacità che desideri acquistare, scegli Avanti.
11. (Facoltativo) Nella pagina Aggiungi tag, scegli Aggiungi nuovo tag.
12. La pagina Verifica e acquista elenca la data di inizio e di fine, la durata, il numero totale di istanze e il prezzo.

> **Note**
>
> Non è possibile modificare o annullare i blocchi di capacità dopo averli prenotati.

13. Nella finestra popup Acquista un blocco di capacità, digita conferma, quindi scegli Acquista.

AWS CLI

Per trovare un Capacity Block, usa il AWS CLI

Utilizza il comando `describe-capacity-block-offerings`.

L'esempio seguente cerca un blocco di capacità con 16 istanze `p5.48xlarge` con un intervallo di date che inizia il `2023-08-14` e termina il `2023-10-22` e con una durata di 48 ore. Il numero di istanze deve essere un numero intero scelto da una serie predefinita di opzioni: 1, 2, 4, 8, 16, 32 o 64. La durata della capacità deve essere un numero intero multiplo di 24 compreso tra 24 e 336, che indica il numero di giorni espresso in ore.

```
aws ec2 describe-capacity-block-offerings --instance-type p5.48xlarge \
  --instance-count 16 --start-date-range 2023-08-14T00:00:00Z \
  --end-date-range 2023-10-22-T00:00:00Z --capacity-duration 48
```

Per acquistare un Capacity Block utilizzando il AWS CLI

Utilizza il comando `purchase-capacity-block` e specifica l'ID dell'offerta del blocco di capacità che desideri acquistare e la piattaforma di istanza.

```
aws ec2 purchase-capacity-block \
  --capacity-block-offering-id cbr-0123456789abcdefg \
  --instance-platform Linux/UNIX
```

Avvio delle istanze nei blocchi di capacità

Dopo aver prenotato un blocco di capacità, puoi visualizzare la rispettiva prenotazione nel tuo account AWS . Puoi visualizzare `start-date` e `end-date` per vedere quando la prenotazione avrà inizio e fine. Prima dell'inizio di una prenotazione di blocco di capacità, la capacità disponibile visualizzata è pari a zero. Puoi vedere quante istanze saranno disponibili nel blocco di capacità in base al valore del tag per la chiave del tag `aws:ec2capacityreservation:incrementalRequestedQuantity`.

Quando inizia la prenotazione di un blocco di capacità, lo stato della prenotazione passa da `scheduled` a `active`. Emettiamo un evento tramite Amazon EventBridge per informarti che il Capacity Block è disponibile per l'uso. Per ulteriori informazioni, consulta Monitoraggio dei blocchi di capacità.

Per utilizzare il blocco di capacità, devi specificare l'ID di prenotazione del blocco di capacità all'avvio delle istanze. L'avvio di un'istanza in un blocco di capacità ne riduce la capacità disponibile in misura pari al numero di istanze avviate. Ad esempio, se la capacità dell'istanza acquistata è di otto istanze e ne avvii quattro, la capacità disponibile viene ridotta di quattro unità.

Se termini un'istanza in esecuzione nel blocco di capacità prima della fine della prenotazione, puoi avviare una nuova istanza al suo posto. Quando si arresta o si termina un'istanza in un blocco di capacità, occorrono diversi minuti per ripulire l'istanza prima di poterne avviare un'altra per sostituirla. Durante questo periodo, l'istanza si troverà in uno stato di arresto o `shutting-down`. Una volta completato questo processo, lo stato dell'istanza diventa `stopped` o `terminated`. Quindi, la capacità disponibile nel blocco di capacità verrà aggiornata per mostrare un'altra istanza disponibile per l'uso.

I passaggi seguenti spiegano come avviare le istanze in un Capacity Block nello `active` stato utilizzando il AWS Management Console o il. AWS CLI

Per informazioni su come configurare un gruppo di nodi EKS per utilizzare automaticamente un blocco di capacità quando ha inizio, consulta la pagina Capacity Blocks for ML nella Guida per l'utente di Amazon EKS.

Per informazioni su come avviare le istanze in un blocco di capacità utilizzando il parco istanze EC2, consulta Tutorial: avvio delle istanze in Blocchi di capacità.

Per informazioni su come creare un modello di avvio destinato a un blocco di capacità, consulta Avvio di un'istanza da un modello di avvio.

È possibile utilizzare uno dei seguenti metodi per avviare le istanze in un blocco di capacità.

Console

Avvio di istanze in un blocco di capacità utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore della schermata, seleziona la regione della prenotazione del blocco di capacità.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
4. (Facoltativo) In Nome e tag, è possibile assegnare un nome e un tag all'istanza. Per ulteriori informazioni sui tag, consulta la pagina Tagging delle risorse Amazon EC2.
5. In Immagini di applicazioni e sistema operativo, seleziona un'Amazon Machine Image (AMI).
6. In Tipo di istanza, seleziona il tipo di istanza che corrisponde alla tua prenotazione del blocco di capacità.
7. In Coppia di chiavi (login), scegli una coppia di chiavi esistente oppure scegli Crea nuova coppia di chiavi per crearne una nuova. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.
8. In Network settings (Impostazioni di rete), utilizza le impostazioni predefinite o scegli Edit (Modifica) per configurare le impostazioni di rete come necessario.

   > **Important**
   >
   > L'istanza non può essere avviata in una sottorete ubicata in una zona di disponibilità diversa da quella in cui si trova il blocco di capacità.

9. In Dettagli avanzati, configura la richiesta di istanza nel modo seguente.

a. In Opzione di acquisto (tipo di mercato), seleziona Blocchi di capacità.
b. In Prenotazione della capacità, seleziona Destinazione per ID.
c. Seleziona l'ID di prenotazione della capacità della tua prenotazione del blocco di capacità.

10. Nel pannello Summary (Riepilogo), per Number of instances (Numero di istanze), inserisci il numero di istanze da avviare.
11. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Per avviare le istanze in un Capacity Block utilizzando il AWS CLI

- Utilizza il comando `run-instances` e specifica come `MarketType` il valore `capacity-block` nella struttura `instance-market-options`. È inoltre necessario specificare il parametro `capacity-reservation-specification`.

  Nell'esempio seguente viene avviata una sola istanza `p5.48xlarge` in un blocco di capacità attivo che abbia attributi corrispondenti e capacità disponibile.

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 \
  --instance-type p5.48xlarge --key-name MyKeyPair \
  --subnet-id subnet-1234567890abcdef1 \
  --instance-market-options MarketType='capacity-block'
  --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

Visualizzazione dei blocchi di capacità

I blocchi di capacità possono assumere i seguenti stati:

- `payment-pending`: il pagamento anticipato non è stato ancora elaborato.
- `payment-failed`: non è stato possibile elaborare il pagamento nell'arco di 12 ore. Il tuo blocco di capacità è stato rilasciato.
- `scheduled`: il pagamento è stato elaborato e la prenotazione del blocco di capacità non è ancora iniziata.
- `active`: la capacità riservata è disponibile per l'utilizzo.

- `expired`: la prenotazione del blocco di capacità è scaduta automaticamente alla data e ora specificate nella richiesta di prenotazione. La capacità riservata non è più disponibile per l'utilizzo.

È possibile utilizzare uno dei seguenti metodi per visualizzare la prenotazione del blocco di capacità.

Console

Visualizzazione dei blocchi di capacità tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Nella pagina Panoramica delle prenotazioni di capacità, viene visualizzata una tabella delle risorse con i dettagli su tutte le tue risorse di prenotazione della capacità. Per trovare le tue prenotazioni di blocchi di capacità, seleziona Blocchi di capacità dall'elenco a discesa sopra l'ID di prenotazione della capacità. Nella tabella puoi visualizzare informazioni sui tuoi blocchi di capacità, come date di inizio e fine, durata e stato.
4. Per maggiori dettagli su un blocco di capacità, seleziona l'ID di prenotazione corrispondente al blocco di capacità che desideri visualizzare. La pagina Dettagli della prenotazione della capacità mostra tutte le proprietà della prenotazione e il numero di istanze in uso e disponibili nel blocco di capacità.

> **Note**
>
> Prima dell'inizio di una prenotazione di blocco di capacità, la capacità disponibile visualizzata è pari a zero. Puoi vedere quante istanze saranno disponibili quando inizia la prenotazione del blocco di capacità in base al valore del tag per la chiave del tag `aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

Per visualizzare i blocchi di capacità utilizzando il AWS CLI

Per impostazione predefinita, quando si utilizza il describe-capacity-reservationscomando vengono elencate sia le prenotazioni On-Demand Capacity Reservations che le prenotazioni Capacity Block. Per visualizzare solo le prenotazioni di blocchi di capacità, filtra i risultati utilizzando `capacity-block` per il parametro `capacity-reservation-type`.

Ad esempio, il comando seguente descrive una o più prenotazioni di Capacity Block tra quelle correnti Regione AWS.

```
aws ec2 describe-capacity-reservations -reservation-type capacity-block
```

Output di esempio:

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-12345678",
            "EndDateType": "limited",
            "ReservationType": "capacity-block"
            "AvailabilityZone": "eu-east-2a",
            "InstanceMatchCriteria": "targeted",
            "EphemeralStorage": false,
            "CreateDate": "2023-11-29T14:22:45Z",
            "StartDate": "2023-12-15T12:00:00Z",
            "EndDate": "2023-08-19T12:00:00Z",
            "AvailableInstanceCount": 0,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 16,
            "State": "payment-pending",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "p5.48xlarge"
        },
        ...
```

Monitoraggio dei blocchi di capacità

Argomenti

- Monitora i blocchi di capacità con EventBridge
- La registrazione di Capacity Blocca le chiamate API con AWS CloudTrail

Monitora i blocchi di capacità con EventBridge

Quando inizia la prenotazione Capacity Block, Amazon EC2 emetterà un evento EventBridge che indica che la capacità è pronta per l'uso. Quaranta minuti prima della scadenza della prenotazione di Capacity Block, ricevi un altro EventBridge evento che ti informa che tutte le istanze in esecuzione

nella prenotazione inizieranno a terminare dopo 10 minuti. Per ulteriori informazioni sugli EventBridge eventi, consulta Amazon EventBridge Events.

Le seguenti strutture di eventi per gli eventi emessi per i blocchi di capacità:

Blocco di capacità fornito

Nell'esempio seguente viene illustrato un evento per un blocco di capacità fornito.

```
{
  "customer_event_id": "[Capacity Reservation Id]-delivered",
  "detail_type": "Capacity Block Reservation Delivered",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Avviso di scadenza del blocco di capacità

Nell'esempio seguente viene illustrato un avviso di scadenza per un blocco di capacità.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Reservation Expiration Warning",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

La registrazione di Capacity Blocca le chiamate API con AWS CloudTrail

Capacity Blocks è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Capacity Blocks. CloudTrail acquisisce le chiamate API per Capacity Blocks come eventi. Le chiamate acquisite includono le chiamate dalla console di Blocchi di capacità e le chiamate di codice alle operazioni delle API di Blocchi di capacità. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Capacity Blocks. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata a Capacity Blocks, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni su Capacity Blocks in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in Capacity Blocks, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi per Capacity Blocks, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni di Capacity Blocks vengono registrate CloudTrail e documentate nell'Amazon EC2 API Reference. Ad esempio, le chiamate a e le `CapacityBlockScheduled` `CapacityBlockActive` azioni generano voci nei file di registro. CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Informazioni sulle voci di file di log di Blocchi di capacità

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Gli esempi seguenti mostrano le voci di CloudTrail registro per:

- TerminateCapacityBlocksInstances
- CapacityBlockPaymentFailed
- CapacityBlockScheduled
- CapacityBlockActive
- CapacityBlockFailed
- CapacityBlockExpired

> **Note**
>
> Alcuni campi degli esempi sono stati oscurati per la privacy dei dati.

TerminateCapacityBlocksInstances


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:instance/
i-1234567890abcdef0"
    }
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws::ec2:US East (N. Virginia):123456789012:instance/
i-0598c7d356eba48d7"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      }
}
```


CapacityBlockPaymentFailed


```
{
  "eventVersion": "1.05",
```

```
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "payment-failed"
      }
}
```


CapacityBlockScheduled


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockScheduled",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
```

```
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "scheduled"
      }
}
```

CapacityBlockActive

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
```

```
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "active"
      }
 }
```

CapacityBlockFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "failed"
```

```
      }
 }
```

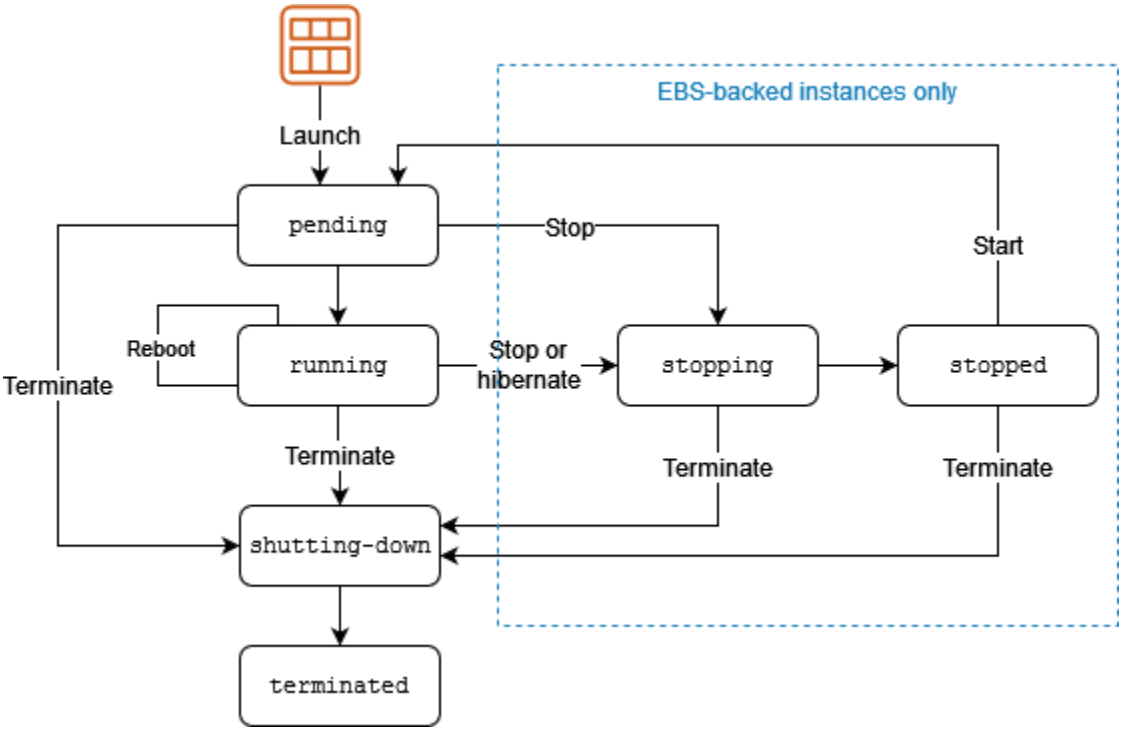
CapacityBlockExpired

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "expired"
      }
 }
```

Ciclo di vita dell'istanza

Un'istanza Amazon EC2 passa attraverso stati diversi dal momento in cui la si avvia fino alla sua terminazione.

La figura che segue rappresenta le transizioni tra gli stati di un'istanza. Da notare che non puoi arrestare e avviare un'istanza supportata da instance store. Per ulteriori informazioni sulle istanze supportate da instance store, consulta Archiviazione del dispositivo root.



La tabella seguente fornisce una breve descrizione di ogni stato dell'istanza e indica se l'utilizzo dell'istanza viene fatturato. Alcune AWS risorse, come i volumi Amazon EBS e gli indirizzi IP elastici, comportano costi indipendentemente dallo stato dell'istanza. Per ulteriori informazioni, consulta l'argomento Evitare costi inattesi nella Guida per l'utente AWS Billing .

Stato istanza	Descrizione	Fatturazione per l'utilizzo dell'istanza
`pendinc`	L'istanza si sta preparando a diventare `running`. Un'istanza assume lo stato `pending` quando viene avviata o quando viene aperta dopo che è stata `stopped`.	Non fatturata

Stato istanza	Descrizione	Fatturazione per l'utilizzo dell'istanza
`running`	L'istanza è in esecuzione e pronta per l'uso.	Fatturato
`stopping`	L'istanza si sta preparando all'arresto.	Non fatturata
`stopped`	L'istanza è terminata e non può essere utilizzata. L'istanza può essere avviata in qualsiasi momento.	Non fatturata
`shutting-down`	L'istanza si sta preparando a essere terminata.	Non fatturata
`terminated`	L'istanza è stata eliminata definitivamente e non può essere avviata.	Non fatturata **Note** Le istanze riservate applicate a istanze terminate sono fatturate fino alla fine del loro termine in base alla loro opzione di pagamento. Per ulteriori informazioni, consulta la sezione Istanze riservate .

Indice

- Lancio dell'istanza
- Arresta e avvia le istanze Amazon EC2
- Metti in ibernazione la tua istanza Amazon EC2
- Riavvio dell'istanza
- Termina le istanze Amazon EC2
- Ritiro dell'istanza
- Resilienza delle istanze

Avvio dell'istanza

Quando avvii un'istanza, il suo stato è `pending`. Il tipo di istanza specificato all'avvio determina l'hardware del computer host utilizzato per tale istanza. Utilizziamo l'Amazon Machine Image (AMI) che hai specificato all'avvio per avviare l'istanza. Quando l'istanza è pronta, il relativo stato diventa `running`. Puoi collegarti all'istanza in esecuzione e utilizzarla come un normale computer.

Non appena lo stato dell'istanza diventa `running`, ti verrà addebitato il costo al secondo, con un minimo di un minuto, per il tempo che l'istanza è in esecuzione, anche se inattiva e non ti colleghi a essa.

Arresto e avvio dell'istanza (solo istanze supportate da Amazon EBS)

Se l'istanza non supera il controllo dello stato oppure se non esegue le applicazioni nel modo previsto e se il volume root dell'istanza è un volume Amazon EBS, puoi arrestare e avviare l'istanza per cercare di risolvere il problema.

Quando arresti l'istanza, il relativo stato diventa `stopping` e quindi `stopped`. Non ti vengono addebitati i costi di utilizzo o di trasferimento dei dati per la tua istanza quando è `stopped`. Sono previsti costi per l'archiviazione di qualsiasi volume Amazon EBS. Quando lo stato dell'istanza è `stopped`, puoi modificare determinati attributi dell'istanza, compreso il tipo di istanza.

Una volta avviata, l'istanza entra nello stato `pending` e viene spostata su un nuovo computer host (anche se in alcuni casi, rimane sull'host corrente). Quando arresti e avvii un'istanza, perdi tutti i dati sui volumi di instance store collegati al precedente computer host.

L'istanza conserva il proprio indirizzo IPv4 privato, ovvero all'istanza continua a essere associato un indirizzo IP elastico associato all'indirizzo IPv4 privato o all'interfaccia di rete. Se l'istanza dispone di un indirizzo IPv6, conserverà il relativo indirizzo IPv6.

Ogni volta che si esegue la transizione di un'istanza da `stopped` a `running`, ti verrà addebitato un costo al secondo quando l'istanza è in esecuzione, con un minimo di un minuto per avvio di istanza.

Per ulteriori informazioni sull'arresto e sull'avvio di un'istanza, consulta Arresta e avvia le istanze Amazon EC2.

Ibernazione dell'istanza (solo istanze supportate da Amazon EBS)

Quando ibernate un'istanza, segnaliamo al sistema operativo di eseguire l'ibernazione (suspend-to-disk), che salva i contenuti dalla memoria dell'istanza (RAM) al volume root di Amazon EBS. Rendiamo persistente il volume root di Amazon EBS dell'istanza ed eventuali volumi di dati di Amazon EBS collegati. Quando avvii l'istanza, il volume root di Amazon EBS viene ripristinato allo stato precedente e i contenuti RAM vengono ricaricati. I volumi di dati precedentemente collegati vengono collegati nuovamente e l'istanza conserva il proprio ID.

Quando iberni l'istanza, il relativo stato diventa `stopping` e quindi `stopped`. Non addebitiamo l'utilizzo per un'istanza ibernata quando si trova nello stato `stopped`, ma lo addebitiamo quando si trova nello stato `stopping`, a differenza di quando arresti un'istanza senza ibernarla. Non addebitiamo l'utilizzo del trasferimento di dati, ma addebitiamo l'archivizione di tutti i volumi Amazon EBS, compreso l'archiviazione per i dati RAM.

Una volta avviata, l'istanza di ibernazione entra nello stato `pending` e viene spostata su un nuovo computer host (anche se in alcuni casi, rimane sull'host corrente).

L'istanza conserva il proprio indirizzo IPv4 privato, ovvero all'istanza continua a essere associato un indirizzo IP elastico associato all'indirizzo IPv4 privato o all'interfaccia di rete. Se l'istanza dispone di un indirizzo IPv6, essa conserverà il relativo indirizzo IPv6.

Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.

Riavvio dell'istanza

Puoi riavviare l'istanza utilizzando la console Amazon EC2, uno strumento a riga di comando e l'API Amazon EC2. Ti consigliamo di utilizzare Amazon EC2 per riavviare l'istanza anziché eseguire il comando di riavvio del sistema operativo dall'interno dell'istanza.

Il riavvio di un'istanza equivale al riavvio di un sistema operativo. L'istanza rimane sullo stesso computer host e mantiene il nome DNS pubblico e l'indirizzo IP privato propri e tutti i dati presenti nei volumi instance store. Il completamento del riavvio in genere richiede pochi minuti, ma il tempo necessario dipende dalla configurazione dell'istanza.

Il reboot di un'istanza non comporta l'inizio di un nuovo periodo di fatturazione. La fatturazione al secondo continua senza un ulteriore addebito minimo di un minuto.

Per ulteriori informazioni, consulta Riavvio dell'istanza.

Interruzione dell'istanza

Se decidi che un'istanza non è più necessaria, puoi interromperla. Appena lo stato di un'istanza cambia in `shutting-down` o `terminated`, vengono bloccati i rispettivi addebiti.

Se hai abilitato la protezione da interruzione, non puoi interrompere l'istanza tramite la console, le CLI o l'API.

Dopo essere stata interrotta, un'istanza rimane visibile nella console per un breve periodo, trascorso il quale la relativa voce viene eliminata automaticamente. Puoi definire un'istanza interrotta anche tramite la CLI e l'API. Le risorse, ad esempio i tag, vengono gradualmente scollegate dall'istanza interrotta e pertanto potrebbero non risultare più visibili sull'istanza interrotta dopo un breve periodo di tempo. Non puoi collegarti a un'istanza interrotta, né recuperarla.

Ogni istanza supportata da Amazon EBS supporta l'`InstanceInitiatedShutdownBehavior`attributo, che controlla se l'istanza si arresta o termina quando si avvia l'arresto dall'interno dell'istanza stessa (ad esempio, utilizzando il comando su Linux). shutdown Il comportamento di default prevede l'arresto dell'istanza. Puoi modificare l'impostazione di questo attributo mentre l'istanza è in esecuzione o quando è arrestata.

Ogni volume Amazon EBS supporta l'attributo `DeleteOnTermination` che controlla se il volume viene eliminato o conservato quando interrompi l'istanza a cui è collegato. Il comportamento di default prevede l'eliminazione del volume dispositivo root e la conservazione di qualsiasi altro volume EBS.

Per ulteriori informazioni, consulta Termina le istanze Amazon EC2.

Differenze tra riavvio, arresto, ibernazione e interruzione

La tabella che segue riepiloga le principali differenze tra riavvio, arresto, ibernazione e interruzione dell'istanza.

Caratteristica	Riavvio	Arresto/avvio (solo istanze supportate da Amazon EBS)	Ibernazione (solo istanze supportate da Amazon EBS)	Interruzione
Computer host	L'istanza rimane sullo stesso computer host	Spostiamo l'istanza su un nuovo computer host (anche se in alcuni casi, rimane sull'host corrente).	Spostiamo l'istanza su un nuovo computer host (anche se in alcuni casi, rimane sull'host corrente).	Nessuno
Indirizzi IPv4 privati e pubblici	Questi indirizzi rimangono invariati	L'istanza conserva il proprio indirizzo IPv4 privato. All'istanza viene assegnato un nuovo indirizzo IPv4 pubblico, a meno che non abbia un indirizzo IP elastico, che non varia durante la fase di arresto/avvio.	L'istanza conserva il proprio indirizzo IPv4 privato. All'istanza viene assegnato un nuovo indirizzo IPv4 pubblico, a meno che non abbia un indirizzo IP elastico, che non varia durante la fase di arresto/avvio.	Nessuno
Indirizzi IP elastici (IPv4)	L'indirizzo IP elastico rimane associato all'istanza	L'indirizzo IP elastico rimane associato all'istanza	L'indirizzo IP elastico rimane associato all'istanza	L'indirizzo IP elastico viene scollegato dall'istanza
Indirizzo IPv6	L'istanza conserva il proprio indirizzo IPv6	L'istanza conserva il proprio indirizzo IPv6	L'istanza conserva il proprio indirizzo IPv6	Nessuno
Volumi di instance store	I dati vengono conservati	I dati vengono cancellati	I dati vengono cancellati	I dati vengono cancellati

Caratteristica	Riavvio	Arresto/avvio (solo istanze supportate da Amazon EBS)	Ibernazione (solo istanze supportate da Amazon EBS)	Interruzione
Volume dispositivo root	Il volume viene conservato	Il volume viene conservato	Il volume viene conservato	Per impostazione di default, il volume viene eliminato
RAM (contenuto della memoria)	La RAM viene cancellata	La RAM viene cancellata	La RAM viene salvata in un file nel volume root	La RAM viene cancellata
Fatturazione	L'ora di fatturazione dell'istanza non cambia	Appena lo stato di un'istanza diventa `stopping`, vengono bloccati i rispettivi addebiti. Ogni volta che lo stato dell'istanza passa da `stopped` a `running`, inizia un nuovo periodo di fatturazione, con un minimo di un minuto ogni volta che l'istanza viene avviata.	Vengono addebitati dei costi mentre l'istanza è nello stato `stopping`, ma gli addebiti terminano quando l'istanza è nello stato `stopped`. Ogni volta che lo stato dell'istanza passa da `stopped` a `running`, inizia un nuovo periodo di fatturazione, con un minimo di un minuto ogni volta che l'istanza viene avviata.	Smetti di incorrere in addebiti per un'istanza non appena il suo stato cambia in `shutting-down`

I comandi di chiusura del sistema operativo interrompono sempre un'istanza supportata da instance store. Puoi determinare se i comandi di chiusura del sistema operativo arrestano o interrompono un'istanza supportata da Amazon EBS. Per ulteriori informazioni, consulta Modifica del comportamento di arresto avviato dall'istanza.

Lancio dell'istanza

Un'istanza è un server virtuale nel AWS cloud. Puoi avviare un'istanza da un'Amazon Machine Image (AMI). L'AMI fornisce il sistema operativo, il server applicazioni e le applicazioni per l'istanza.

Quando ti registri AWS, puoi iniziare a usare Amazon EC2 gratuitamente utilizzando il. Piano gratuito di AWS Puoi utilizzare il piano gratuito per avviare e utilizzare un'`t2.micro`istanza gratuitamente per 12 mesi (nelle regioni in cui non `t2.micro` è disponibile, puoi utilizzare un'`t3.micro`istanza con il piano gratuito).Ti verranno addebitati costi per l'istanza o l'utilizzo che rientrano nei limiti del piano gratuito mentre l'istanza è in esecuzione, anche se rimane inattiva. Per ulteriori informazioni, consulta Prezzi di Amazon EC2.

Puoi avviare un'istanza utilizzando uno dei seguenti metodi.

Metodo	Documentazione
[Console Amazon EC2] Utilizzare la procedura guidata di avvio delle istanze per specificare i parametri di avvio.	Avvio di un'istanza tramite la vecchia procedura guidata di avvio
[Console Amazon EC2] Creare un modello di avvio e avviare l'istanza dal modello di avvio.	Avvio di un'istanza da un modello di avvio
[Console Amazon EC2] Utilizzare un'istanza esistente come base.	Avvio di un'istanza con i parametri di un'istanza esistente
[Console Amazon EC2] Utilizza un'AMI acquistata da Marketplace AWS.	Avvia un' Marketplace AWS istanza
[AWS CLI] Utilizzare un'AMI selezionata.	Utilizzo di Amazon EC2 tramite la CLI AWS
[AWS Tools for Windows PowerShell] Utilizzare un'AMI selezionata.	Amazon EC2 di AWS Tools for Windows PowerShell
[AWS CLI] Utilizza la Serie di istanze EC2 per eseguire il provisioning della capacità tra tipi di istanza EC2 e zone di disponibilità diversi e tra modelli di acquisto Istanza on demand, Istanza riservata e Istanza spot.	EC2 Fleet

Metodo	Documentazione
[AWS CloudFormation] Utilizza un AWS CloudFormation modello per specificare un'istanza.	AWS::EC2::Instance nella Guida per l'utente di AWS CloudFormation
[AWS SDK] Utilizza un AWS SDK specifico per la lingua per avviare un'istanza.	AWS SDK per.NET AWS SDK per C++ AWS SDK for Go AWS SDK per Java AWS SDK per JavaScript AWS SDK per PHP V3 AWS SDK per Python AWS SDK per Ruby V3

Note

Per avviare un'istanza EC2 in una sottorete solo IPv6, è necessario utilizzare le istanze create sul sistema Nitro. AWS

Note

Quando si avvia un'istanza solo IPv6, è possibile che DHCPv6 non fornisca immediatamente l'istanza con il server dei nomi DNS IPv6. Durante questo ritardo iniziale, l'istanza potrebbe non essere in grado di risolvere i domini pubblici.
Per le istanze in esecuzione su Amazon Linux 2, se si desidera aggiornare immediatamente il file /etc/resolv.conf con il server dei nomi DNS IPv6, eseguire la seguente direttiva cloud-init all'avvio:

```
#cloud-config
bootcmd:
```

```
- /usr/bin/sed -i -E 's,^nameserver\s+[\.[:digit:]]+$,nameserver
 fd00:ec2::253,' /etc/resolv.conf
```

Un'altra opzione è quella di modificare il file di configurazione e reimpostare l'AMI in modo che l'indirizzo del server dei nomi DNS IPv6 sia immediatamente presente nel file all'avvio.

Quando si avvia l'istanza, è possibile avviarla in una sottorete associata a una delle seguenti risorse:

- Una zona di disponibilità: è l'opzione predefinita.
- Local Zone - Per avviare un'istanza in una Local Zone è necessario accettare esplicitamene la Local Zone e quindi creare una sottorete nella zona. Per ulteriori informazioni, consulta la Guida introduttiva a Local Zones
- Zona Wavelength - Per avviare un'istanza in una zona Wavelength è necessario accettare esplicitamente la zona Wavelength e quindi creare una sottorete nella zona. Per informazioni su come avviare un'istanza in una Wavelength Zone, consulta la Guida introduttiva. AWS Wavelength
- Un Outpost: per avviare un'istanza in un Outpost, è necessario crearlo. Per informazioni su come creare un Outpost, consulta la Guida introduttiva a. AWS Outposts

Dopo aver avviato l'istanza, puoi stabilire una connessione e utilizzarla. All'inizio lo stato dell'istanza è `pending`. Quando lo stato dell'istanza è `running`, significa che è iniziato l'avvio dell'istanza. Potrebbe passare qualche minuto prima di riuscire a connetterti all'istanza. Si noti che i tipi di istanza bare metal potrebbero richiedere più tempo per l'avvio.

L'istanza riceve un nome DNS pubblico che potrai utilizzare per contattare l'istanza da Internet. L'istanza riceve inoltre un nome DNS privato che le altre istanze all'interno dello stesso VPC potranno utilizzare per contattare l'istanza.

Quando un'istanza non è più necessaria, assicurati di terminarla. Per ulteriori informazioni, consulta Termina le istanze Amazon EC2.

Avvio di un'istanza tramite la procedura guidata di avvio istanza

È possibile avviare un'istanza tramite la nuova procedura guidata di avvio. La procedura guidata di avvio specifica tutti i parametri di avvio necessari per l'avvio di un'istanza. Se la procedura guidata di avvio dell'istanza fornisce un valore di default, è possibile accettare tale valore o specificare il proprio. Se si accettano i valori di default, è possibile avviare un'istanza selezionando solo una coppia di chiavi.

> **Important**
>
> Ti verranno addebitati costi per l'istanza o l'utilizzo che rientrano nei limiti del piano gratuito mentre l'istanza è in esecuzione, anche se rimane inattiva.

Argomenti

Avvio rapido di un'istanza

Per configurare rapidamente un'istanza a scopo di test, completare la seguente procedura per avviare rapidamente un'istanza. Verrà selezionato il sistema operativo e la coppia di chiavi e accettati i valori di default. Per informazioni su tutti i parametri della procedura guidata di avvio istanza, consultare Avvio di un'istanza utilizzando parametri definiti.

Come avviare rapidamente un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore dello schermo, viene visualizzata la AWS regione corrente (ad esempio, Stati Uniti orientali (Ohio)). Selezionare una regione in cui avviare l'istanza. Questa scelta è importante perché, a differenza di altre, alcune risorse Amazon EC2 possono essere condivise tra più regioni. Per ulteriori informazioni, consulta Posizioni delle risorse.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
4. (Facoltativo) in Name and tags (Nome e tag), per Name (Nome), inserire un nome descrittivo per la propria istanza.
5. In Application and OS Images (Amazon machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), scegli Quick Start (Avvio rapido), quindi scegli il sistema operativo (SO) per la tua istanza.
6. In Key pair (login) (Coppia di chiavi (login), per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o creane una nuova.
7. Nel pannello Summary (Riepilogo), scegliere Launch instance (Avvia istanza).

Avvio di un'istanza utilizzando parametri definiti

Ad eccezione della coppia di chiavi, la procedura guidata di avvio istanza fornisce i valori di default per tutti i parametri. È possibile accettare uno o tutti i valori predefiniti o configurare un'istanza specificando i propri valori per ciascun parametro. I parametri vengono raggruppati nella procedura guidata di avvio istanza. Le seguenti istruzioni sono relative a ogni gruppo di parametri.

Parametri per la configurazione di un'istanza

- Iniziare il lancio dell'istanza
- Nome e tag
- Immagini di applicazioni e sistema operativo (Amazon Machine Image)
- Tipo di istanza
- Coppia di chiavi (login)
- Impostazioni di rete
- Per configurare l'archiviazione
- Dettagli avanzati
- Riepilogo

Iniziare il lancio dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore dello schermo, viene visualizzata la AWS regione corrente (ad esempio, Stati Uniti orientali (Ohio)). Selezionare una regione in cui avviare l'istanza. Questa scelta è importante perché, a differenza di altre, alcune risorse Amazon EC2 possono essere condivise tra più regioni. Per ulteriori informazioni, consulta Posizioni delle risorse.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).

Nome e tag

Il nome dell'istanza è un tag, dove la chiave è Name (Nome) e il valore è il nome specificato. È possibile etichettare l'istanza, i volumi e le interfacce di rete. Per le istanze spot, è possibile aggiungere un tag solo alla richiesta di istanza spot. Per ulteriori informazioni sui tag, consulta Tagging delle risorse Amazon EC2..

La specifica di un nome di istanza e dei tag aggiuntivi è facoltativa.

- Per Name (Nome), inserire un nome descrittivo per l'istanza. Se non si specifica un nome, l'istanza può essere identificata dal relativo ID, che viene generato automaticamente all'avvio dell'istanza.
- Per aggiungere altri tag, scegliere Add additional tags (Aggiungi altri tag). Scegliere Add tag (Aggiungi tag), quindi immettere una chiave e un valore e selezionare il tipo di risorsa da taggare. Scegliere Add tag (Aggiungi tag) per ogni tag aggiuntivo.

Immagini di applicazioni e sistema operativo (Amazon Machine Image)

Un'Amazon Machine Image (AMI) contiene tutte le informazioni necessarie per creare un'istanza. Ad esempio, un'AMI potrebbe contenere il software necessario per fungere da server Web, come Linux, Apache e il tuo sito Web.

È possibile trovare un'AMI adatta come descritto di seguito: In caso contrario, scegliere Cancel (Annulla) (in alto a destra) per tornare alla procedura guidata di avvio istanza senza scegliere un'AMI.

Barra di ricerca

Per ricercare tra tutte le AMI disponibili, inserisci una parola chiave nella barra di ricerca AMI e premi Invio. Scegliere Select (Seleziona) per selezionare l'AMI.

Recents (Recenti

Le AMI usate di recente.

Scegliere Recently launched (Avviati di recente) o Currently in use (Correntemente in uso) e poi, da Amazon Machine Image (AMI), selezionare un'AMI.

My AMIs (Le mie AMI)

AMI private di proprietà o AMI private condivise da altri utenti.

Scegliere Owned by me (Di mia proprietà) o Shared with me (Condiviso con me) e poi, da Amazon Machine Image (AMI), selezionare un'AMI.

Quick Start

Le AMI sono raggruppate per sistema operativo (SO) in modo che possano essere utilizzate rapidamente.

Per prima cosa selezionare il sistema operativo di cui si ha bisogno e quindi da Amazon Machine Image (AMI), selezionare un'AMI. Per selezionare un'AMI idonea al piano gratuito, assicurarsi che l'AMI sia contrassegnata come Free tier eligible (Idonea al piano gratuito).

Ricerca di altre AMI

Scegliere Browse more AMIs (Sfoglia altre AMI) per sfogliare il catalogo completo di AMI.

- Per ricercare tra tutte le AMI disponibili, inserisci una parola chiave nella barra di ricerca e premi Invio.
- Per trovare un'AMI utilizzando un parametro di Systems Manager, seleziona il pulsante freccia a destra della barra di ricerca, quindi scegli Search by Systems Manager parameter (Cerca per parametro Systems Manager). Per ulteriori informazioni, consulta Trova un'AMI utilizzando un parametro Systems Manager.
- Per cercare per categoria, scegliere Quickstart AMIs (Avvio rapido delle AMI), My AMIs (Le mie AMI), Marketplace AWS AMI (AMI MKT), oppure Community AMIs (AMI della community).

  Marketplace AWS È un negozio online in cui è possibile acquistare software che funziona su AWS, comprese le AMI. Per ulteriori informazioni sull'avvio di un'istanza da Marketplace AWS, consulta. Avvia un' Marketplace AWS istanza In Community AMIs (AMI della community), è possibile trovare AMI che i membri della community AWS hanno reso disponibili per l'uso da parte di altri utenti. Le AMI di Amazon o di un partner verificato sono contrassegnate con la dicitura Verified provider (fornitore verificato).
- Per filtrare l'elenco delle AMI, selezionare una o più caselle di controllo sotto Refine results (Definisci i risultati) a sinistra dello schermo. Le opzioni di filtro sono diverse a seconda della categoria di ricerca selezionata.
- Controllare le voci per ciascuna AMI nell'elenco Root device type (Tipo dispositivo root). Individuare le AMI del tipo desiderato: ebs (supportate da Amazon EBS) o instance-store (supportate dall'archivio istanza). Per ulteriori informazioni, consulta Archiviazione del dispositivo root.
- Controllare le voci per ciascuna AMI nell'elenco Virtualization type (Tipo di virtualizzazione). Nota quali AMI sono del tipo di cui hai bisogno: hvm o paravirtuale. Ad esempio, alcuni tipi di istanza richiedono HVM. Per ulteriori informazioni sui tipi di virtualizzazione Linux, vedere. Tipi di virtualizzazione dell'AMI
- Controllare la modalità di avvio elencata per ogni AMI. Individuare quali AMI utilizzano la modalità di avvio necessaria: legacy-bios, uefi o uefi-preferred. Per ulteriori informazioni, consulta Modalità di avvio di Amazon EC2.
- Scegliere un'AMI conforme alle specifiche esigenze, quindi scegliere Select (Seleziona).

Avviso relativo alle modifiche dell'AMI

Se modifichi la configurazione di volumi o gruppi di sicurezza associati all'AMI selezionata e successivamente scegli un'AMI diversa, viene visualizzata una finestra che informa che alcune delle impostazioni correnti verranno modificate o rimosse. Puoi esaminare le modifiche apportate ai gruppi di sicurezza e ai volumi. Inoltre, puoi visualizzare quali volumi verranno aggiunti ed eliminati oppure visualizzare solo i volumi che verranno aggiunti.

Tipo di istanza

Il tipo di istanza definisce la configurazione hardware e le dimensioni dell'istanza. I tipi di istanza più grandi dispongono di una maggiore quantità di CPU e memoria. Per ulteriori informazioni, consulta Tipi di istanze Amazon EC2.

- Per Tipo di istanza, selezionare il tipo di istanza per l'istanza.

  Piano gratuito: se hai Account AWS meno di 12 mesi, puoi utilizzare Amazon EC2 nel piano gratuito selezionando il tipo di istanza t2.micro (o il tipo di istanza t3.micro nelle regioni in cui t2.micro non è disponibile). Se un tipo di istanza è idoneo al piano gratuito, viene etichettato Idoneo al piano gratuito.
- Confronto dei tipi di istanza: È possibile confrontare diversi tipi di istanza con i seguenti attributi: numero di vCPUs, architettura, quantità di memoria (GiB), quantità di archiviazione (GB), tipo di archiviazione e prestazioni di rete.
- Fatti consigliare: puoi ottenere indicazioni e suggerimenti per i tipi di istanza dal selettore dei tipi di istanza EC2 di Amazon Q. Per ulteriori informazioni, consulta Ottenimento delle raccomandazioni per i tipi di istanza per un nuovo carico di lavoro.

Coppia di chiavi (login)

In Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente oppure scegliere Create new key pair (Crea nuova coppia di chiavi) per creane una nuova. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.

> **Important**
>
> Se si sceglie l'opzione Proceed without key pair (Not recommended) (Procedi senza una coppia di chiavi [non consigliato]), non sarà possibile connetterti all'istanza a meno che non si scelga un'AMI configurata per offrire agli utenti un metodo di accesso alternativo.

Impostazioni di rete

Configurare le impostazioni di rete, se necessario.

- VPC: scegli un VPC esistente per la tua istanza. Puoi scegliere il VPC predefinito o uno creato in precedenza. Per ulteriori informazioni, consulta the section called “Cloud privati virtuali”.
- Sottorete: è possibile avviare un'istanza in una sottorete associata a una zona di disponibilità, una Local Zone, una zona Wavelength o un Outpost.

  Per avviare l'istanza in una zona di disponibilità, selezionare la sottorete in cui avviare l'istanza. Per creare una nuova sottorete, scegliere Create new subnet (Crea nuova sottorete) per passare alla console Amazon VPC. Al termine, tornare alla procedura guidata di avvio istanza e scegliere Refresh (Aggiorna) per caricare la sottorete nell'elenco.

  Per avviare l'istanza in una sottorete solo IPv6, l'istanza deve essere basata su Nitro System.

  Per avviare l'istanza in una Local Zone, selezionare una sottorete creata nella Local Zone.

  Per avviare un'istanza in un Outpost, selezionare una sottorete in un VPC associato a un Outpost.
- Auto-assign Public IP (Assegna IP pubblico automaticamente): specificare se l'istanza riceve un indirizzo IPv4 pubblico. Per impostazione di default, le istanze in una sottorete di default ricevono un indirizzo IPv4 pubblico, al contrario delle istanze in una sottorete non di default. Selezionare Enable (Abilita) o Disable (Disabilita) per sostituire l'impostazione di default della sottorete. Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici.
- Firewall (security groups) (Firewall [gruppi di sicurezza]): utilizzare un gruppo di sicurezza per definire le regole del firewall per l'istanza. Tali regole specificano quale traffico di rete in entrata deve viene distribuito sulla tua istanza. Tutto il traffico rimanente verrà ignorato. Per ulteriori informazioni sui gruppi di sicurezza, consulta Gruppi di sicurezza Amazon EC2 per le tue istanze EC2.

  Se si aggiunge un'interfaccia di rete, si dovrà specificare lo stesso gruppo di sicurezza.

  Selezionare o creare un gruppo di sicurezza nel seguente modo:

  - Per selezionare un gruppo di sicurezza esistente, scegli Select an existing security group (Seleziona un gruppo di sicurezza esistente), quindi seleziona il gruppo di sicurezza da Common security groups (Gruppi di sicurezza comuni).
  - Per creare un nuovo gruppo di sicurezza per il tuo VPC, scegli Create security group (Crea gruppo di sicurezza). La procedura guidata di avvio dell'istanza definisce automaticamente il

gruppo di sicurezza launch-wizard-x e fornisce le seguenti caselle di controllo per aggiungere rapidamente le regole del gruppo di sicurezza:

(Linux) Consenti traffico SSH da: crea una regola in entrata per consentirti di connetterti all'istanza tramite SSH (porta 22).

(Windows) Consenti traffico RDP da: crea una regola in entrata per consentirti di connetterti all'istanza tramite RDP (porta 3389).

Specifica l'origine del traffico: Anywhere (Ovunque), Custom (Personalizzato) o My IP (Il mio IP).

Allow HTTPs traffic from the internet (Consenti traffico HTTPS da Internet): crea una regola in entrata che apre la porta 443 (HTTPS) per consentire il traffico Internet da qualsiasi luogo. Se la tua istanza sarà un server Web, dovrai utilizzare questa regola.

Allow HTTP traffic from the internet (Consenti traffico HTTP da Internet): crea una regola in entrata che apre la porta 80 (HTTP) per consentire il traffico Internet da qualsiasi luogo. Se la tua istanza sarà un server Web, dovrai utilizzare questa regola.

Puoi modificare queste regole e aggiungerne altre in base alle tue esigenze.

Per modificare o aggiungere una regola, scegli Edit (Modifica) in alto a destra. Per aggiungere una regola, scegliere Add security group rule (Aggiungi regola del gruppo di sicurezza). Per Type (Tipo), selezionare il tipo di traffico di rete. Il campo Protocol (Protocollo) viene automaticamente compilato con il protocollo da aprire al traffico di rete. Per Source type (Tipo di origine) scegliere il tipo di origine. Scegli My IP (Il mio IP) per consentire alla procedura guidata di avvio istanza di aggiungere l'indirizzo IP pubblico del computer in uso. Tuttavia, in caso di connessione tramite un ISP o con la protezione di un firewall senza un indirizzo IP statico, è necessario individuare l'intervallo degli indirizzi IP utilizzati dai computer client.

> **Warning**
>
> Le regole che abilitano tutti gli indirizzi IP (`0.0.0.0/0`) per accedere all'istanza tramite SSH o RDP sono accettabili se si avvia brevemente un'istanza di test e la si interrompe o termina presto, ma non sono sicure negli ambienti di produzione. Dovrai autorizzare solo un determinato indirizzo IP o un intervallo di indirizzi per accedere a un'istanza.

- Advanced network configuration (Configurazione avanzata di rete): disponibile solo se si sceglie una sottorete.

Interfaccia di rete

- Device index (Indice dispositivo): l'indice della scheda di rete. L'interfaccia di rete primaria deve essere assegnata all'indice della scheda di rete 0. Alcuni tipi di istanza supportano più schede di rete.
- Network interface (Interfaccia di rete): selezionare New interface (Nuova interfaccia) per consentire ad Amazon EC2 di creare una nuova interfaccia oppure selezionare un'interfaccia di rete esistente disponibile.
- Description (Descrizione): (facoltativo) una descrizione per la nuova interfaccia di rete.
- Subnet (Sottorete): la sottorete nella quale creare la nuova interfaccia di rete. Per l'interfaccia di rete principale, questa è la sottorete in cui viene avviata l'istanza. Se hai inserito un'interfaccia di rete esistente come interfaccia di rete principale, l'istanza viene avviata nella sottorete in cui si trova l'interfaccia di rete.
- Gruppi di sicurezza: i gruppi di sicurezza a cui associare l'interfaccia di rete.
- Primary IP (IP primario): un indirizzo IPv4 privato dall'intervallo della sottorete. Lasciare vuoto il campo per consentire ad Amazon EC2 di scegliere un indirizzo IPv4 privato per tuo conto.
- IP secondario: indirizzi IPv4 privati aggiuntivi dall'intervallo della sottorete. Scegli Assegna manualmente e inserisci un indirizzo IPv4. Scegli Aggiungi IP per aggiungere un altro indirizzo IPv4. In alternativa, scegli Assegna automaticamente e inserisci un valore per indicare il numero di indirizzi IPv4 che Amazon EC2 sceglie per te.
- (solo IPv6) IP IPv6: indirizzi IPv6 dall'intervallo della sottorete. Scegli Assegna manualmente e inserisci un indirizzo IPv6. Scegli Aggiungi IP per aggiungere un altro indirizzo IPv6. In alternativa, scegli Assegna automaticamente e inserisci un valore per indicare il numero di indirizzi IPv6 che Amazon EC2 sceglie per te.
- Prefissi IPv4: prefissi IPv4. Scegli Assegna manualmente e inserisci un prefisso IPv4. In alternativa, scegli Assegna automaticamente e inserisci un valore per indicare il numero di prefissi IPv4 che Amazon EC2 sceglie per te.
- Prefissi IPv6: prefissi IPv6. Scegli Assegna manualmente e inserisci un prefisso IPv6. In alternativa, scegli Assegna automaticamente e inserisci un valore per indicare il numero di prefissi IPv6 che Amazon EC2 sceglie per te.
- (Dual-stack e solo IPv6) Assegna IP IPv6 primario: quando avvii un'istanza in una sottorete dual-stack o solo IPv6, puoi indicare se deve avere un indirizzo IPv6 primario. Questo aiuta a prevenire interruzioni del traffico verso l'istanza o l'interfaccia di rete. Scegli Sì se fai affidamento sul fatto che l'indirizzo IPv6 di questa istanza non cambi e AWS scegli un indirizzo IPv6 associato all'interfaccia di rete come indirizzo IPv6 principale. Non puoi rimuovere l'indirizzo IPv6

primario in un secondo momento. Quando si abilita un indirizzo GUA IPv6 come IPv6 primario, il primo GUA IPv6 diventa l'indirizzo IPv6 principale finché l'istanza non viene terminata o l'interfaccia di rete non viene scollegata. Se hai più indirizzi IPv6 associati a un'interfaccia di rete collegata alla tua istanza e consenti ad Amazon EC2 di assegnare un indirizzo IPv6 primario, il primo indirizzo GUA IPv6 associato all'interfaccia di rete diventa l'indirizzo IPv6 primario.

- Elimina alla terminazione: indica se l'interfaccia di rete viene eliminata quando l'istanza viene eliminata.
- Elastic Fabric Adapter (EFA): indica se l'interfaccia di rete sia di tipo Elastic Fabric Adapter (EFA). Per ulteriori informazioni, consulta Elastic Fabric Adapter.
- ENA Express: ENA Express è alimentato dalla tecnologia AWS Scalable Reliable Datagram (SRD). La tecnologia SRD utilizza un meccanismo di distribuzione dei pacchetti ("packet spraying") per distribuire il carico ed evitare la congestione della rete. L'abilitazione di ENA Express consente alle istanze supportate di comunicare utilizzando SRD in aggiunta al normale traffico TCP, quando possibile. La procedura guidata di avvio dell'istanza non include la configurazione ENA Express per l'istanza, a meno che non si selezioni Abilita o Disabilita dall'elenco.
- UDP ENA Express: se hai abilitato ENA Express, puoi facoltativamente utilizzarlo per il traffico UDP. La procedura guidata di avvio dell'istanza non include la configurazione ENA Express per l'istanza, a meno che non si selezioni Abilita o Disabilita dall'elenco.

Scegli Aggiungi interfaccia di rete per aggiungere interfacce di rete aggiuntive. Le interfacce di rete aggiuntive possono risiedere in una sottorete diversa dello stesso VPC o in una sottorete di un VPC diverso di vostra proprietà (purché la sottorete si trovi nella stessa zona di disponibilità dell'istanza). Se scegli di aggiungere un'interfaccia di rete aggiuntiva che risiede in un'altra sottorete VPC, vedrai l'opzione Subnet multi-VPC quando selezioni una sottorete. Se selezioni una sottorete in un altro VPC, l'etichetta Multi-VPC viene visualizzata accanto all'interfaccia di rete che hai aggiunto. Ciò consente di creare istanze multi-homed su VPC con configurazioni di rete e sicurezza differenti. Tieni presente che se colleghi un ENI aggiuntivo da un altro VPC, devi scegliere un gruppo di sicurezza per l'ENI da quel VPC.

Per ulteriori informazioni, consulta Interfacce di rete elastiche. Se si specifica più di un'interfaccia di rete, l'istanza non può ricevere un indirizzo IPv4 pubblico. Inoltre, se si specifica un'interfaccia di rete esistente per eth0, non è possibile sostituire l'impostazione dell'indirizzo IPv4 pubblico della sottorete utilizzando Auto-assign Public IP (Assegna automaticamente IP pubblico). Per ulteriori informazioni, consulta Assegnare un indirizzo IPv4 pubblico durante l'avvio dell'istanza.

Per configurare l'archiviazione

L'AMI selezionata include uno o più volumi di archiviazione, compreso il volume dispositivo root. È possibile specificare altri volumi da collegare all'istanza.

È possibile utilizzare la vista Semplice o Avanzato. Con la vista Simple (Semplice), si specificano la dimensione e il tipo di volume. Per specificare tutti i parametri del volume, scegli la vista Advanced (Avanzata) (nella parte superiore destra della scheda).

Con la vista Avanzato, è possibile configurare ciascun volume come segue:

- Storage type (Tipo di archiviazione): selezionare volumi Amazon EBS o dell'archivio istanza da associare alla propria istanza. I tipi di volume disponibili nell'elenco dipendono dal tipo di istanza scelta. Per ulteriori informazioni, consulta i volumi Instance store Amazon EC2 e Amazon EBS.
- Device (Dispositivo): selezionare dall'elenco di nomi dei dispositivi disponibili per il volume.
- Snapshot: selezionare lo snapshot da cui ripristinare il volume. È inoltre possibile cercare snapshot pubblici e condivisi disponibili digitando il testo nel campo Snapshot.
- Dimensioni: per i volumi EBS, è possibile specificare una dimensione di archiviazione. Se è stata selezionata un'AMI e l'istanza è idonea per il piano gratuito, per rientrare nel piano gratuito è necessario mantenersi al di sotto dei 30 GiB di archiviazione totale.
- Volume Type (Tipo di volume): per i volumi EBS, selezionare un tipo di volume. Per ulteriori informazioni, consulta i tipi di volume di Amazon EBS nella Amazon EBS User Guide.
- IOPS: se hai selezionato un tipo di volume SSD con capacità di IOPS allocata, puoi inserire il numero di operazioni I/O al secondo (IOPS) supportate dal volume.
- Delete on termination (Elimina alla terminazione): per i volumi Amazon EBS, scegliere Yes (Sì) per eliminare il volume quando l'istanza viene terminata oppure No per conservare il volume. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.
- Encrypted (Crittografato): se il tipo di istanza supporta la crittografia EBS, scegliere Yes (Sì) per abilitare la crittografia per il volume. Se hai abilitato la crittografia per impostazione predefinita in questa regione allora la crittografia è abilitata. Per ulteriori informazioni, consulta Amazon EBS encryption nella Amazon EBS User Guide.
- KMS key (Chiave KMS): se si è selezionato Yes (Sì) per Encrypted (Crittografato), allora è necessario selezionare una chiave gestita dal cliente da utilizzare per crittografare il volume. Se hai abilitato la crittografia per impostazione predefinita in questa Regione, viene selezionata automaticamente la chiave gestita dal cliente predefinita. È possibile selezionare una chiave diversa o specificare l'ARN di qualsiasi chiave gestita dal cliente creata.

- File system: monta un file system Amazon EFS o Amazon FSx sull'istanza. Per ulteriori informazioni su come montare un file system Amazon EFS, consulta Usa Amazon EFS con istanze Linux. Per ulteriori informazioni su come montare un file system Amazon FSx, consulta Utilizzo di Amazon FSx con Amazon EC2

Dettagli avanzati

Per Advanced Details (Dettagli avanzati), espandi la sezione per visualizzare i campi e specifica eventuali parametri aggiuntivi per l'istanza.

- Directory di unione del dominio: seleziona la AWS Directory Service directory (dominio) a cui viene aggiunta l'istanza dopo il lancio. Se si seleziona un dominio, è necessario selezionare un ruolo IAM con le autorizzazioni necessarie. Per ulteriori informazioni sull'aggiunta al dominio, consulta Unire senza interruzioni un'istanza Amazon EC2 Linux alla directory Microsoft AD AWS gestita (istanze Linux) e Unire senza soluzione di continuità un'istanza Amazon EC2 Windows alla directory Microsoft AD AWS gestita (istanze Windows).
- Profilo dell'istanza IAM: seleziona un profilo di istanza AWS Identity and Access Management (IAM) da associare all'istanza. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.
- Hostname type (Tipo di nome host): selezionare se il nome host del sistema operativo guest dell'istanza deve includere il nome della risorsa o il nome IP. Per ulteriori informazioni, consulta Tipi di nomi host delle istanze Amazon EC2.
- DNS Hostname (Nome host DNS): determina se le query DNS al nome IP o al nome della risorsa (a seconda di cosa si seleziona in Hostname type (Tipo di nome host) risponderanno con l'indirizzo IPv4 (registro A), l'indirizzo IPv6 (registro AAAA) o entrambi. Per ulteriori informazioni, consulta Tipi di nomi host delle istanze Amazon EC2.
- Ripristino automatico dell'istanza: se abilitato, ripristina l'istanza se i controlli dello stato del sistema falliscono. Questa impostazione è abilitata per impostazione predefinita all'avvio per i tipi di istanze supportati. Per ulteriori informazioni, consulta Configura il ripristino automatico semplificato.
- Shutdown behavior (Comportamento di arresto): selezionare se l'istanza deve interrompersi o terminare all'arresto. Per ulteriori informazioni, consulta Modifica del comportamento di arresto avviato dall'istanza.
- Stop - Hibernate behavior (Comportamento di interruzione/ibernazione): per abilitare l'ibernazione, scegliere Enable (Abilita). Questa opzione è disponibile solo se l'istanza soddisfa i prerequisiti di ibernazione. Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.
- Termination protection (Protezione da terminazione): per impedire la terminazione accidentale, scegliere Enable (Abilita). Per ulteriori informazioni, consulta Abilitare la protezione da cessazione.

- Protezione da arresto: per evitare l'arresto accidentale, scegli Enable (Abilita). Per ulteriori informazioni, consulta Abilitare la protezione da arresto.
- CloudWatch Monitoraggio dettagliato: scegli Abilita per attivare il monitoraggio dettagliato della tua istanza tramite Amazon CloudWatch. Vengono applicati costi aggiuntivi. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.
- GPU elastica: Amazon Elastic Graphics ha raggiunto la fine del ciclo di vita l'8 gennaio 2024. Per carichi di lavoro che richiedono l'accelerazione grafica, ti consigliamo di utilizzare istanze Amazon EC2 G4ad, G4dn o G5.
- Elastic inference (Inferenza elastica): un acceleratore di inferenza elastica da collegare all'istanza della CPU EC2. Per ulteriori informazioni, consulta la sezione Lavorare con Amazon Elastic Inference nella Guida per gli sviluppatori di Amazon Elastic Inference.

> **Note**
>
> A partire dal 15 aprile 2023, non AWS effettuerà l'onboarding di nuovi clienti in Amazon Elastic Inference (EI) e aiuterà i clienti attuali a migrare i propri carichi di lavoro verso opzioni che offrono prezzi e prestazioni migliori. Dopo il 15 aprile 2023, i nuovi clienti non saranno in grado di avviare istanze con acceleratori Amazon EI su Amazon, SageMaker Amazon ECS o Amazon EC2. Tuttavia, i clienti che hanno utilizzato Amazon EI almeno una volta negli ultimi 30 giorni sono considerati clienti attuali e potranno continuare a usufruire del servizio.

- Credit specification (Specifica credito): scegliere Unlimited (Illimitato) per consentire l'espansione delle applicazioni oltre la baseline per tutto il periodo necessario. Questo campo è valido solo per le istanze T. Potrebbero essere applicati costi aggiuntivi. Per ulteriori informazioni, consulta Istanze a prestazioni espandibili.
- Gruppo di collocamento: specifica un gruppo di collocamento in cui avviare l'istanza. È possibile selezionare un gruppo di collocamento esistente o crearne uno nuovo. Non tutti i tipi di istanza supportano l'avvio di una istanza in un gruppo di collocazione. Per ulteriori informazioni, consulta Gruppi di collocamento.
- EBS-optimized instance (Istanza ottimizzata per EBS): un'istanza ottimizzata per Amazon EBS usa uno stack di configurazione ottimizzato e offre una capacità aggiuntiva dedicata per l'I/O Amazon EBS. Se il tipo di istanza supporta questa caratteristica, scegliere Enable (Abilita) per abilitarla. Vengono applicati costi aggiuntivi. Per ulteriori informazioni, consulta the section called “Ottimizzazione di Amazon EBS”.

- Opzione di acquisto: scegli Istanze Spot per richiedere istanze Spot al prezzo Spot, limitato al prezzo on demand, e scegli le opzioni Personalizza istanze Spot per modificare le impostazioni predefinite dell'istanza Spot. Puoi impostare il prezzo massimo (sconsigliato) e modificare il tipo di richiesta, la durata della richiesta e il comportamento di interruzione. Se non si richiede un'istanza spot, Amazon EC2 avvia un'istanza on demand per impostazione di default. Per ulteriori informazioni, consulta Creare una richiesta di istanza spot.
- Capacity Reservation (Prenotazione di capacità): specificare se avviare l'istanza in una qualsiasi prenotazione della capacità aperta (Open), una prenotazione della capacità specificare (Target by ID) o in un gruppo di prenotazione della capacità (Target by group). Per specificare che non deve essere utilizzata una prenotazione della capacità, selezionare None (Nessuno). Per ulteriori informazioni, consulta Avvio di istanze in una Prenotazione di capacità esistente.
- Tenancy: seleziona se eseguire l'istanza su hardware condiviso (Shared [Condiviso]), isolato, hardware dedicato (Dedicated [Dedicato]) o su un Host dedicato (Dedicated host [Host dedicato]). Se decidi di avviare l'istanza su un Host dedicato, puoi specificare se avviare l'istanza in un gruppo di risorse host o usare uno specifico Host dedicato come target. Potrebbero essere applicati costi aggiuntivi. Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2 e Host dedicati di Amazon EC2.
- RAM disk ID (ID disco RAM) (valido solo per AMI paravirtuali [PV]): selezionare un disco RAM per l'istanza. Se è stato selezionato un kernel, potrebbe essere necessario selezionare un disco RAM specifico con i driver per supportarlo.
- Kernel ID [ID kernel] (valido solo per AMI paravirtuali (PV)): un kernel per l'istanza.
- Nitro Enclave: permette di creare ambienti di esecuzione isolati, denominati enclavi, da istanze Amazon EC2. Seleziona Abilita per abilitare l'istanza per Nitro Enclaves. AWS Per ulteriori informazioni, consulta Che cos'è AWS Nitro Enclaves? nella Guida per l'utente di AWS Nitro Enclaves.
- Configurazioni licenza: è possibile avviare istanze con la configurazione di licenza specificata per tenere traccia dell'utilizzo della licenza. Per ulteriori informazioni, consulta Creazione di una configurazione di licenza nella Guida per l'utente di AWS License Manager.
- Metadati accessibili: è possibile abilitare o disabilitare l'accesso ai metadati dell'istanza. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- Endpoint IPv6 per metadati: è possibile consentire all'istanza di utilizzare l'indirizzo IPv6 IMDS per recuperare i metadati dell'istanza. `[fd00:ec2::254]` Questa opzione è disponibile solo se si avviano istanze create sul sistema AWS Nitro in una sottorete supportata da IPv6 (dual stack o solo IPv6). Per ulteriori informazioni su come recuperare i metadati dell'istanza, consulta Recupero dei metadati dell'istanza.

- Metadata version (Versione dei metadati): se si abilita l'accesso ai metadati dell'istanza, è possibile scegliere di richiedere l'utilizzo di Servizio di metadati dell'istanza Versione 2 quando si richiedono i metadati dell'istanza. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- Limite di hop della risposta dei metadati: se si abilitano i metadati dell'istanza, è possibile impostare il numero consentito di hop di rete per il token dei metadati. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- Allow tags in metadata (Consenti tag nei metadati): se selezioni Enable (Abilita), l'istanza consentirà l'accesso a tutti i suoi tag dai metadati. Se non viene specificato alcun valore, l'accesso ai tag nei metadati dell'istanza non è permesso di default. Per ulteriori informazioni, consulta Per consentire l'accesso ai tag nei metadati delle istanze.
- User data (Dati utente): è possibile specificare i dati utente per configurare un'istanza durante l'avvio o per eseguire uno script di configurazione. Per ulteriori informazioni sui dati utente per le istanze Linux, consulta. Esegui comandi sulla tua istanza Amazon EC2 al momento del lancio Per ulteriori informazioni sui dati utente per le istanze Windows, consulta. In che modo Amazon EC2 gestisce i dati utente per le istanze Windows

Riepilogo

Utilizzare il pannello Summary (Riepilogo) per specificare il numero di istanze da avviare , esaminare la configurazione dell'istanza e avviare le istanze.

- Number of instances (Numero di istanze): immettere il numero di istanze da avviare. Tutte le istanze verranno avviate con la stessa configurazione.

> **Tip**
>
> Per garantire avvii di istanza più veloci, suddividi le richieste di grandi dimensioni in batch più piccoli. Ad esempio, crea cinque richieste di avvio distinte per 100 istanze invece di un'unica richiesta di avvio per 500 istanze.

- (Opzionale) Se viene specificata più di un'istanza, per assicurarsi di disporre del numero corretto di istanze per la gestione del carico di richieste dell'applicazione, è possibile scegliere Consider EC2 Auto Scaling (Considera EC2 Auto Scaling) per creare un modello di avvio e un gruppo Auto Scaling. La funzionalità Auto Scaling dimensiona il numero di istanze nel gruppo in base alle specifiche. Per ulteriori informazioni, consulta Guida per l'utente di Amazon EC2 Auto Scaling.

> **Note**
>
> Se Amazon EC2 Auto Scaling contrassegna un'istanza che si trova in un gruppo Auto Scaling come non integra, l'istanza viene automaticamente pianificata per la sostituzione in cui viene terminata e viene avviata un'altra istanza e i dati dell'istanza originale vengono persi. Un'istanza è contrassegnata come non integra se arresti o riavvii l'istanza o se un altro evento contrassegna l'istanza come non integra. Per ulteriori informazioni, consulta Health checks for instances in an Auto Scaling group nella Amazon EC2 Auto Scaling User Guide.

- Esaminare i dettagli dell'istanza e apportare eventuali modifiche necessarie. È possibile passare direttamente a una sezione scegliendo il relativo collegamento nel pannello Summary (Riepilogo).
- Quando si è pronti per avviare l'istanza, scegliere Launch instance (Avvia istanza).

  Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

  (Facoltativo) È possibile creare un avviso di fatturazione per l'istanza. Nella schermata di conferma, in Next Steps (Fasi successive), scegli Create billing alerts (Crea avvisi di fatturazione) e segui le istruzioni. Gli avvisi di fatturazione possono essere creati anche dopo l'avvio dell'istanza. Per ulteriori informazioni, consulta Creazione di un allarme di fatturazione per monitorare gli AWS addebiti stimati nella Amazon CloudWatch User Guide.

Avvio di un'istanza tramite la vecchia procedura guidata di avvio

Puoi avviare un'istanza tramite la vecchia procedura guidata di avvio solo se anche la regione la supporta. La procedura guidata di avvio dell'istanza specifica tutti i parametri di avvio necessari per avviare un'istanza. Se la procedura guidata di lancio dell'istanza fornisce un valore predefinito, è possibile accettare il valore predefinito o specificare il proprio valore. È necessario specificare un'AMI e una coppia di chiavi per avviare un'istanza.

Per le istruzioni per l'uso della nuova procedura guidata di avvio dell'istanza, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

> **Important**
>
> Quando avvii un'istanza che non rientra nel Piano gratuito di AWS, ti viene addebitato il tempo in cui l'istanza è in esecuzione, anche se rimane inattiva.

Fasi di lancio di un'istanza:

- Iniziare il lancio dell'istanza
- Fase 1: scelta di un'Amazon Machine Image (AMI)
- Fase 2: scegliere un tipo di istanza
- Fase 3: configurare i dettagli dell'istanza
- Fase 4: aggiungere archiviazione
- Fase 5: aggiungi i tag
- Fase 6: configura il gruppo di sicurezza
- Fase 7: rivedere l'avvio dell'istanza e selezionare la coppia di chiavi

Iniziare il lancio dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore della schermata, viene visualizzata la regione corrente (ad esempio US East [Ohio]). Seleziona una regione per l'istanza che soddisfa le tue esigenze. Questa scelta è importante perché, a differenza di altre, alcune risorse Amazon EC2 possono essere condivise tra più regioni. Per ulteriori informazioni, consulta Posizioni delle risorse.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).

Fase 1: scelta di un'Amazon Machine Image (AMI)

Quando avvii un'istanza, devi selezionare una configurazione, anche nota come Amazon Machine Image (AMI). Un'AMI contiene le informazioni necessarie per creare una nuova istanza. Ad esempio, un'AMI potrebbe contenere il software necessario per fungere da server Web, come Linux, Apache e il tuo sito Web.

Quando avvii un'istanza, puoi selezionare un'AMI dall'elenco o selezionare un parametro Systems Manager che punta ad un ID AMI. Per ulteriori informazioni, consulta the section called “Trova un'AMI utilizzando un parametro Systems Manager”.

Nella pagina Choose an Amazon Machine Image (AMI) (Scegli Amazon Machine Image [AMI]), utilizza una delle due opzioni per scegliere un'AMI. Cerca nell'elenco di AMI o cerca in base al parametro Systems Manager.

Per ricerca nell'elenco di AMI

1. Selezionare il tipo di AMI da utilizzare nel riquadro a sinistra:

   Quick Start

   Una selezione di AMI più comunemente usate per iniziare rapidamente a utilizzare il prodotto. Per selezionare un'AMI adatta al piano gratuito, scegliere Free tier only (Solo piano gratuito) nel riquadro a sinistra. Queste AMI sono contrassegnate dalla dicitura Free tier eligible (Idoneo al piano gratuito).

   My AMIs (Le mie AMI)

   AMI private di proprietà o AMI private condivise da altri utenti. Per visualizzare le AMI condivise, scegliere Shared with me (Condivisi con me) nel riquadro a sinistra.

   Marketplace AWS

   Un negozio online in cui è possibile acquistare software che funziona su AWS, tra cui AMI. Per ulteriori informazioni sull'avvio di un'istanza da Marketplace AWS, consulta. Avvia un' Marketplace AWS istanza

   Community AMIs (AMI della community)

   Le AMI che i membri AWS della community hanno reso disponibili per l'uso da parte di altri utenti. Per filtrare l'elenco di AMI in base al sistema operativo, scegliere la casella di controllo appropriata in Operating system (Sistema operativo). È anche possibile filtrare in base all'architettura e al tipo di dispositivo root.

2. (istanze Linux) Controlla il tipo di dispositivo root elencato per ogni AMI. Individuare le AMI del tipo desiderato: `ebs` (supportate da Amazon EBS) o `instance-store` (supportate da instance store). Per ulteriori informazioni, consulta Archiviazione del dispositivo root.
3. Controllare le voci per ciascuna AMI nell'elenco Virtualization type (Tipo di virtualizzazione). Individuare le AMI del tipo desiderato: `hvm` o `paravirtual`. Ad esempio, alcuni tipi di istanza

richiedono HVM. Per ulteriori informazioni sui tipi di virtualizzazione Linux, vedere. Tipi di virtualizzazione dell'AMI

4. Controllare la modalità di avvio elencata per ogni AMI. Individuare quali AMI utilizzano la modalità di avvio necessaria, `legacy-bios` o `uefi`. Per ulteriori informazioni, consulta Modalità di avvio di Amazon EC2.
5. Scegliere un'AMI conforme alle specifiche esigenze, quindi scegliere Select (Seleziona).

Per parametro Systems Manager

1. Scegliere Search by Systems Manager parameter (Cerca per parametro Systems Manager) (in alto a destra).
2. Per Systems Manager parameter (Parametro Systems Manager), selezionare un parametro. L'ID AMI corrispondente viene visualizzato accanto a Currently resolves to (Attualmente si risolve in).
3. Selezionare Search (Cerca). Le AMI che corrispondono all'ID AMI vengono visualizzate nell'elenco.
4. Selezionare l'AMI dall'elenco e scegliere Select (Seleziona).

Fase 2: scegliere un tipo di istanza

Nella pagina Choose an Instance Type (Scegli un tipo di istanza), selezionare la configurazione hardware e le dimensioni dell'istanza da avviare. I tipi di istanza più grandi dispongono di una maggiore quantità di CPU e memoria. Per ulteriori informazioni, consulta Tipi di istanza Amazon EC2.

Per rimanere idoneo per il livello libero, scegliere il tipo di istanza t2.micro (o il tipo di istanza t3.micro nelle regioni in cui t2.micro non è disponibile). Se un tipo di istanza è idoneo al piano gratuito, viene etichettato Idoneo al piano gratuito.

Per impostazione di default, la procedura guidata visualizza i tipi di interfaccia della generazione corrente e seleziona il primo tipo di istanza disponibile in base all'AMI selezionata. Per visualizzare i tipi di istanza di generazioni precedenti, scegliere All generations (Tutte le generazioni) nell'elenco dei filtri.

> **Note**
>
> Per configurare rapidamente un'istanza a scopo di test, scegliere Review and Launch (Analizza e avvia) per accettare le impostazioni di configurazione di default e avviare

l'istanza. In caso contrario, per configurare ulteriormente l'istanza scegliere Next: Configure Instance Details (Successivo: Configura dettagli dell'istanza).

Fase 3: configurare i dettagli dell'istanza

Nella pagina Configure Instance Details (Configura dettagli dell'istanza), modificare le seguenti impostazioni se necessario (espandere Advanced Details (Dettagli avanzati) per visualizzare tutte le informazioni), quindi scegliere Next: Add storage (Successivo: Aggiungi archiviazione):

- Number of instances (Numero di istanze): immettere il numero di istanze da avviare.

  > **Tip**
  >
  > Per garantire avvii di istanza più veloci, suddividi le richieste di grandi dimensioni in batch più piccoli. Ad esempio, crea cinque richieste di avvio distinte per 100 istanze invece di un'unica richiesta di avvio per 500 istanze.

- (Opzionale) Per assicurarsi di disporre del numero corretto di istanze per la gestione del carico di richieste dell'applicazione, è possibile scegliere Launch into Auto Scaling Group (Avvio nel gruppo Auto Scaling) per creare una configurazione di avvio e un gruppo Auto Scaling. La funzionalità Auto Scaling dimensiona il numero di istanze nel gruppo in base alle specifiche. Per ulteriori informazioni, consulta Guida per l'utente di Amazon EC2 Auto Scaling.

  > **Note**
  >
  > Se Amazon EC2 Auto Scaling contrassegna un'istanza che si trova in un gruppo Auto Scaling come non integra, l'istanza viene automaticamente pianificata per la sostituzione in cui viene terminata e viene avviata un'altra istanza e i dati dell'istanza originale vengono persi. Un'istanza è contrassegnata come non integra se arresti o riavvii l'istanza o se un altro evento contrassegna l'istanza come non integra. Per ulteriori informazioni, consulta Controllo dello stato nelle istanze Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.

- Purchasing option (Opzioni di acquisto): selezionare Request Spot Instances (Richiedi istanze spot) per avviare un'istanza spot. Ciò consente di aggiungere e rimuovere le opzioni da questa pagina. Puoi impostare il prezzo massimo (sconsigliato) e modificare facoltativamente il tipo di

richiesta, il comportamento di interruzione e la validità della richiesta. Per ulteriori informazioni, consulta Creare una richiesta di istanza spot.

- Network (Rete): seleziona il VPC oppure crea un nuovo VPC scegliendo Create new VPC (Crea nuovo VPC) e passando alla console Amazon VPC. Al termine, tornare alla procedura guidata di avvio dell'istanza e scegliere Refresh (Aggiorna) per caricare il VPC nell'elenco.
- Sottorete: puoi avviare un'istanza in una sottorete associata a una zona di disponibilità, una Local Zone, una zona Wavelength o un Outpost.

  Per avviare l'istanza in una zona di disponibilità, selezionare la sottorete in cui avviare l'istanza. È possibile selezionare Nessuna preferenza per consentire di AWS scegliere una sottorete predefinita in qualsiasi zona di disponibilità. Per creare una nuova sottorete, scegliere Create new subnet (Crea nuova sottorete) per passare alla console Amazon VPC. Al termine, tornare alla procedura guidata e scegliere Refresh (Aggiorna) per caricare la sottorete nell'elenco.

  Per avviare l'istanza in una Local Zone, selezionare una sottorete creata nella Local Zone.

  Per avviare un'istanza in un Outpost, selezionare una sottorete in un VPC associato a un Outpost.
- Auto-assign Public IP (Assegna IP pubblico automaticamente): specificare se l'istanza riceve un indirizzo IPv4 pubblico. Per impostazione di default, le istanze in una sottorete di default ricevono un indirizzo IPv4 pubblico, al contrario delle istanze in una sottorete non di default. Selezionare Enable (Abilita) o Disable (Disabilita) per sostituire l'impostazione di default della sottorete. Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici.
- Auto-assign IPv6 IP (Assegna IP IPv6 automaticamente): specificare se l'istanza riceve un indirizzo IPv6 dall'intervallo della sottorete. Selezionare Enable (Abilita) o Disable (Disabilita) per sostituire l'impostazione predefinita della sottorete. Questa opzione è disponibile solo se al VPC e alla sottorete è associato un blocco CIDR IPv6. Per ulteriori informazioni, consulta Aggiunta di blocchi CIDR IPv6 a un VPC nella Guida per l'utente di Amazon VPC.
- Hostname type (Tipo di nome host): selezionare se il nome host del sistema operativo guest dell'istanza deve includere il nome della risorsa o il nome IP. Per ulteriori informazioni, consulta Tipi di nomi host delle istanze Amazon EC2.
- DNS Hostname (Nome host DNS): determina se le query DNS al nome IP o al nome della risorsa (a seconda di cosa si seleziona in Hostname type (Tipo di nome host) risponderanno con l'indirizzo IPv4 (registro A), l'indirizzo IPv6 (registro AAAA) o entrambi. Per ulteriori informazioni, consulta Tipi di nomi host delle istanze Amazon EC2.
- Directory di unione del dominio: seleziona la AWS Directory Service directory (dominio) a cui viene aggiunta l'istanza dopo il lancio. Se si seleziona un dominio, è necessario selezionare un

ruolo IAM con le autorizzazioni necessarie. Per ulteriori informazioni sull'aggiunta al dominio, consulta Unire senza interruzioni un'istanza Amazon EC2 Linux alla directory Microsoft AD AWS gestita (istanze Linux) e Unire senza soluzione di continuità un'istanza Amazon EC2 Windows alla directory Microsoft AD AWS gestita (istanze Windows).

- Placement group name (Nome del gruppo di collocamento): un gruppo di collocamento determina la strategia di posizionamento delle istanze. Selezionare un gruppo di collocamento esistente o crearne uno nuovo. Questa opzione è disponibile solo se è stato selezionato un tipo di istanza che supporta i gruppi di collocamento. Per ulteriori informazioni, consulta Gruppi di collocamento.
- Prenotazione di capacità: specificare se avviare l'istanza in capacità condivisa, qualsiasi open Prenotazione di capacità, uno specifico Prenotazione di capacità o un gruppo Prenotazione di capacità. Per ulteriori informazioni, consulta Avvio di istanze in una Prenotazione di capacità esistente.
- Ruolo IAM: seleziona un ruolo AWS Identity and Access Management (IAM) da associare all'istanza. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.
- CPU options (Opzioni CPU): selezionare Specify CPU options (Specifica le opzioni CPU) per specificare un numero personalizzato di vCPU durante l'avvio. Imposta il numero di thread per core e di core CPU. Per ulteriori informazioni, consulta Ottimizzazione delle opzioni della CPU.
- Shutdown behavior (Comportamento di arresto): selezionare se l'istanza deve interrompersi o terminare all'arresto. Per ulteriori informazioni, consulta Modifica del comportamento di arresto avviato dall'istanza.
- Stop - Hibernate behavior (Comportamento di interruzione/ibernazione): per abilitare l'ibernazione, selezionare questa casella di controllo. Questa opzione è disponibile solo se l'istanza soddisfa i prerequisiti di ibernazione. Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.
- Enable termination protection (Abilita la protezione da interruzione): per impedire l'interruzione accidentale, selezionare questa casella di controllo. Per ulteriori informazioni, consulta Abilitare la protezione da cessazione.
- Enable termination protection (Abilita la protezione da interruzione): per impedire l'interruzione accidentale, seleziona questa casella di controllo. Per ulteriori informazioni, consulta Abilitare la protezione da arresto.
- Monitoraggio: seleziona questa casella di controllo per attivare il monitoraggio dettagliato della tua istanza tramite Amazon CloudWatch. Vengono applicati costi aggiuntivi. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.

- Istanza ottimizzata per EBS: un'istanza ottimizzata per Amazon EBS usa uno stack di configurazione ottimizzato e offre una capacità aggiuntiva dedicata per l'I/O Amazon EBS. Se il tipo di istanza supporta questa caratteristica, seleziona questa casella di spunta per abilitarla. Vengono applicati costi aggiuntivi. Per ulteriori informazioni, consulta Amazon EBS: tipi di istanza ottimizzati.
- Tenancy: in caso di avvio dell'istanza in un VPC, puoi scegliere di eseguire l'istanza su hardware dedicato isolato (Dedicated (Dedicato)) oppure su un host dedicato (Dedicated host [Host dedicato]). Potrebbero essere applicati costi aggiuntivi. Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2 e Host dedicati di Amazon EC2.
- T2/T3 Unlimited (Illimitato T2/T3): selezionare questa casella di controllo per consentire l'espansione delle applicazioni oltre la baseline per tutto il periodo necessario. Potrebbero essere applicati costi aggiuntivi. Per ulteriori informazioni, consulta Istanze a prestazioni espandibili.
- File system: per creare un nuovo file system da montare sull'istanza, scegliere Create new file system (Crea nuovo file system), immettere un nome per il nuovo file system, quindi scegliere Create (Crea). Il file system viene creato utilizzando la creazione rapida di Amazon EFS, che applica le impostazioni consigliate per il servizio. I gruppi di sicurezza necessari per abilitare l'accesso al file system vengono automaticamente creati e collegati all'istanza e alle destinazioni di montaggio del file system. È inoltre possibile scegliere di creare e allegare manualmente i gruppi di sicurezza richiesti. Per montare uno o più file system Amazon EFS esistenti nell'istanza, scegliere Add file system (Aggiungi file system), quindi scegliere i file system da montare e i punti di montaggio da utilizzare. Per ulteriori informazioni, consulta Usa Amazon EFS con istanze Linux.
- Network interfaces (Interfacce di rete): se viene selezionata una sottorete specifica, è possibile specificare fino a due interfacce di rete per l'istanza:
  - Per Interfaccia di rete, seleziona Nuova interfaccia di rete per consentire la AWS creazione di una nuova interfaccia o seleziona un'interfaccia di rete esistente e disponibile.
  - Per IP primario, inserisci un indirizzo IPv4 privato dall'intervallo della sottorete o lascia che venga assegnato automaticamente l'indirizzo IPv4 per AWS scegliere un indirizzo IPv4 privato per te.
  - Per Secondary IP addresses (Indirizzi IP secondari), scegliere Add IP (Aggiungi IP) per assegnare più di un indirizzo IPv4 privato all'interfaccia di rete selezionata.
  - (Solo IPv6) Per gli IP IPv6, scegli Aggiungi IP e inserisci un indirizzo IPv6 dall'intervallo della sottorete oppure lascia che sia tu a sceglierne uno automaticamente. AWS
  - Indice scheda di rete: l'indice della scheda di rete. L'interfaccia di rete primaria deve essere assegnata all'indice della scheda di rete 0. Alcuni tipi di istanza supportano più schede di rete.

- Scegliere Add Device (Aggiungi dispositivo) per aggiungere un'interfaccia di rete secondaria. Un'interfaccia di rete secondaria può trovarsi in una sottorete diversa del VPC, a condizione che sia nella stessa zona di disponibilità dell'istanza.

Per ulteriori informazioni, consulta Interfacce di rete elastiche. Se si specifica più di un'interfaccia di rete, l'istanza non può ricevere un indirizzo IPv4 pubblico. Inoltre, se si specifica un'interfaccia di rete esistente per eth0, non è possibile sostituire l'impostazione dell'indirizzo IPv4 pubblico della sottorete utilizzando Auto-assign Public IP (Assegna automaticamente IP pubblico). Per ulteriori informazioni, consulta Assegnare un indirizzo IPv4 pubblico durante l'avvio dell'istanza.

- Kernel ID (ID kernel): (valido solo per AMIs paravirtuali [PV]) Selezionare Use default (Utilizza le impostazioni predefinite) a meno che non si desideri utilizzare un kernel specifico.
- RAM disk ID (ID disco RAM): (valido solo per AMIs paravirtuali [PV]) Selezionare Use default (Utilizza impostazioni predefinite) a meno che non si desideri utilizzare un disco RAM specifico. Se è stato selezionato un kernel, potrebbe essere necessario selezionare un disco RAM specifico con i driver per supportarlo.
- Enclave: seleziona Enable per abilitare l'istanza per Nitro Enclaves. AWS Per ulteriori informazioni, consulta Che cos'è Nitro Enclaves? AWS nella Guida per l'utente di AWS Nitro Enclaves.
- Metadati accessibili: puoi abilitare o disabilitare l'accesso al Servizio di metadati dell'istanza (IMDS). Per ulteriori informazioni, consulta Usa IMDSv2.
- Endpoint IPv6 per metadati: è possibile consentire all'istanza di utilizzare l'indirizzo IPv6 IMDS per recuperare i metadati dell'istanza. `[fd00:ec2::254]` Questa opzione è disponibile solo se si avviano istanze create sul sistema AWS Nitro in una sottorete supportata da IPv6 (dual stack o solo IPv6). Per ulteriori informazioni su come recuperare i metadati dell'istanza, consulta Recupero dei metadati dell'istanza.
- Versione dei metadati: se abiliti l'accesso a IMDS, puoi scegliere di richiedere l'utilizzo di Servizio di metadati dell'istanza Versione 2 quando si richiedono i metadati dell'istanza. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- Limite di hop di risposta di token di metadati: se abiliti l'accesso a IMDS, puoi impostare il numero consentito di hop di rete per il token dei metadati. Per ulteriori informazioni, consulta Usa IMDSv2.
- User data (Dati utente): è possibile specificare i dati utente per configurare un'istanza durante l'avvio o per eseguire uno script di configurazione. Per collegare un file, selezionare l'opzione As file (Come file) e cercare il file da collegare.

Fase 4: aggiungere archiviazione

L'AMI selezionata include uno o più volumi di storage, compreso il volume dispositivo root. Nella pagina Add storage (Aggiungi archiviazione), è possibile specificare altri volumi da collegare all'istanza scegliendo Add New Volume (Aggiungi nuovo volume). Configura ogni volume come segue, quindi scegli Next: Add Tags (Successivo: Aggiungi tag).

- Type (Tipo): selezionare l'instance store o i volumi Amazon EBS da associare all'istanza. I tipi di volume disponibili nell'elenco dipendono dal tipo di istanza scelta. Per ulteriori informazioni, consulta i volumi Instance store Amazon EC2 e Amazon EBS.
- Device (Dispositivo): selezionare dall'elenco di nomi di dispositivo disponibili per il volume.
- Snapshot: immettere il nome o l'ID dello snapshot in base al quale ripristinare un volume. È inoltre possibile cercare snapshot pubblici e condivisi disponibili digitando il testo nel campo Snapshot. Le descrizioni degli snapshot fanno distinzione tra maiuscole e minuscole.
- Size (Dimensioni): per i volumi supportati da EBS, è possibile specificare una dimensione di archiviazione. Anche se è stata selezionata un'AMI e l'istanza è idonea per il piano gratuito, per rientrare nel piano gratuito è necessario mantenersi al di sotto dei 30 GiB di archiviazione totale.
- Volume Type (Tipo di volume): per i volumi EBS, selezionare un tipo di volume. Per ulteriori informazioni, consulta i tipi di volume di Amazon EBS nella Amazon EBS User Guide.
- IOPS: se hai selezionato un tipo di volume SSD con capacità di IOPS allocata, puoi inserire il numero di operazioni I/O al secondo (IOPS) supportate dal volume.
- Delete on Termination (Elimina al termine): per i volumi Amazon EBS, seleziona questa casella di controllo quando l'istanza viene terminata. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.
- Encrypted (Crittografato): se il tipo di istanza supporta la crittografia su EBS, puoi specificare lo stato di crittografia del volume. Se hai abilitato la crittografia per impostazione predefinita in questa Regione, viene selezionata automaticamente la chiave gestita dal cliente predefinita. Puoi selezionare una chiave diversa o disabilitare la crittografia. Per ulteriori informazioni, consulta Amazon EBS encryption nella Amazon EBS User Guide.

Fase 5: aggiungi i tag

Nella pagina Add Tags (Aggiungi tag), specificare i tag immettendo le combinazioni di chiave e valore. È possibile contrassegnare con tag l'istanza, i volumi o entrambi. Per le istanze spot, è possibile aggiungere un tag solo alla richiesta di istanza spot. Scegliere Add another tag (Aggiungi

un altro tag) per aggiungere più di un tag alle risorse. Scegliere Next: Configure Security Group (Successivo: Configura il gruppo di sicurezza).

Fase 6: configura il gruppo di sicurezza

Nella pagina Configure Security Group (Configura il gruppo di sicurezza), selezionare un gruppo di sicurezza per definire le regole del firewall per l'istanza. Tali regole specificano quale traffico di rete in entrata deve viene distribuito sulla tua istanza. Tutto il traffico rimanente verrà ignorato. Per ulteriori informazioni sui gruppi di sicurezza, consulta Gruppi di sicurezza Amazon EC2 per le tue istanze EC2. Selezionare o creare un gruppo di sicurezza nel seguente modo, quindi scegliere Review and Launch (Analizza e avvia).

- Per selezionare un gruppo di sicurezza esistente, scegliere Select an existing security group (Seleziona un gruppo di sicurezza esistente), quindi selezionare il gruppo di sicurezza. Non è possibile modificare le regole di un gruppo di sicurezza esistente, ma è possibile copiarle in un nuovo gruppo scegliendo Copy to new (Copia su nuovo). A questo punto, puoi aggiungere le regole come descritto nella fase successiva.
- Per creare un nuovo gruppo di sicurezza, scegliere Create a new security group (Crea un nuovo gruppo di sicurezza). La procedura guidata definisce automaticamente il gruppo di sicurezza launch-wizard- x e crea una regola in entrata per consentirti di connetterti alla tua istanza. Le istanze Linux utilizzano una regola in entrata per SSH (porta 22) e le istanze Windows utilizzano una regola in entrata per RDP (porta 3389).
- È possibile aggiungere regole in base alle tue esigenze. Ad esempio, se l'istanza è un server Web, aprire le porte 80 (HTTP) e 443 (HTTPS) per consentire il traffico Internet.

  Per aggiungere una regola, scegliere Add Rule (Aggiungi regola), selezionare il protocollo per aprire il traffico di rete, quindi specificare l'origine. Scegliere My IP (Il mio IP) dall'elenco Source (Origine) per consentire alla procedura guidata di aggiungere l'indirizzo IP pubblico del computer in uso. Tuttavia, in caso di connessione tramite un ISP o con la protezione di un firewall senza un indirizzo IP statico, è necessario individuare l'intervallo degli indirizzi IP utilizzati dai computer client.

  > **Warning**
  >
  > Le regole che consentono a tutti gli indirizzi IP (`0.0.0.0/0`) di accedere all'istanza tramite SSH o RDP sono accettabili per questo breve esercizio, ma non sono sicure negli ambienti

di produzione. Dovrai autorizzare solo un determinato indirizzo IP o un intervallo di indirizzi per accedere a un'istanza.

Fase 7: rivedere l'avvio dell'istanza e selezionare la coppia di chiavi

Nella pagina Review Instance Launch (Rivedi l'avvio dell'istanza), controllare i dettagli dell'istanza e apportare le modifiche necessarie scegliendo il collegamento Edit (Modifica) appropriato.

Al termine, scegliere Launch (Avvia).

Nella finestra di dialogo Select an existing key pair or create a new key pair (Seleziona una coppia di chiavi esistente o crea una nuova coppia di chiavi), è possibile scegliere una coppia di chiavi esistenti o crearne una nuova. Ad esempio, scegliere Choose an existing key pair (Scegli una coppia di chiavi esistente), quindi selezionare la coppia di chiavi creata durante la configurazione. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.

Important

Se scegli l'opzione Proceed without key pair (Procedi senza una coppia di chiavi), non sarai in grado di connetterti all'istanza a meno che tu non scelga un'AMI configurata per offrire agli utenti un metodo di accesso alternativo.

Per avviare l'istanza, selezionare la casella di controllo di conferma, quindi scegliere Launch Instances (Avvia istanze).

(Opzionale) È possibile creare un allarme di verifica dello stato per l'istanza (potrebbero essere applicati costi aggiuntivi). Nella schermata di conferma, scegliere Create status check alarms (Crea allarmi di verifica stato) e seguire le istruzioni. È possibile creare gli allarmi di controllo dello stato anche dopo l'avvio dell'istanza. Per ulteriori informazioni, consulta Creazione e modifica degli allarmi di controllo dello stato.

Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

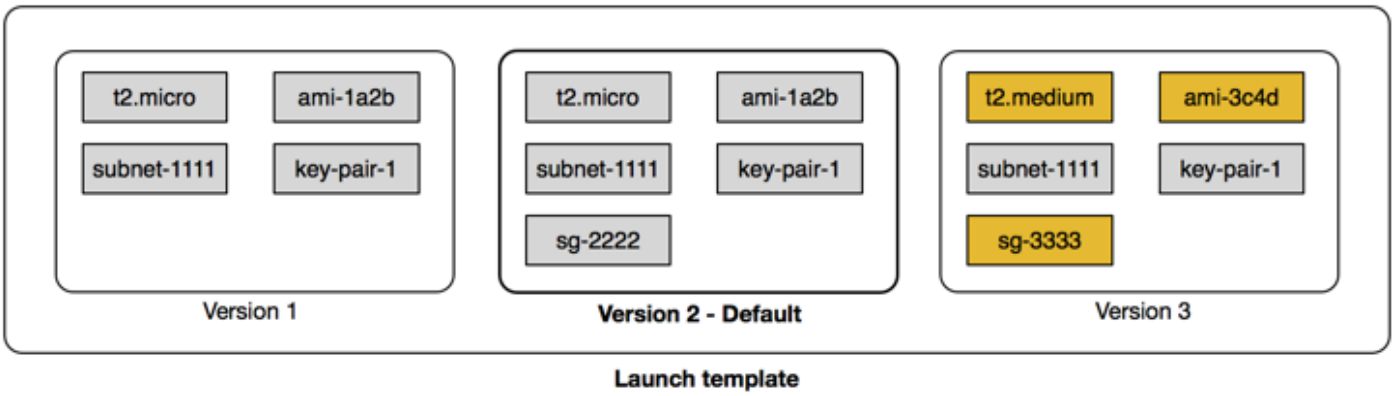
Avvio di un'istanza da un modello di avvio

È possibile utilizzare un modello di avvio per memorizzare i parametri di avvio dell'istanza in modo da non doverli specificare ogni volta che si avvia un'istanza. Ad esempio, puoi creare un modello di avvio

con l'ID AMI, il tipo di istanza e le impostazioni di rete che utilizzi in genere per avviare le istanze. Quando avvii un'istanza utilizzando la console Amazon EC2, un AWS SDK o uno strumento da riga di comando, puoi specificare il modello di avvio anziché inserire nuovamente i parametri.

Per ogni modello di avvio, è possibile creare una o più versioni del modello di avvio numerate. Ogni versione può avere parametri di lancio diversi. Quando avvii un'istanza da un modello di avvio, è possibile utilizzare qualsiasi versione del modello di avvio. Se non specifichi una versione, viene utilizzata la versione predefinita. È possibile impostare qualsiasi versione del modello di avvio come versione predefinita; per impostazione predefinita, è la prima versione del modello di avvio.

Nel seguente diagramma viene indicato il modello di avvio con tre versioni. La prima versione specifica il tipo di istanza, l'ID istanza AMI, la sottorete e la coppia di chiavi da utilizzare per avviare l'istanza. La seconda versione è basata sulla prima versione e specifica anche un gruppo di sicurezza per l'istanza. La terza versione utilizza valori diversi per alcuni parametri. La versione 2 è impostata come versione predefinita. Se avviassi un'istanza da questo modello di avvio, i parametri di lancio dalla versione 2 verrebbero utilizzati se non fosse stata specificata un'altra versione.



Indice

- Limiti modello di avvio
- Controllo dell'accesso ai modelli di avvio con le autorizzazioni IAM
- Utilizzo dei modelli di avvio per controllare l'avvio delle istanze
- Creazione di un modello di avvio
- Modificare un modello di avvio (gestire le versioni dei modelli di avvio)
- Eliminare un modello di avvio
- Avvio di istanze da un modello di avvio

Limiti modello di avvio

Le seguenti regole si applicano ai modelli di avvio e alle versioni del modello di avvio:

- Quote: per visualizzare le quote per i modelli di lancio e le versioni dei modelli di avvio, apri la console Service Quotas o usa il comando. list-service-quotas AWS CLI Ogni AWS account può avere fino a un massimo di 5.000 modelli di lancio per regione e fino a 10.000 versioni per modello di lancio. I tuoi account potrebbero avere quote diverse in base all'età e alla cronologia di utilizzo.
- I parametri sono facoltativi: i parametri del modello di avvio sono facoltativi. Tuttavia, è necessario verificare che la richiesta di avvio di un'istanza includa tutti i parametri necessari. Ad esempio, se il modello di avvio non include un ID istanza AMI, è necessario specificare sia il modello di avvio sia un ID istanza AMI quando avvii un'istanza.
- I parametri non sono convalidati: i parametri del modello di avvio non sono pienamente convalidati quando crei il modello di avvio. Se si specificano valori errati per i parametri o se non si utilizzano combinazioni di parametri supportate, non è possibile avviare istanze utilizzando questo modello di avvio. Assicurati di specificare i valori corretti per i parametri e di utilizzare le combinazioni di parametri supportate. Ad esempio, per avviare un'istanza in un gruppo di collocamento, è necessario specificare un tipo di istanza supportato.
- Tag: è possibile assegnare dei tag a un modello di avvio, ma non è possibile assegnare tag a una versione del modello di avvio.
- Immutabilità: i modelli di avvio sono immutabili. Per modificare un modello di avvio, è necessario creare una nuova versione del modello di avvio.
- Numeri di versione: le versioni del modello di avvio sono numerate nell'ordine in cui sono state create. Quando crei una versione del modello di avvio, non è possibile specificare il numero di versione.

Controllo dell'accesso ai modelli di avvio con le autorizzazioni IAM

È possibile utilizzare le autorizzazioni IAM per controllare quali operazioni del modello di avvio possono eseguire gli utenti, come la visualizzazione, la creazione o l'eliminazione dei modelli di avvio.

Quando concedi agli utenti il permesso di creare modelli di lancio e lanciare versioni dei modelli, non puoi utilizzare le autorizzazioni a livello di risorsa per limitare le risorse che possono specificare in un modello di lancio. Pertanto, assicuratevi di concedere le autorizzazioni per creare modelli di lancio e avviare versioni dei modelli solo agli amministratori appropriati.

È necessario concedere a chiunque utilizzerà un modello di lancio le autorizzazioni necessarie per creare e accedere alle risorse specificate nel modello di lancio. Per esempio:

- Per avviare un'istanza da un'Amazon Machine Image (AMI) privata condivisa, l'utente deve disporre dell'autorizzazione di avvio per l'AMI.
- Per creare volumi EBS con tag tratti da istantanee esistenti, l'utente deve disporre dell'accesso in lettura alle istantanee e delle autorizzazioni per creare e contrassegnare volumi.

Indice

ec2: CreateLaunchTemplate

Per creare un modello di avvio nella console o utilizzando le API, il principale deve disporre dell'autorizzazione `ec2:CreateLaunchTemplate` in una policy IAM. Quando possibile, è consigliabile utilizzare i tag per controllare l'accesso ai modelli di avvio nell'account.

Ad esempio, la seguente istruzione di policy IAM fornisce al principale l'autorizzazione per creare modelli di avvio solo se il modello utilizza il tag specificato (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
    "Action": "ec2:CreateLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

I principali che creano i modelli di avvio potrebbero richiedere alcune autorizzazioni correlate, come ad esempio:

- ec2: CreateTags — Per aggiungere tag al modello di avvio durante l'`CreateLaunchTemplate`operazione, il `CreateLaunchTemplate` chiamante deve disporre dell'`ec2:CreateTags`autorizzazione in una policy IAM.
- ec2: RunInstances — Per avviare le istanze EC2 dal modello di avvio che hanno creato, il principale deve inoltre disporre dell'`ec2:RunInstances`autorizzazione in una policy IAM.

Per le operazioni di creazione delle risorse in cui vengono applicati i tag, gli utenti devono disporre dell'autorizzazione `ec2:CreateTags`. La seguente istruzione di policy IAM utilizza la chiave di condizione `ec2:CreateAction` per consentire agli utenti di creare i tag soltanto nel contesto di `CreateLaunchTemplate`. Gli utenti non possono aggiungere tag ai modelli di avvio o altre risorse esistenti. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

```
{
    "Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
    "Action": "ec2:CreateTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateLaunchTemplate"
        }
    }
}
```

L'utente IAM che crea un modello di avvio non dispone automaticamente dell'autorizzazione a utilizzare il modello di avvio che ha creato. Come qualsiasi altro principale, il creatore del modello di avvio deve ottenere l'autorizzazione tramite una policy IAM. Se un utente IAM desidera avviare un'istanza EC2 da un modello di avvio, deve disporre dell'autorizzazione `ec2:RunInstances`. Quando si concedono queste autorizzazioni, è possibile specificare che gli utenti possono utilizzare solo modelli di avvio con tag o ID specifici. Inoltre, è possibile controllare l'AMI e altre risorse alle quali chiunque utilizzi i modelli di avvio può fare riferimento e che può utilizzare per avviare le istanze specificando le autorizzazioni a livello di risorsa per la chiamata `RunInstances`. Per esempi di policy, consulta Modelli di lancio.

ec2: DescribeLaunchTemplates

Per elencare i modelli di avvio nell'account, il principale deve disporre dell'autorizzazione `ec2:DescribeLaunchTemplates` in una policy IAM. Dato che le operazioni `Describe` non supportano le autorizzazioni a livello di risorsa, devono essere specificate senza condizioni e il valore dell'elemento risorsa nella policy deve essere `"*"`.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per elencare tutti i modelli di avvio nell'account.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplates",
    "Action": "ec2:DescribeLaunchTemplates",
    "Effect": "Allow",
    "Resource": "*"
}
```

ec2: DescribeLaunchTemplateVersions

I responsabili che visualizzano i modelli di avvio dovrebbero inoltre disporre dell'autorizzazione `ec2:DescribeLaunchTemplateVersions` per recuperare l'intero set di attributi che compongono i modelli di avvio.

Per elencare le versioni del modello di avvio nell'account, il principale deve disporre dell'autorizzazione `ec2:DescribeLaunchTemplateVersions` in una policy IAM. Dato che le operazioni `Describe` non supportano le autorizzazioni a livello di risorsa, devono essere specificate senza condizioni e il valore dell'elemento risorsa nella policy deve essere `"*"`.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per elencare tutte le versioni del modello di avvio nell'account.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
    "Effect": "Allow",
    "Action": "ec2:DescribeLaunchTemplateVersions",
    "Resource": "*"
}
```

ec2: DeleteLaunchTemplate

> **Important**
>
> È necessario prestare attenzione quando si concedono ai principali le autorizzazioni per eliminare una risorsa. L'eliminazione di un modello di avvio potrebbe causare un errore in una AWS risorsa che si basa sul modello di avvio.

Per eliminare un modello di avvio, il principale deve disporre dell'autorizzazione `ec2:DeleteLaunchTemplate` in una policy IAM. Quando possibile, si consiglia di utilizzare le chiavi di condizione basate su tag per limitare le autorizzazioni.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per eliminare modelli di avvio solo se il modello utilizza il tag specificato (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplates",
    "Action": "ec2:DeleteLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

In alternativa, è possibile utilizzare gli ARN per identificare il modello di avvio a cui si applica la policy IAM.

Un modello di avvio ha il seguente ARN.

```
"Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d310e"
```

È possibile specificare più ARN del modello di avvio fornendo un elenco oppure un valore `Resource` di `"*"` senza l'elemento `Condition` per consentire al principale di eliminare qualsiasi modello di avvio nell'account.

Controllo delle autorizzazioni di controllo delle versioni

Agli amministratori attendibili, è possibile concedere l'accesso per la creazione e l'eliminazione delle versioni di un modello di avvio e per modificare la versione predefinita di un modello di avvio utilizzando policy IAM simili agli esempi seguenti.

Important

Fai attenzione quando concedi ai responsabili il permesso di creare versioni dei modelli di lancio o modificare i modelli di lancio.

- Quando crei una versione del modello di lancio, influisci su tutte AWS le risorse che consentono ad Amazon EC2 di avviare istanze per tuo conto con la versione. `Latest`
- Quando modifichi un modello di lancio, puoi cambiare la versione `Default` e quindi influire su tutte AWS le risorse che consentono ad Amazon EC2 di avviare istanze per tuo conto con questa versione modificata.

Inoltre, devi essere cauto nel modo in cui gestisci AWS le risorse che interagiscono con la versione del modello `Latest` o la `Default` lanciano, come EC2 Fleet e Spot Fleet. Quando viene utilizzata una versione diversa del modello di avvio per `Latest` o `Default`, Amazon EC2 non ricontrolla le autorizzazioni per le operazioni da completare quando si avviano nuove istanze per soddisfare la capacità prevista del parco istanze, poiché non avviene alcuna interazione fra l'utente e la risorsa AWS . Concedendo a un utente l'autorizzazione a richiamare le API `CreateLaunchTemplateVersion` e `ModifyLaunchTemplate`, all'utente viene effettivamente concessa anche l'autorizzazione `iam:PassRole` se indirizza il parco istanze a una versione diversa del modello di avvio che contiene un profilo dell'istanza (un container per un ruolo IAM). Significa che un utente può potenzialmente aggiornare un modello di avvio per passare un ruolo IAM a un'istanza anche se non dispone dell'autorizzazione `iam:PassRole`. È possibile gestire questo rischio prestando attenzione quando si concedono le autorizzazioni a chi può creare e gestire le versioni dei modelli di avvio.

ec2: CreateLaunchTemplateVersion

Per creare una nuova versione di un modello di avvio, il principale deve disporre dell'autorizzazione `ec2:CreateLaunchTemplateVersion` per il modello di avvio in una policy IAM.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per creare versioni dei modelli di avvio solo se la versione utilizza il tag specificato (*environment*=*production*). In alternativa, è possibile specificare uno o più ARN del modello di avvio oppure un valore `Resource` di `"*"` senza l'elemento `Condition` per consentire al principale di creare versioni di qualsiasi modello di avvio nell'account.

```
{
    "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
    "Action": "ec2:CreateLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2: DeleteLaunchTemplateVersion

> **Important**
>
> Come sempre, è necessario prestare attenzione quando si concedono le autorizzazioni per eliminare una risorsa. L'eliminazione di una versione del modello di avvio potrebbe causare un errore in una AWS risorsa che si basa sulla versione del modello di avvio.

Per eliminare una versione di un modello di avvio, il principale deve disporre dell'autorizzazione `ec2:DeleteLaunchTemplateVersion` per il modello di avvio in una policy IAM.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per eliminare versioni dei modelli di avvio solo se la versione utilizza il tag specificato (*environment*=*production*). In alternativa, è possibile specificare uno o più ARN del modello di avvio oppure un valore `Resource` di `"*"` senza l'elemento `Condition` per consentire al principale di eliminare versioni di qualsiasi modello di avvio nell'account.

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
    "Action": "ec2:DeleteLaunchTemplateVersion",
    "Effect": "Allow",
```

```
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2: ModifyLaunchTemplate

Per modificare la versione `Default` associata a un modello di avvio, il principale deve disporre dell'autorizzazione `ec2:ModifyLaunchTemplate` per il modello di avvio in una policy IAM.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per modificare i modelli di avvio solo se il modello di avvio utilizza il tag specificato (*`environment`*=*`production`*). In alternativa, è possibile specificare uno o più ARN del modello di avvio oppure un valore `Resource` di `"*"` senza l'elemento `Condition` per consentire al principale di modificare qualsiasi modello di avvio nell'account.

```
{
    "Sid": "IAMPolicyForModifyingLaunchTemplates",
    "Action": "ec2:ModifyLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

Controllo dell'accesso ai tag sui modelli di avvio

È possibile utilizzare le chiavi di condizione per limitare le autorizzazioni di applicazione di tag quando la risorsa è un modello di avvio. Ad esempio, la seguente policy IAM consente di rimuovere solo il tag con la chiave *`temporary`* dai modelli di avvio nell'account e nella regione specificati.

```
{
    "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
    "Action": "ec2:DeleteTags",
    "Effect": "Allow",
```

```
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["temporary"]
        }
    }
}
```

Per ulteriori informazioni sulle chiavi di condizione utilizzabili per controllare le chiavi e i valori dei tag che possono essere applicati alle risorse Amazon EC2, consulta la pagina Controllo dell'accesso a tag specifici.

Utilizzo dei modelli di avvio per controllare l'avvio delle istanze

È possibile specificare che gli utenti possono avviare istanze soltanto utilizzando un modello di avvio specifico. Puoi anche controllare chi può creare, modificare, descrivere ed eliminare i modelli di avvio e le versioni del modello di avvio.

Utilizzo dei modelli di avvio per controllare i parametri di avvio

Un modello di avvio può contenere tutti o alcuni dei parametri per avviare un'istanza. Quando avvii un'istanza utilizzando un modello di avvio, puoi sostituire i parametri specificati nel modello di avvio. Oppure puoi specificare parametri aggiuntivi che non si trovano nel modello di avvio.

> **Note**
>
> Non è possibile rimuovere i parametri del modello di avvio durante l'avvio (ad esempio, non è possibile specificare un valore nullo per il parametro). Per rimuovere un parametro, crea una nuova versione del modello di avvio senza il parametro e utilizza tale versione per avviare l'istanza.

Per avviare le istanze, gli utenti devono disporre delle autorizzazioni per utilizzare l'operazione `ec2:RunInstances`. Gli utenti devono anche disporre delle autorizzazioni per creare o utilizzare le risorse create o associate all'istanza. Puoi utilizzare le autorizzazioni a livello di risorsa per l'operazione `ec2:RunInstances` per controllare i parametri di avvio che gli utenti possono specificare. In alternativa, puoi concedere agli utenti le autorizzazioni per avviare un'istanza utilizzando un modello di avvio. Ciò consente di gestire i parametri di lancio in un modello di avvio anziché in una policy IAM e utilizzare un modello di avvio come veicolo di autorizzazione per l'avvio delle istanze. Ad esempio, è possibile specificare che gli utenti possono solo avviare istanze

utilizzando un solo modello di avvio specifico. È anche possibile controllare i parametri di lancio che gli utenti possono sovrascrivere nel modello di avvio. Per esempi di policy, consulta Modelli di lancio.

Controllo dell'utilizzo dei modelli di avvio

Per impostazione predefinita, gli utenti non dispongono delle autorizzazioni per lavorare con i modelli di lancio. Puoi creare una policy dell'utente che concede agli utenti le autorizzazioni per creare, modificare, descrivere ed eliminare i modelli di avvio e le versioni del modello di avvio. È anche possibile applicare le autorizzazioni a livello di risorsa ad alcune operazioni del modello di avvio per controllare la capacità di un utente di utilizzare risorse specifiche per tali azioni. Per ulteriori informazioni, consulta le seguenti policy di esempio: Esempio: utilizzo dei modelli di avvio.

Fai attenzione quando concedi agli utenti le autorizzazioni per utilizzare le operazioni `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. Non è possibile utilizzare le autorizzazioni a livello di risorse per controllare le risorse che gli utenti possono specificare nel modello di avvio. Per limitare le risorse utilizzate per avviare un'istanza, assicurarsi di concedere le autorizzazioni per creare modelli di avvio e le versioni del modello di avvio solo agli amministratori appropriati.

Importanti problemi di sicurezza quando si utilizzano modelli di avvio con parchi istanze EC2 o serie di istanze spot

Per utilizzare i modelli di avvio, devi concedere agli utenti le autorizzazioni per creare, modificare, descrivere ed eliminare tali modelli e le relative versioni. Puoi controllare chi può creare modelli di avvio e versioni del modello di avvio controllando l'accesso alle operazioni `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. Puoi anche controllare chi può modificare i modelli di avvio controllando l'accesso all'operazione `ec2:ModifyLaunchTemplate`.

> **Important**
>
> Se un parco istanze EC2 o una serie di istanze spot è configurata per utilizzare la versione più recente o predefinita del modello di avvio, il parco istanze non sa se la versione Più recente o Predefinita viene successivamente modificata per puntare a una versione del modello di avvio diversa. Quando viene utilizzata una versione diversa del modello di avvio per Più recente o Predefinita, Amazon EC2 non ricontrolla le autorizzazioni per le operazioni da completare quando si avviano nuove istanze per soddisfare la capacità prevista del parco istanze. Questa è una considerazione importante quando si concedono le autorizzazioni a chi può creare e gestire le versioni dei modelli di avvio, in particolare

l'operazione `ec2:ModifyLaunchTemplate` che consente a un utente di modificare la versione predefinita del modello di avvio.

Concedendo a un utente l'autorizzazione a utilizzare le operazioni EC2 per le API dei modelli di avvio, all'utente viene effettivamente concessa anche l'autorizzazione `iam:PassRole` se crea o aggiorna un parco istanze EC2 o una serie di istanze spot in modo che punti a una versione diversa del modello di avvio che contiene un profilo dell'istanza (un container per un ruolo IAM). Significa che un utente può potenzialmente aggiornare un modello di avvio per passare un ruolo IAM a un'istanza anche se non dispone dell'autorizzazione `iam:PassRole`. Per ulteriori informazioni e per una policy IAM di esempio, consulta la sezione Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per ulteriori informazioni, consulta Controllo dell'utilizzo dei modelli di avvio e Esempio: utilizzo dei modelli di avvio.

Creazione di un modello di avvio

Crea un modello di lancio utilizzando i parametri che definisci oppure utilizza un modello di lancio esistente o un'istanza come base per un nuovo modello di lancio.

Attività

- Crea un modello di lancio dai parametri
- Creazione di un modello di avvio da un modello di avvio esistente
- Creazione di un modello di avvio da un'istanza
- Usare un parametro Systems Manager invece di un'ID AMI

Crea un modello di lancio dai parametri

Per creare un modello di avvio, è necessario specificare il nome del modello di avvio e almeno un parametro di configurazione dell'istanza.

Indicazioni della console

Per creare un modello di avvio utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Modelli di avvio quindi Crea modello di avvio.

3. I parametri del modello di lancio sono raggruppati. Per informazioni dettagliate su ciascun gruppo, consulta le sezioni seguenti.
4. Utilizza il pannello Riepilogo per rivedere la configurazione del modello di lancio. È possibile accedere a qualsiasi sezione selezionando il relativo collegamento e quindi apportare le modifiche necessarie.
5. Quando è tutto pronto per creare il modello di avvio, scegliere Create launch template (Crea modello di avvio).

Nome, descrizione e tag del modello di avvio

1. In nome modello di avvio, inserire un nome descrittivo per il modello di avvio.
2. In Template version description (Descrizione versione modello), fornire una breve descrizione della versione del modello di avvio.
3. Per applicare un tag al modello di avvio al momento della creazione, espandi Template tags (Tag del modello) e scegli Add tag (Aggiungi tag), quindi inserisci una coppia chiave e valore di tag. Scegliere Add tag (Aggiungi tag) per ogni tag aggiuntivo.

> **Note**
>
> Per applicare un tag alle risorse create all'avvio di un'istanza, è necessario specificare i tag in Resource tags (Tag delle risorse). Per ulteriori informazioni, consulta Tag delle risorse.

Immagini di applicazioni e sistema operativo (Amazon Machine Image)

Un'Amazon Machine Image (AMI) contiene tutte le informazioni necessarie per creare un'istanza. Ad esempio, un'AMI potrebbe contenere il software necessario per fungere da server Web, come Linux, Apache e il tuo sito Web.

È possibile trovare un'AMI adatta come descritto di seguito: Con ogni opzione per trovare un'AMI, è possibile scegliere Cancel (Annulla) (in alto a destra) per tornare al modello di avvio senza scegliere un'AMI.

Barra di ricerca

Per ricercare tra tutte le AMI disponibili, inserisci una parola chiave nella barra di ricerca AMI e premi Invio. Scegliere Select (Seleziona) per selezionare l'AMI.

Recents (Recenti

Le AMI usate di recente.

Scegliere Recently launched (Avviati di recente) o Currently in use (Correntemente in uso) e poi, da Amazon Machine Image (AMI), selezionare un'AMI.

My AMIs (Le mie AMI)

AMI private di proprietà o AMI private condivise da altri utenti.

Scegliere Owned by me (Di mia proprietà) o Shared with me (Condiviso con me) e poi, da Amazon Machine Image (AMI), selezionare un'AMI.

Quick Start

Le AMI sono raggruppate per sistema operativo (SO) in modo che possano essere utilizzate rapidamente.

Per prima cosa selezionare il sistema operativo di cui si ha bisogno e quindi da Amazon Machine Image (AMI), selezionare un'AMI. Per selezionare un'AMI idonea al piano gratuito, assicurarsi che l'AMI sia contrassegnata come Free tier eligible (Idonea al piano gratuito).

Ricerca di altre AMI

Scegliere Browse more AMIs (Sfoglia altre AMI) per sfogliare il catalogo completo di AMI.

- Per ricercare tra tutte le AMI disponibili, inserisci una parola chiave nella barra di ricerca e premi Invio.
- Per trovare un'AMI utilizzando un parametro di Systems Manager, seleziona il pulsante freccia a destra della barra di ricerca, quindi seleziona Search by Systems Manager parameter (Cerca per parametro Systems Manager). Per ulteriori informazioni, consulta Trova un'AMI utilizzando un parametro Systems Manager.
- Per specificare un parametro Systems Manager che si risolverà in un'AMI nel momento in cui un'istanza viene avviata dal modello di avvio, seleziona il pulsante freccia a destra della barra di ricerca, quindi seleziona Specifica valore personalizzato/parametro Systems Manager. Per ulteriori informazioni, consulta Usare un parametro Systems Manager invece di un'ID AMI.
- Per cercare per categoria, scegliere Quickstart AMIs (Avvio rapido delle AMI), My AMIs (Le mie AMI), Marketplace AWS AMI (AMI MKT), oppure Community AMIs (AMI della community).

  Marketplace AWS È un negozio online in cui è possibile acquistare software che funziona su AWS, comprese le AMI. Per ulteriori informazioni sull'avvio di un'istanza da Marketplace AWS, consulta. Avvia un' Marketplace AWS istanza Nelle AMI della community, puoi trovare le AMI

che i membri AWS della comunità hanno reso disponibili per l'uso da parte di altri. Le AMI di Amazon o di un partner verificato sono contrassegnate con la dicitura Verified provider (fornitore verificato).

- Per filtrare l'elenco delle AMI, selezionare una o più caselle di controllo sotto Refine results (Definisci i risultati) a sinistra dello schermo. Le opzioni di filtro sono diverse a seconda della categoria di ricerca selezionata.
- Controllare le voci per ciascuna AMI nell'elenco Root device type (Tipo dispositivo root). Individuare le AMI del tipo desiderato: ebs (supportate da Amazon EBS) o instance-store (supportate dall'archivio istanza). Per ulteriori informazioni, consulta Archiviazione del dispositivo root.
- Controllare le voci per ciascuna AMI nell'elenco Virtualization type (Tipo di virtualizzazione). Nota quali AMI sono del tipo di cui hai bisogno: hvm o paravirtuale. Ad esempio, alcuni tipi di istanza richiedono HVM. Per ulteriori informazioni, consulta Tipi di virtualizzazione dell'AMI.
- Controllare la modalità di avvio elencata per ogni AMI. Individuare quali AMI utilizzano la modalità di avvio necessaria: legacy-bios, uefi o uefi-preferred. Per ulteriori informazioni, consulta Modalità di avvio di Amazon EC2.
- Scegliere un'AMI conforme alle specifiche esigenze, quindi scegliere Select (Seleziona).

Tipo di istanza

Il tipo di istanza definisce la configurazione hardware e le dimensioni dell'istanza. I tipi di istanza più grandi dispongono di una maggiore quantità di CPU e memoria. Per ulteriori informazioni, consulta i tipi di istanze Amazon EC2.

Per Instance type (Tipo di istanza), puoi selezionare un tipo di istanza oppure specificare gli attributi di istanza e consentire ad Amazon EC2 di identificare i tipi di istanza con questi attributi.

> **Note**
>
> La specifica degli attributi di istanza è supportata solo quando si utilizzano i gruppi Auto Scaling, il parco istanze EC2 e la serie di istanze spot per l'avvio delle istanze. Per ulteriori informazioni, consultare Creazione di un gruppo Auto Scaling utilizzando la selezione del tipo di istanza basata su attributi, Selezione del tipo di istanza basata su attributi per il parco istanze EC2 e Selezione del tipo di istanza basata su attributi per serie di istanze spot.
> Se prevedi di utilizzare il modello di lancio nella procedura guidata di avvio dell'istanza o con l'RunInstancesAPI, devi selezionare un tipo di istanza.

- Instance type (Tipo di istanza): assicurarsi che il tipo di istanza sia compatibile con l'AMI specificata. Per ulteriori informazioni, consulta Tipi di istanza Amazon EC2.
- Confronto dei tipi di istanza: È possibile confrontare diversi tipi di istanza con i seguenti attributi: numero di vCPUs, architettura, quantità di memoria (GiB), quantità di archiviazione (GB), tipo di archiviazione e prestazioni di rete.
- Fatti consigliare: puoi ottenere indicazioni e suggerimenti per i tipi di istanza dal selettore dei tipi di istanza EC2 di Amazon Q. Per ulteriori informazioni, consulta Ottenimento delle raccomandazioni per i tipi di istanza per un nuovo carico di lavoro.
- Advanced (Avanzato): per specificare gli attributi di istanza e consentire ad Amazon EC2 di identificare i tipi di istanza con tali attributi, scegliere Advanced (Avanzato) e quindi Specify instance type attributes (Specifica attributi del tipo di istanza).
  - Number of vCPUs (Numero di vCPU): inserire il numero minimo e massimo di vCPU per i requisiti di calcolo. Per indicare nessun limite, inserire un valore minimo **0** e lasciare vuoto il campo del valore massimo.
  - Amount of memory (MiB) (Quantità di memoria [MiB]): inserire la quantità minima e massima di memoria, in MiB, per i propri requisiti di calcolo. Per indicare nessun limite, inserire un valore minimo **0** e lasciare vuoto il campo del valore massimo.
  - Espandere Optional instance type attributes (Attributi facoltativi del tipo di istanza) e scegliere Add attribute (Aggiungi attributo) per esprimere i requisiti di calcolo in modo più dettagliato. Per informazioni su ciascun attributo, consulta InstanceRequirementsRequestil riferimento alle API di Amazon EC2.
  - Resulting instance types (Tipi di istanza risultanti): è possibile visualizzare in anteprima i tipi di istanza che corrispondono agli attributi specificati. Per escludere i tipi di istanza, scegliere Add attribute (Aggiungi attributo), quindi dall'elenco Attribute (Attributo), scegliere Excluded instance types (Tipi di istanza escluse). Dall'elenco Attribute value (Valore attributo), selezionare i tipi di istanza da escludere.

Coppia di chiavi (login)

La coppia di chiavi per l'istanza.

In Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente oppure scegliere Create new key pair (Crea nuova coppia di chiavi) per creane una nuova. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.

Impostazioni di rete

Configurare le impostazioni di rete, se necessario.

- Sottorete: è possibile avviare un'istanza in una sottorete associata a una zona di disponibilità, una Local Zone, una zona Wavelength o un Outpost.

  Per avviare l'istanza in una zona di disponibilità, selezionare la sottorete in cui avviare l'istanza. Per creare una nuova sottorete, scegliere Create new subnet (Crea nuova sottorete) per passare alla console Amazon VPC. Al termine, tornare alla procedura guidata e scegliere Refresh (Aggiorna) per caricare la sottorete nell'elenco.

  Per avviare l'istanza in una Local Zone, selezionare una sottorete creata nella Local Zone.

  Per avviare un'istanza in un Outpost, selezionare una sottorete in un VPC associato a un Outpost.
- Firewall (security groups) (Firewall [gruppi di sicurezza]): utilizzare uno o più gruppi di sicurezza per definire le regole del firewall per l'istanza. Tali regole specificano quale traffico di rete in entrata deve viene distribuito sulla tua istanza. Tutto il traffico rimanente verrà ignorato. Per ulteriori informazioni sui gruppi di sicurezza, consulta Gruppi di sicurezza Amazon EC2 per le tue istanze EC2.

  Se si aggiunge un'interfaccia di rete, si dovrà specificare lo stesso gruppo di sicurezza al suo interno.

  Selezionare o creare un gruppo di sicurezza nel seguente modo:

  - Per selezionare un gruppo di sicurezza esistente, scegliere Select an existing security group (Seleziona un gruppo di sicurezza esistente), quindi selezionare il gruppo di sicurezza da Common security groups (Gruppi di sicurezza comuni).
  - Per creare un nuovo gruppo di sicurezza, scegliere Create security group (Crea gruppo di sicurezza).

    È possibile aggiungere regole in base alle tue esigenze. Ad esempio, se l'istanza sarà un server Web, aprire le porte 80 (HTTP) e 443 (HTTPS) per consentire il traffico Internet.

    Per aggiungere una regola, scegliere Add security group rule (Aggiungi regola del gruppo di sicurezza). Per Type (Tipo), selezionare il tipo di traffico di rete. Il campo Protocol (Protocollo) viene automaticamente compilato con il protocollo da aprire al traffico di rete. Per Source type (Tipo di origine) scegliere il tipo di origine. Scegliere My IP (Il mio IP) per consentire al modello di avvio di aggiungere l'indirizzo IP pubblico del computer in uso. Tuttavia, in caso di connessione

tramite un ISP o con la protezione di un firewall senza un indirizzo IP statico, è necessario individuare l'intervallo degli indirizzi IP utilizzati dai computer client.

> **Warning**
>
> Le regole che abilitano tutti gli indirizzi IP (`0.0.0.0/0`) per accedere all'istanza tramite SSH o RDP sono accettabili se si avvia brevemente un'istanza di test e la si interrompe o termina presto, ma non sono sicure negli ambienti di produzione. Dovrai autorizzare solo un determinato indirizzo IP o un intervallo di indirizzi per accedere a un'istanza.

- Configurazione di rete avanzata

  Interfaccia di rete

  - Device index (Indice dispositivo): il numero del dispositivo per l'interfaccia di rete, ad esempio `eth0` per l'interfaccia di rete primaria. Se lasci vuoto il campo, AWS crea l'interfaccia di rete primaria.
  - Network interface (Interfaccia di rete): selezionare New interface (Nuova interfaccia) per consentire ad Amazon EC2 di creare una nuova interfaccia oppure selezionare un'interfaccia di rete esistente disponibile.
  - Description (Descrizione): (facoltativo) una descrizione per la nuova interfaccia di rete.
  - Subnet (Sottorete): la sottorete nella quale creare la nuova interfaccia di rete. Per l'interfaccia di rete primaria (`eth0`), questa è la sottorete nella quale viene avviata l'istanza. Se si è inserita un'interfaccia di rete esistente per `eth0`, l'istanza viene avviata nella sottorete nella quale si trova l'interfaccia di rete.
  - Gruppi di sicurezza: uno o più gruppi di sicurezza nel VPC a cui associare l'interfaccia di rete.
  - Auto-assign public IP (Assegna IP pubblico automaticamente): specificare se l'istanza riceve un indirizzo IPv4 pubblico. Per impostazione di default, le istanze in una sottorete di default ricevono un indirizzo IPv4 pubblico, al contrario delle istanze in una sottorete non di default. Selezionare Enable (Abilita) o Disable (Disabilita) per sostituire l'impostazione di default della sottorete. Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici.
  - Primary IP (IP primario): un indirizzo IPv4 privato dall'intervallo della sottorete. Lasciare vuoto il campo per consentire ad Amazon EC2 di scegliere un indirizzo IPv4 privato per tuo conto.
  - IP secondario: uno o più indirizzi IPv4 privati aggiuntivi dall'intervallo della sottorete. Scegliere Manually assign (Assegnazione manuale) e inserire un indirizzo IP. Scegliere Add IP (Aggiungi IP) per aggiungere un altro indirizzo IP. In alternativa, scegliere Automatically assign (Assegna

automaticamente) per consentire ad Amazon EC2 di sceglierne uno per te, quindi inserire un valore per indicare il numero di indirizzi IP da aggiungere.

- (Solo IPv6) IPv6 IPs (IP IPv6): un indirizzo IPv6 dall'intervallo della sottorete. Scegliere Manually assign (Assegnazione manuale) e inserire un indirizzo IP. Scegliere Add IP (Aggiungi IP) per aggiungere un altro indirizzo IP. In alternativa, scegliere Automatically assign (Assegna automaticamente) per consentire ad Amazon EC2 di sceglierne uno per te, quindi inserire un valore per indicare il numero di indirizzi IP da aggiungere.
- Prefissi IPv4: i prefissi IPv4 per l'interfaccia di rete.
- Prefissi IPv6: i prefissi IPv6 per l'interfaccia di rete.
- (Facoltativo) Assegna IP IPv6 primario: se stai lanciando un'istanza in una sottorete dual-stack o solo IPv6, disponi dell'opzione Assegna IP IPv6 primario. L'assegnazione di un indirizzo IPv6 primario consente di evitare l'interruzione del traffico verso istanze o ENI. Scegli Abilita se questa istanza si basa sul fatto che il suo indirizzo IPv6 non cambia. All'avvio dell'istanza, AWS assegnerà automaticamente un indirizzo IPv6 associato all'ENI collegato all'istanza come indirizzo IPv6 principale. Dopo aver abilitato un indirizzo GUA IPv6 come IPv6 primario, non è possibile disattivarlo. Quando si abilita un indirizzo GUA IPv6 come IPv6 primario, la prima GUA IPv6 verrà impostata come indirizzo IPv6 primario fino alla chiusura dell'istanza o alla disconnessione dell'interfaccia di rete. Se disponi di più indirizzi IPv6 associati a un ENI collegato all'istanza e abiliti un indirizzo IPv6 primario, il primo indirizzo GUA IPv6 associato all'ENI diventa l'indirizzo IPv6 primario.
- Delete on termination (Elimina al termine): se eliminare l'interfaccia di rete quando l'istanza viene eliminata.
- Elastic Fabric Adapter (EFA): indica se l'interfaccia di rete è di tipo Elastic Fabric Adapter (EFA). Per ulteriori informazioni, consulta the section called “Elastic Fabric Adapter”.
- Indice della scheda di rete: l'indice della scheda di rete. L'interfaccia di rete primaria deve essere assegnata all'indice della scheda di rete 0. Alcuni tipi di istanza supportano più schede di rete.
- ENA Express: ENA Express è alimentato dalla tecnologia AWS Scalable Reliable Datagram (SRD). La tecnologia SRD utilizza un meccanismo di distribuzione dei pacchetti ("packet spraying") per distribuire il carico ed evitare la congestione della rete. L'abilitazione di ENA Express consente alle istanze supportate di comunicare utilizzando SRD in aggiunta al normale traffico TCP, quando possibile. Il modello di avvio non include la configurazione ENA Express per l'istanza, a meno che non si selezioni Abilita o Disabilita dall'elenco.
- UDP ENA Express: se hai abilitato ENA Express, puoi facoltativamente utilizzarlo per il traffico UDP. Il modello di avvio non include la configurazione ENA Express per l'istanza, a meno che non si selezioni Abilita o Disabilita.

Per aggiungere altre interfacce di rete, selezionare Add network interface (Aggiungi interfaccia di rete). Il numero di interfacce di rete che puoi aggiungere dipende dal numero supportato dal tipo di istanza selezionato. Le interfacce di rete aggiuntive possono risiedere in una sottorete diversa dello stesso VPC o in una sottorete di un VPC diverso di vostra proprietà (purché la sottorete si trovi nella stessa zona di disponibilità dell'istanza). Se selezioni una sottorete in un altro VPC, l'etichetta Multi-VPC viene visualizzata accanto all'interfaccia di rete che hai aggiunto. Ciò consente di creare istanze multi-homed su VPC con configurazioni di rete e sicurezza differenti. Tieni presente che se colleghi un ENI aggiuntivo da un altro VPC, devi scegliere un gruppo di sicurezza per l'ENI da quel VPC.

Per ulteriori informazioni, consulta Interfacce di rete elastiche. Se si specifica più di un'interfaccia di rete, l'istanza non può ricevere un indirizzo IPv4 pubblico. Inoltre, se si specifica un'interfaccia di rete esistente per eth0, non è possibile sostituire l'impostazione dell'indirizzo IPv4 pubblico della sottorete utilizzando Auto-assign Public IP (Assegna automaticamente IP pubblico). Per ulteriori informazioni, consulta Assegnare un indirizzo IPv4 pubblico durante l'avvio dell'istanza.

Per configurare l'archiviazione

Se si specifica un'AMI per il modello di avvio, l'AMI include uno o più volumi di archiviazione, compreso il volume root (Volume 1 [AMI Root]). È possibile specificare altri volumi da collegare all'istanza.

È possibile utilizzare la vista Semplice o Avanzato. Con la vista Semplice, si specifica la dimensione e il tipo di volume. Per specificare tutti i parametri del volume, scegli la vista Advanced (Avanzata) (nella parte superiore destra della scheda).

Per aggiungere un nuovo volume, scegli Add new volume (Aggiungi nuovo volume).

Con la vista Avanzato, è possibile configurare ciascun volume come segue:

- Storage Type (Tipo di archiviazione): il tipo di volume (EBS o temporaneo) da associare all'istanza. Il tipo di volume dell'archivio istanza (temporaneo) è disponibile solo se si seleziona un tipo di istanza che lo supporta. Per ulteriori informazioni, consulta i volumi Instance store Amazon EC2 e Amazon EBS.
- Dispositivo: seleziona dall'elenco di nomi dei dispositivi disponibili per il volume.
- Snapshot: selezionare lo snapshot da cui creare il volume. È inoltre possibile cercare snapshot pubblici e condivisi disponibili digitando il testo nel campo Snapshot.

- Dimensioni: per i volumi EBS, è possibile specificare una dimensione di archiviazione. Se è stata selezionata un'AMI e l'istanza è idonea per il piano gratuito, per rientrare nel piano gratuito è necessario mantenersi al di sotto dei 30 GiB di archiviazione totale.
- Volume Type (Tipo di volume): per i volumi EBS, selezionare un tipo di volume. Per ulteriori informazioni, consulta i tipi di volume di Amazon EBS nella Amazon EBS User Guide.
- IOPS: se è stato selezionato il tipo di volume SSD con capacità di IOPS allocata (`io1` e `io2`) o SSD per uso generale (`gp3`), è possibile inserire il numero di operazioni I/O per secondo (IOPS) che il volume può supportare. Ciò è necessario per i volumi io1, io2 e gp3. Non è supportato per gp2, st1, sc1 o volumi standard. Se si omette questo parametro per il modello di avvio, è necessario specificare un valore quando si avvia un'istanza dal modello di avvio.
- Delete on termination (Elimina alla terminazione): per i volumi Amazon EBS, scegliere Yes (Sì) per eliminare il volume quando l'istanza viene terminata oppure No per conservare il volume. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.
- Encrypted (Crittografato): se il tipo di istanza supporta la crittografia EBS, scegliere Yes (Sì) per abilitare la crittografia per il volume. Se hai abilitato la crittografia per impostazione predefinita in questa regione allora la crittografia è abilitata. Per ulteriori informazioni, consulta Amazon EBS encryption nella Amazon EBS User Guide.
- KMS key (Chiave KMS): se si è selezionato Yes (Sì) per Encrypted (Crittografato), allora è necessario selezionare una chiave gestita dal cliente da utilizzare per crittografare il volume. Se hai abilitato la crittografia per impostazione predefinita in questa Regione, viene selezionata automaticamente la chiave gestita dal cliente predefinita. È possibile selezionare una chiave diversa o specificare l'ARN di qualsiasi chiave gestita dal cliente creata.

Tag delle risorse

Per applicare un tag alle risorse create all'avvio di un'istanza, in Resource tags (Tag delle risorse) scegli Add tag (Aggiungi tag), quindi inserisci una coppia chiave e valore di tag. Per Resource types (Tipi di risorsa), specifica le risorse alle quali applicare un tag al momento della creazione. È possibile specificare lo stesso tag per tutte le risorse o specificare tag diversi per risorse diverse. Scegliere Add tag (Aggiungi tag) per ogni tag aggiuntivo.

È possibile specificare i tag per le seguenti risorse che vengono create quando si utilizza un modello di avvio:

- Istanze
- Volumi

- Richieste di istanza spot
- Interfacce di rete

> **Note**
>
> Per applicare un tag al modello di avvio stesso, è necessario specificare i tag in Template tags (Tag del modello). Per ulteriori informazioni, consulta Nome, descrizione e tag del modello di avvio.

Dettagli avanzati

Per Advanced Details (Dettagli avanzati), espandi la sezione per visualizzare i campi e specifica eventuali parametri aggiuntivi per l'istanza.

- Opzione di acquisto: scegliere Request Spot Instances (Richiesta istanze spot) per richiedere le istanze spot al prezzo Spot, limitato al prezzo on demand, e scegliere Customize (Personalizza) per modificare le impostazioni dell'istanza spot di default. Puoi impostare il prezzo massimo (sconsigliato) e modificare il tipo di richiesta, la durata della richiesta e il comportamento di interruzione. Se non si richiede un'istanza spot, EC2 avvia un'istanza on demand per impostazione predefinita. Per ulteriori informazioni, consulta Spot Instances.
- IAM instance profile (Profilo dell'istanza IAM): un profilo dell'istanza AWS Identity and Access Management (IAM) da associare all'istanza. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.
- Hostname type (Tipo di nome host): selezionare se il nome host del sistema operativo guest dell'istanza deve includere il nome della risorsa o il nome IP. Per ulteriori informazioni, consulta Tipi di nomi host delle istanze Amazon EC2.
- Ripristino automatico dell'istanza: se abilitato, ripristina l'istanza se i controlli dello stato del sistema falliscono. Questa impostazione è abilitata per impostazione predefinita all'avvio per i tipi di istanze supportati. Per ulteriori informazioni, consulta Configura il ripristino automatico semplificato.

  DNS Hostname (Nome host DNS): determina se le query DNS al nome IP o al nome della risorsa (a seconda di cosa si seleziona in Hostname type (Tipo di nome host) risponderanno con l'indirizzo IPv4 (registro A), l'indirizzo IPv6 (registro AAAA) o entrambi. Per ulteriori informazioni, consulta Tipi di nomi host delle istanze Amazon EC2.

- Shutdown behavior (Comportamento di arresto): selezionare se l'istanza deve interrompersi o terminare all'arresto. Per ulteriori informazioni, consulta Modifica del comportamento di arresto avviato dall'istanza.
- Stop - Hibernate behavior (Comportamento di interruzione/ibernazione): per abilitare l'ibernazione, scegliere Enable (Abilita). Questo campo è solo valido per le istanze che soddisfano i requisiti di ibernazione. Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.
- Termination protection (Protezione da terminazione): per impedire la terminazione accidentale, scegliere Enable (Abilita). Per ulteriori informazioni, consulta Abilitare la protezione da cessazione.
- Protezione da arresto: per evitare l'arresto accidentale, scegli Enable (Abilita). Per ulteriori informazioni, consulta Abilitare la protezione da arresto.
- CloudWatch Monitoraggio dettagliato: scegli Abilita per abilitare il monitoraggio dettagliato dell'istanza tramite Amazon CloudWatch. Vengono applicati costi aggiuntivi. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.
- GPU elastica: Amazon Elastic Graphics ha raggiunto la fine del ciclo di vita l'8 gennaio 2024. Per carichi di lavoro che richiedono l'accelerazione grafica, ti consigliamo di utilizzare istanze Amazon EC2 G4ad, G4dn o G5.
- Elastic inference (Inferenza elastica): un acceleratore di inferenza elastica da collegare all'istanza della CPU EC2. Per ulteriori informazioni, consulta la sezione Lavorare con Amazon Elastic Inference nella Guida per gli sviluppatori di Amazon Elastic Inference.

  > **Note**
  >
  > A partire dal 15 aprile 2023, non AWS effettuerà l'onboarding di nuovi clienti in Amazon Elastic Inference (EI) e aiuterà i clienti attuali a migrare i propri carichi di lavoro verso opzioni che offrono prezzi e prestazioni migliori. Dopo il 15 aprile 2023, i nuovi clienti non saranno in grado di avviare istanze con acceleratori Amazon EI su Amazon, SageMaker Amazon ECS o Amazon EC2. Tuttavia, i clienti che hanno utilizzato Amazon EI almeno una volta negli ultimi 30 giorni sono considerati clienti attuali e potranno continuare a usufruire del servizio.

- Credit specification (Specifica credito): scegliere Unlimited (Illimitato) per consentire l'espansione delle applicazioni oltre la baseline per tutto il periodo necessario. Questo campo è valido solo per le istanze T. Potrebbero essere applicati costi aggiuntivi. Per ulteriori informazioni, consulta Istanze a prestazioni espandibili.
- Gruppo di collocamento: specifica un gruppo di collocamento in cui avviare l'istanza. È possibile selezionare un gruppo di collocamento esistente o crearne uno nuovo. Non tutti i tipi di istanza

possono essere avviati in un gruppo di collocamento. Per ulteriori informazioni, consultare Gruppi di collocamento.

- EBS-optimized instance (Istanza ottimizzata per EBS): selezionare Enable (Abilita) per fornire una capacità aggiuntiva dedicata per l'I/O di Amazon EBS. Non tutti i tipi di istanze supportano questa caratteristica. Vengono applicati costi aggiuntivi. Per ulteriori informazioni, consulta the section called “Ottimizzazione di Amazon EBS”.
- Capacity Reservation (Prenotazione di capacità): specificare se avviare l'istanza in una qualsiasi prenotazione della capacità aperta (Open), una prenotazione della capacità specificare (Target by ID) o in un gruppo di prenotazione della capacità (Target by group). Per specificare che non deve essere utilizzata una prenotazione della capacità, selezionare None (Nessuno). Per ulteriori informazioni, consulta Avvio di istanze in una Prenotazione di capacità esistente.
- Tenancy: seleziona se eseguire l'istanza su hardware condiviso (Shared [Condiviso]), isolato, hardware dedicato (Dedicated [Dedicato]) o su un Host dedicato (Dedicated host [Host dedicato]). Se decidi di avviare l'istanza su un Host dedicato, puoi specificare se avviare l'istanza in un gruppo di risorse host o usare uno specifico Host dedicato come target. Potrebbero essere applicati costi aggiuntivi. Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2 e Host dedicati di Amazon EC2.
- RAM disk ID (ID disco RAM) (valido solo per AMI paravirtuali [PV]): selezionare un disco RAM per l'istanza. Se è stato selezionato un kernel, potrebbe essere necessario selezionare un disco RAM specifico con i driver per supportarlo.
- Kernel ID [ID kernel] (valido solo per AMI paravirtuali (PV)): un kernel per l'istanza.
- Nitro Enclave: permette di creare ambienti di esecuzione isolati, denominati enclavi, da istanze Amazon EC2. Selezionare Enable (Abilita) per abilitare l'istanza per AWS Nitro Enclaves. Per ulteriori informazioni, consulta Che cos'è AWS Nitro Enclaves? nella Guida dell'utente di AWS Nitro Enclaves.
- Configurazioni licenza: è possibile avviare istanze con la configurazione di licenza specificata per tenere traccia dell'utilizzo della licenza. Per ulteriori informazioni, consulta Creazione di una configurazione di licenza nella Guida per l'utente di AWS License Manager.
- CPU options (Opzioni CPU): selezionare Specify CPU options (Specifica le opzioni CPU) per specificare un numero personalizzato di vCPU durante l'avvio. Imposta il numero di thread per core e di core CPU. Per ulteriori informazioni, consulta Ottimizzazione delle opzioni della CPU.
- Endpoint IPv6 per metadati: è possibile consentire all'istanza di utilizzare l'indirizzo IPv6 IMDS per recuperare i metadati dell'istanza. `[fd00:ec2::254]` Questa opzione è disponibile solo se si avviano istanze create sul sistema AWS Nitro in una sottorete supportata da IPv6 (dual stack o solo IPv6). Per ulteriori informazioni, consulta Recupero dei metadati dell'istanza.

- Metadati accessibili: puoi abilitare o disabilitare l'accesso a IMDS. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- Versione dei metadati: se abiliti l'accesso a IMDS, puoi scegliere di richiedere l'utilizzo di Servizio di metadati dell'istanza Versione 2 quando si richiedono i metadati dell'istanza. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- Limite di hop della risposta dei metadati: se abiliti l'accesso a IMDS, puoi impostare il numero consentito di hop di rete per il token dei metadati. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- Allow tags in metadata (Consenti tag nei metadati): se selezioni Enable (Abilita), l'istanza consentirà l'accesso a tutti i suoi tag dai metadati. Se non si include questa impostazione nel modello, l'accesso ai tag nei metadati dell'istanza non è permesso di default. Per ulteriori informazioni, consulta Per consentire l'accesso ai tag nei metadati delle istanze.
- User data (Dati utente): è possibile specificare i dati utente per configurare un'istanza durante l'avvio o per eseguire uno script di configurazione. Per ulteriori informazioni, consulta Esegui comandi sulla tua istanza Amazon EC2 al momento del lancio.

AWS CLI esempio

L'esempio seguente utilizza il create-launch-templatecomando per creare un modello di avvio con il nome e la configurazione dell'istanza specificati.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Di seguito è riportato un esempio JSON che specifica i dati del modello di avvio per la configurazione dell'istanza. Salvate il codice JSON in un file e includetelo nel `--launch-template-data` parametro come mostrato nel comando di esempio.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
```

```
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r4.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

Di seguito è riportato un output di esempio.

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

AWS Tools for Windows PowerShell esempio

L'esempio seguente utilizza il New-EC2LaunchTemplatecmdlet per creare un modello di avvio con il nome e la configurazione dell'istanza specificati.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
    ImageId = 'ami-8c1be5f6'
    InstanceType = 'r4.4xlarge'
    NetworkInterfaces = @(
        [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
            AssociatePublicIpAddress = $true
            DeviceIndex = 0
            Ipv6AddressCount = 1
            SubnetId = 'subnet-7b16de0c'
```

```
        }
    )
    TagSpecifications = @(
        [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
            ResourceType = 'instance'
            Tags = [Amazon.EC2.Model.Tag]@{
                Key = 'Name'
                Value = 'webserver'
            }
        }
    )
    CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
        CoreCount = 4
        ThreadsPerCore = 2
    }
}
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' -VersionDescription
 'WebVersion1' -LaunchTemplateData $launchTemplateData -TagSpecification
 $tagSpecificationData
```

Di seguito è riportato un output di esempio.

```
CreatedBy            : arn:aws:iam::123456789012:root
CreateTime           : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId     : lt-01238c059eEXAMPLE
LaunchTemplateName   : TemplateForWebServer
Tags                 : {purpose}
```

Creazione di un modello di avvio da un modello di avvio esistente

È possibile clonare un modello di avvio esistente e quindi modificare i parametri per crearne uno nuovo. Tuttavia, puoi farlo solo quando usi la console Amazon EC2; non AWS CLI supporta la clonazione di un modello.

Console

Creazione di un modello di avvio da un modello di avvio esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Modelli di avvio quindi Crea modello di avvio.
3. In nome modello di avvio, inserire un nome descrittivo per il modello di avvio.
4. In Template version description (Descrizione versione modello), fornire una breve descrizione della versione del modello di avvio.
5. Per applicare un tag al modello di avvio al momento della creazione, selezionare Template tags (Tag del modello), Add tag (Aggiungi tag), quindi inserire una chiave tag e una coppia valori.
6. Espandere Modello origine e per Nome modello di avvio scegliere un modello di avvio su cui basare il nuovo modello di avvio.
7. Per Source template version (Versione modello origine), scegli la versione del modello di avvio su cui basare il nuovo modello di avvio.
8. Regola i parametri di lancio come necessario e scegli Create launch template (Crea modello di avvio).

Creazione di un modello di avvio da un'istanza

Console

Creazione di un modello di avvio da un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza e scegliere Actions (Operazioni), Create template from instance (Crea modello dall'istanza).
4. Specificare un nome, una descrizione e i tag e modificare i parametri di lancio come necessario.

> **Note**
>
> Quando si crea un modello di avvio da un'istanza, gli ID dell'interfaccia di rete e gli indirizzi IP dell'istanza non sono inclusi nel modello.

5. Scegli Create launch template (Crea modello di avvio).

AWS CLI

Puoi utilizzare il AWS CLI per creare un modello di avvio da un'istanza esistente ottenendo prima i dati del modello di lancio da un'istanza e quindi creando un modello di avvio utilizzando i dati del modello di avvio.

Recupero dei dati del modello di avvio da un'istanza

- Utilizzate il get-launch-template-datacomando e specificate l'ID dell'istanza. È possibile utilizzare l'output come base per creare un nuovo modello di avvio o una nuova versione del modello di avvio. Per impostazione predefinita, l'output include un oggetto `LaunchTemplateData` di primo livello, che non può essere specificato nei dati del modello di avvio. Utilizzare l'opzione `--query` per escludere questo oggetto.

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData"
```

Di seguito è riportato un output di esempio.

```
    {
        "Monitoring": {},
        "ImageId": "ami-8c1be5f6",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/xvda",
                "Ebs": {
                    "DeleteOnTermination": true
                }
            }
        ],
        "EbsOptimized": false,
```

```
        "Placement": {
            "Tenancy": "default",
            "GroupName": "",
            "AvailabilityZone": "us-east-1a"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
            {
                "Description": "",
                "NetworkInterfaceId": "eni-35306abc",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
                        "PrivateIpAddress": "10.0.0.72"
                    }
                ],
                "SubnetId": "subnet-7b16de0c",
                "Groups": [
                    "sg-7c227019"
                ],
                "Ipv6Addresses": [
                    {
                        "Ipv6Address": "2001:db8:1234:1a00::123"
                    }
                ],
                "PrivateIpAddress": "10.0.0.72"
            }
        ]
    }
```

È possibile scrivere l'output direttamente su un file, ad esempio:

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

Creazione di un modello di avvio utilizzando i dati del modello di avvio

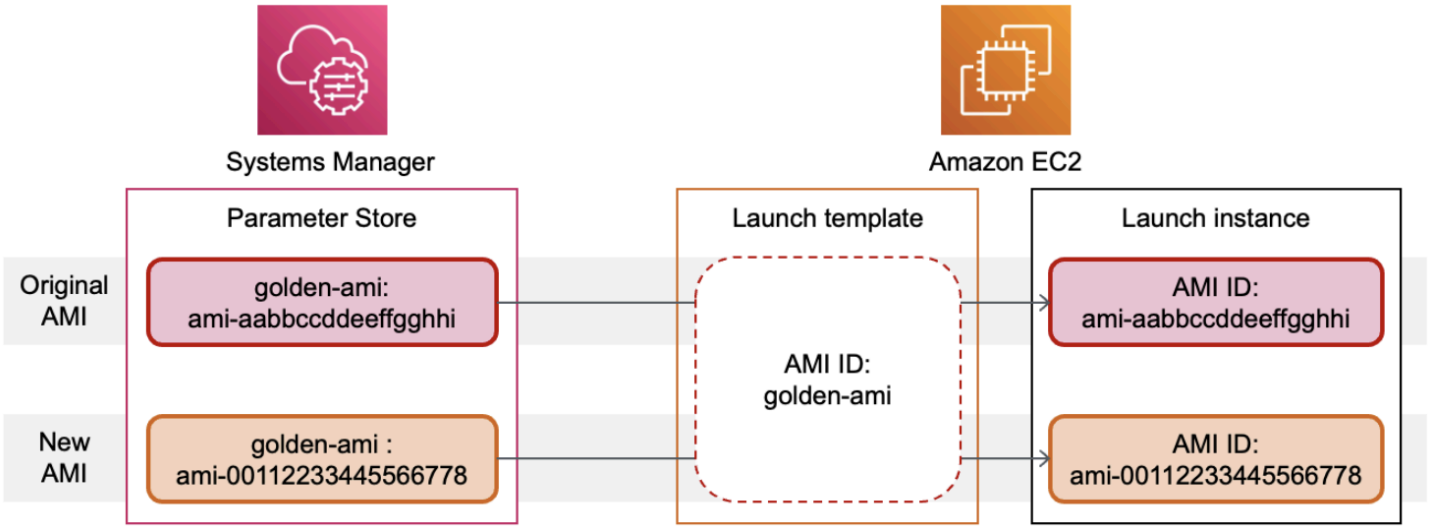
- Utilizzate il create-launch-templatecomando per creare un modello di avvio utilizzando l'output della procedura precedente. Per ulteriori informazioni sulla creazione di un modello di lancio utilizzando il AWS CLI, vedereCrea un modello di lancio dai parametri.

Usare un parametro Systems Manager invece di un'ID AMI

Anziché specificare un ID AMI nei modelli di avvio, puoi specificare un parametro AWS Systems Manager . Se l'ID AMI cambia, è possibile aggiornare l'ID AMI in un'unica posizione aggiornando il parametro Systems Manager nel Parameter Store di Systems Manager. I parametri possono anche essere condivisi con altri Account AWS. Puoi archiviare e gestire centralmente i parametri AMI in un account e condividerli con ogni altro account che deve farvi riferimento. Utilizzando un parametro Systems Manager, tutti i modelli di avvio possono essere aggiornati con un'unica operazione.

Un parametro Systems Manager è una coppia chiave-valore definita dall'utente che viene creata in Parameter Store.AWS Systems Manager Parameter Store fornisce un luogo centralizzato per archiviare i valori di configurazione dell'applicazione.

Nel diagramma seguente, il parametro `golden-ami` viene prima mappato all'AMI originale `ami-aabbccddeeffgghhi` nel Parameter Store. Nel modello di avvio, il valore dell'ID AMI è `golden-ami`. Quando un'istanza viene avviata utilizzando questo modello di avvio, l'ID AMI si risolve nell'`ami-aabbccddeeffgghhi`. Successivamente, l'AMI viene aggiornata con il risultato di un nuovo ID AMI. Nel Parameter Store, il parametro `golden-ami` è mappato alla nuova `ami-00112233445566778`. Il modello di avvio rimane invariato. Quando un'istanza viene avviata utilizzando questo modello di avvio, l'ID AMI si risolve nella nuova `ami-00112233445566778`.



Formato dei parametri Systems Manager per gli ID AMI

I modelli di avvio richiedono che i parametri Systems Manager definiti dall'utente rispettino il seguente formato quando vengono utilizzati al posto di un ID AMI:

- Tipo parametro: `String`

- Tipo di dati del parametro: `aws:ec2:image`. Garantisce che Parameter Store convalidi che il valore immesso sia nel formato corretto per un ID AMI.

Per ulteriori informazioni sulla creazione di un parametro valido per un ID AMI, consulta Creazione dei parametri Systems Manager nella Guida per l'utente AWS Systems Manager .

Formato dei parametri Systems Manager nei modelli di avvio

Per utilizzare un parametro Systems Manager al posto di un ID AMI in un modello di avvio, è necessario utilizzare uno dei seguenti formati quando si specifica il parametro nel modello di avvio:

Per fare riferimento a un parametro pubblico:

- `resolve:ssm:public-parameter`

Per fare riferimento a un parametro memorizzato nello stesso account:

- `resolve:ssm:parameter-name`
- `resolve:ssm:parameter-name:version-number`: il numero di versione stesso è un'etichetta predefinita
- `resolve:ssm:parameter-name:label`

Per fare riferimento a un parametro condiviso da un altro Account AWS:

- `resolve:ssm:parameter-ARN`
- `resolve:ssm:parameter-ARN:version-number`
- `resolve:ssm:parameter-ARN:label`

Versioni dei parametri

I parametri Systems Manager sono risorse con versione. Quando si aggiorna un parametro, si creano nuove versioni successive del parametro. Systems Manager supporta etichette dei parametri che è possibile mappare a versioni specifiche di un parametro.

Ad esempio, il parametro `golden-ami` può avere tre versioni: `1`, `2` e `3`. È possibile creare un'etichetta del parametro `beta` che corrisponde alla versione `2` e un'etichetta del parametro `prod` che corrisponde alla versione `3`.

In un modello di avvio, è possibile specificare la versione 3 del parametro `golden-ami` utilizzando uno dei seguenti formati:

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

Specificare la versione o l'etichetta è facoltativo. Quando non è specificata alcuna versione viene utilizzata la versione più recente del parametro.

Specificare un parametro Systems Manager in un modello di avvio

È possibile specificare un parametro Systems Manager in un modello di avvio anziché un ID AMI quando si crea un modello di avvio o una nuova versione di un modello di avvio.

Console

Per specificare un parametro Systems Manager in un modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Modelli di avvio quindi Crea modello di avvio.
3. In nome modello di avvio, inserire un nome descrittivo per il modello di avvio.
4. In Applicazioni e immagini SO (Amazon Machine Image), scegli Sfoglia altre AMI.
5. Scegli il pulsante con la freccia a destra della barra di ricerca, quindi scegli Specifica valore personalizzato/parametro Systems Manager.
6. Nella finestra di dialogo Specifica valore personalizzato o parametro Systems Manager, segui questi passaggi:

   a. Per la stringa ID AMI o parametro Manager Systems, inserisci il nome del parametro Systems Manager utilizzando uno dei seguenti formati:

      Per fare riferimento a un parametro pubblico:

      - **`resolve:ssm:`*`public-parameter`***

      Per fare riferimento a un parametro memorizzato nello stesso account:

      - **`resolve:ssm:`*`parameter-name`***
      - **`resolve:ssm:`*`parameter-name`*`:`*`version-number`***

- **resolve:ssm:*parameter-name*:*label***

  Per fare riferimento a un parametro condiviso da un altro Account AWS:

- **resolve:ssm:*parameter-ARN***
- **resolve:ssm:*parameter-ARN*:*version-number***
- **resolve:ssm:*parameter-ARN*:*label***

b. Selezionare Salva.

7. Specifica qualsiasi altro parametro del modello di avvio, se necessario, quindi scegli Crea modello di avvio.

Per ulteriori informazioni, consulta Crea un modello di lancio dai parametri.

AWS CLI

Per specificare un parametro Systems Manager in un modello di avvio

- Utilizzate il create-launch-templatecomando per creare il modello di lancio. Per specificare l'AMI da utilizzare, inserisci il nome del parametro Systems Manager utilizzando uno dei seguenti formati:

  Per fare riferimento a un parametro pubblico:

- **resolve:ssm:*public-parameter***

  Per fare riferimento a un parametro memorizzato nello stesso account:

- **resolve:ssm:*parameter-name***
- **resolve:ssm:*parameter-name*:*version-number***
- **resolve:ssm:*parameter-name*:*label***

  Per fare riferimento a un parametro condiviso da un altro Account AWS:

- **resolve:ssm:*parameter-ARN***
- **resolve:ssm:*parameter-ARN*:*version-number***
- **resolve:ssm:*parameter-ARN*:*label***

L'esempio seguente crea un modello di avvio che specifica quanto segue:

- Un nome per il modello di avvio (*TemplateForWebServer*)
- Un tag per il modello di avvio (*purpose*=*production*)
- I dati per la configurazione dell'istanza, specificati in un file JSON:
  - L'AMI da usare (`resolve:ssm:`*golden-ami*)
  - Il tipo di istanza da avviare (*m5.4xlarge*)
  - Un tag per l'istanza (*Name*=*webserver*)

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Di seguito è riportato un file JSON di esempio che contiene i dati del modello di avvio per la configurazione dell'istanza. Il valore di `ImageId` è il nome del parametro Systems Manager, inserito nel formato`resolve:ssm:`*golden-ami* richiesto.

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

Verifica che un modello di avvio riceva l'ID AMI corretto

Per risolvere il parametro Systems Manager nell'ID AMI effettivo

Utilizzate il describe-launch-template-versionscomando e includete il `--resolve-alias` parametro.

```
aws ec2 describe-launch-template-versions \
    --launch-template-name my-launch-template \
    --versions $Default \
    --resolve-alias
```

La risposta include l'ID AMI per`ImageId`. In questo esempio, quando un'istanza viene avviata utilizzando questo modello di avvio, l'ID AMI viene risolto in. `ami-0ac394d6a3example`

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-089c023a30example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2022-12-28T19:52:27.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0ac394d6a3example",
                "InstanceType": "t3.micro",
            }
        }
    ]
}
```

Risorse correlate

Per ulteriori informazioni sull'utilizzo dei parametri di Systems Manager, vedere i seguenti materiali di riferimento nella documentazione di Systems Manager.

- Per informazioni su come cercare i parametri pubblici dell'AMI supportati da Amazon EC2, consulta Chiamata dei parametri pubblici dell'AMI.
- Per informazioni sulla condivisione dei parametri con altri AWS account o tramite AWS Organizations, consulta Lavorare con parametri condivisi.
- Per informazioni sul monitoraggio della corretta creazione dei parametri, consulta Supporto nativo dei parametri per Amazon Machine Image ID.

Limitazioni

- Attualmente, i parchi istanze EC2 e le serie di istanze spot non supportano l'utilizzo di un modello di avvio per cui è specificato un parametro System Manager anziché un ID AMI. Per i parchi istanze EC2 e le serie di istanze spot, se nel modello di avvio indichi un'AMI, devi specificare l'ID dell'AMI.
- Amazon EC2 Auto Scaling prevede altre restrizioni. Per ulteriori informazioni, consulta Utilizzare AWS Systems Manager i parametri anziché gli ID AMI nei modelli di avvio nella Guida per l'utente di Amazon EC2 Auto Scaling.

Modificare un modello di avvio (gestire le versioni dei modelli di avvio)

I modelli di avvio sono immutabili; dopo aver creato un modello di avvio, non puoi più modificarlo. È invece possibile creare una nuova versione del modello di avvio che includa tutte le modifiche necessarie.

Per un modello di avvio puoi creare due diverse versioni, impostare la versione di default, descrivere una versione del modello di avvio ed eliminare le versioni non più necessarie.

Attività

- Creazione di una versione del modello di avvio
- Impostazione della versione del modello di avvio predefinita
- Descrizione di una versione del modello di avvio
- Eliminazione di una versione del modello di avvio

Creazione di una versione del modello di avvio

Quando crei una versione del modello di avvio, è possibile specificare nuovi parametri di lancio o utilizzare una versione esistente come base per la nuova versione. Per ulteriori informazioni sui parametri di avvio, vedi Creazione di un modello di avvio.

Console

Creazione di una versione del modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.

3. Seleziona un modello di avvio e poi seleziona Actions (Operazioni), Modify template (Create new version) (Modifica modello - Crea nuova versione).
4. Alla voce Template version description (Descrizione della versione del modello), inserire una descrizione per la versione del modello di avvio.
5. (Facoltativo) Espandere Source template (Modello origine) e selezionare una versione del modello di avvio da utilizzare come base per la nuova versione del modello di avvio. La nuova versione del modello di avvio eredita i parametri di avvio da questa versione del modello di avvio.
6. Regolare i parametri di avvio come desiderato e scegliere Create launch template (Crea modello di avvio).

AWS CLI

Creazione di una versione del modello di avvio

- Utilizza il comando create-launch-template-version. È possibile specificare una versione di origine su cui basare la nuova versione. La nuova versione eredita gli stessi parametri di avvio da questa versione ed è possibile sovrascrivere i parametri utilizzando `--launch-template-data`. L'esempio seguente crea una nuova versione basata sulla versione 1 del modello di avvio e specifica un ID AMI diverso.

```
aws ec2 create-launch-template-version \
    --launch-template-id lt-0abcd290751193123 \
    --version-description WebVersion2 \
    --source-version 1 \
    --launch-template-data "ImageId=ami-c998b6b2"
```

Impostazione della versione del modello di avvio predefinita

È possibile impostare la versione predefinita per il modello di avvio. Quando avvii un'istanza da un modello di avvio e non specifichi una versione, l'istanza viene avviata utilizzando i parametri della versione predefinita.

Console

Impostazione della versione del modello di avvio predefinita

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Selezionare il modello di avvio e scegliere Actions (Operazioni), Set default version (Imposta nome versione predefinita).
4. Per Template version (Versione modello), selezionare il numero di versione da impostare come versione predefinita e scegliere Set as default version (Imposta come versione predefinita).

AWS CLI

Impostazione della versione del modello di avvio predefinita

- Usa il modify-launch-templatecomando e specifica la versione che desideri impostare come predefinita.

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

Descrizione di una versione del modello di avvio

Utilizzando la console, è possibile visualizzare tutte le versioni del modello di avvio selezionato o ottenere un elenco dei modelli di avvio la cui versione più recente o predefinita corrisponde a un numero di versione specifico. Utilizzando AWS CLI, è possibile descrivere tutte le versioni, le singole versioni o una serie di versioni di un modello di lancio specificato. Puoi anche descrivere tutte le versioni più recenti o tutte le versioni predefinite di tutti i modelli di lancio nel tuo account.

Console

Descrizione di una versione del modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Puoi visualizzare una versione di un modello di avvio specifico o ottenere un elenco dei modelli di avvio la cui versione più recente o predefinita corrisponde a un numero di versione specifico.
    - Per visualizzare una versione di un modello di avvio: selezionare il modello di avvio. Nella scheda Versioni in Versione, selezionare una versione per visualizzarne i dettagli.

- Per ottenere un elenco di tutti i modelli di avvio la cui versione più recente corrisponde a un numero di versione specifico: dalla barra di ricerca scegliere Versione più recente, quindi scegliere un numero di versione.
- Per ottenere un elenco di tutti i modelli di avvio la cui versione predefinita corrisponde a un numero di versione specifico: dalla barra di ricerca scegliere Versione predefinita, quindi scegliere un numero di versione.

AWS CLI

Descrizione di una versione del modello di avvio

- Utilizzate il describe-launch-template-versionscomando e specificate i numeri di versione. Nell'esempio seguente vengono specificate le versioni *1* e *3*.

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

Descrizione di tutte le versioni più recenti e predefinite del modello di avvio nell'account

- Utilizzate il describe-launch-template-versionscomando e specificate `$Latest$Default`, o entrambi. Nella chiamata ometti il nome e l'ID del modello di avvio. Non è possibile specificare i numeri di versione.

```
aws ec2 describe-launch-template-versions \
    --versions "$Latest,$Default"
```

Eliminazione di una versione del modello di avvio

Se non è più necessaria una versione del modello di avvio, è possibile eliminarla.

Considerazioni

- Non è possibile sostituire il numero di versione dopo averlo eliminato.
- Non è possibile eliminare la versione predefinita del modello di avvio; è necessario prima assegnare una versione diversa come predefinita. Se la versione predefinita è l'unica versione del modello di avvio, devi eliminare l'intero modello di avvio.

- Utilizzando la console, puoi eliminare una versione del modello alla volta. Quando si utilizza AWS CLI, è possibile eliminare fino a 200 versioni del modello di avvio in un'unica richiesta. Per eliminare più di 200 versioni con una sola richiesta, puoi eliminare il modello di avvio, che elimina anche tutte le sue versioni.

Console

Eliminazione di una versione del modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Selezionare il modello di avvio e scegliere Actions (Operazioni), Delete template version (Elimina versione del modello).
4. Selezionare la versione da eliminare e scegliere Delete (Elimina).

AWS CLI

Eliminazione di una versione del modello di avvio

- Utilizzate il delete-launch-template-versionscomando e specificate i numeri di versione da eliminare. Puoi specificare fino a 200 versioni del modello di avvio da eliminare in una singola richiesta.

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1
```

Eliminare un modello di avvio

Se non è più necessario un modello di avvio, è possibile eliminarlo. L'eliminazione di un modello di avvio ne elimina tutte le versioni. Per eliminare una versione specifica di un modello di avvio, consulta la pagina Eliminazione di una versione del modello di avvio.

Quando elimini un modello di avvio, ciò non influisce sulle istanze avviate da tale modello.

Console

Eliminazione di un modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Selezionare il modello di avvio e scegliere Actions (Operazioni), Delete template (Elimina modello).
4. Immettere **`Delete`** per confermare l'eliminazione, quindi scegliere Delete (Elimina).

AWS CLI

Per eliminare un modello di avvio

Utilizzate il comando delete-launch-template(AWS CLI) e specificate il modello di lancio.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

PowerShell

Per eliminare un modello di avvio

Utilizzate il comando Remove-EC2LaunchTemplate(AWS Tools for PowerShell) e specificate il modello di avvio. Se `-Force` viene omesso, PowerShell richiede una conferma.

```
Remove-EC2LaunchTemplate -LaunchTemplateId lt-0123456789example -Force
```

Avvio di istanze da un modello di avvio

I modelli di avvio sono supportati da diversi servizi di avvio delle istanze. Questo argomento descrive come utilizzare un modello di avvio quando si avvia un'istanza utilizzando la procedura guidata di avvio EC2, Dimensionamento automatico Amazon EC2, parco istanze EC2 e parco istanze spot.

Argomenti

- Avvio di un'istanza da un modello di avvio
- Utilizzo dei modelli di avvio con Amazon EC2 Auto Scaling
- Utilizzo dei modelli di avvio con Parco istanze EC2
- Utilizzo dei modelli di avvio con Parco istanze spot

Avvio di un'istanza da un modello di avvio

È possibile utilizzare i parametri contenuti in un modello di avvio per avviare un'istanza. Hai la possibilità di sovrascrivere o aggiungere parametri di lancio prima di avviare l'istanza.

Alle istanze che vengono avviate tramite un modello di avvio vengono automaticamente assegnati due tag con le chiavi `aws:ec2launchtemplate:id` e `aws:ec2launchtemplate:version`. Non è possibile rimuovere o modificare questi tag.

Console

Per avviare un'istanza da un modello di avvio tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Selezionare il modello di avvio e scegliere Actions (Operazioni), Launch instance from template (Lancia istanza dal modello).
4. Per Source template version (Versione modello origine), selezionare la versione del modello di avvio da utilizzare.
5. Per Number of instances (Numero di istanze), specificare il numero di istanze da lanciare.
6. (Opzionale) È possibile sovrascrivere o aggiungere i parametri del modello di avvio modificando e aggiungendo parametri nella sezione Instance details (Dettagli istanza).
7. Scegliere Launch instance from template (Avvia istanza dal modello).

AWS CLI

Per avviare un'istanza da un modello di avvio tramite AWS CLI

- Utilizzare il comando run-instances e specificare il parametro `--launch-template`. Facoltativamente, specificare la versione del modello di avvio da utilizzare. Se non specifichi la versione, viene utilizzata la versione predefinita.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Per sovrascrivere un parametro del modello di avvio, specificare il parametro nel comando run-instances. L'esempio seguente sovrascrive il tipo di istanza specificato nel modello di avvio (se presente).

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- Se specifichi un parametro nidificato che fa parte di una struttura complessa, l'istanza viene avviata utilizzando la struttura complessa come specificato nel modello di avvio, oltre a eventuali parametri nidificati aggiuntivi specificati.

  Nell'esempio seguente, l'istanza viene avviata con il tag *Owner*=*TeamA*, oltre a qualsiasi altro tag specificato nel modello di avvio. Se il modello di avvio ha un tag esistente con una chiave di *Owner*, il valore viene sostituito con *TeamA*.

  ```
  aws ec2 run-instances \
      --launch-template LaunchTemplateId=lt-0abcd290751193123 \
      --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
  ```

  Nell'esempio seguente, l'istanza viene avviata con un volume con il nome dispositivo */dev/xvdb*, oltre a qualsiasi altra mappatura dei dispositivi a blocchi specificata nel modello di avvio. Se il modello di avvio ha un volume esistente definito per */dev/xvdb*, i suoi valori vengono sostituiti con valori specificati.

  ```
  aws ec2 run-instances \
      --launch-template LaunchTemplateId=lt-0abcd290751193123 \
      --block-device-mappings "DeviceName=/dev/
  xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
  ```

Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

PowerShell

Per avviare un'istanza da un modello di avvio tramite AWS Tools for PowerShell

- Usa il New-EC2Instancecomando e specifica il `-LaunchTemplate` parametro. Facoltativamente, specificare la versione del modello di avvio da utilizzare. Se non specifichi la versione, viene utilizzata la versione predefinita.

  ```
  Import-Module AWS.Tools.EC2
  New-EC2Instance `
  ```

```
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Per sovrascrivere un parametro del modello di avvio, specificate il parametro nel New-EC2Instancecomando. L'esempio seguente sovrascrive il tipo di istanza specificato nel modello di avvio (se presente).

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Se specifichi un parametro nidificato che fa parte di una struttura complessa, l'istanza viene avviata utilizzando la struttura complessa come specificato nel modello di avvio, oltre a eventuali parametri nidificati aggiuntivi specificati.

  Nell'esempio seguente, l'istanza viene avviata con il tag *Owner*=*TeamA*, oltre a qualsiasi altro tag specificato nel modello di avvio. Se il modello di avvio ha un tag esistente con una chiave di *Owner*, il valore viene sostituito con *TeamA*.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
        }
) `
    -TagSpecification (
```

```
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags         = @(
                @{key = "Owner"; value = "TeamA" },
                @{key = "Department"; value = "Operations" }
            )
        }
)
```

Nell'esempio seguente, l'istanza viene avviata con un volume con il nome dispositivo */dev/xvdb*, oltre a qualsiasi altra mappatura dei dispositivi a blocchi specificata nel modello di avvio. Se il modello di avvio ha un volume esistente definito per */dev/xvdb*, i suoi valori vengono sostituiti con valori specificati.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
) `
    -BlockDeviceMapping  (
        New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
            DeviceName = '/dev/xvdb';
            EBS        = (
                New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
                    VolumeSize = 25;
                    VolumeType = 'gp3'
                }
            )
        }
)
```

Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

Utilizzo dei modelli di avvio con Amazon EC2 Auto Scaling

È possibile creare un gruppo Auto Scaling e specificare un modello di avvio da utilizzare per il gruppo. Quando Amazon EC2 Auto Scaling avvia le istanze nel gruppo Auto Scaling, utilizza i parametri di lancio definiti nel modello di avvio associato. Per ulteriori informazioni, consulta Creare un modello di lancio per un gruppo Auto Scaling e Creare un modello di lancio utilizzando impostazioni avanzate nella Guida per l'utente di Amazon EC2 Auto Scaling.

Prima di poter creare un gruppo Auto Scaling utilizzando un modello di avvio, è necessario creare un modello di avvio che includa i parametri necessari per avviare un'istanza in un gruppo Auto Scaling, ad esempio l'ID dell'AMI. La console fornisce indicazioni per aiutarti a creare un modello da utilizzare con Amazon EC2 Auto Scaling.

Per creare un modello di avvio con Auto Scaling utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Modelli di avvio quindi Crea modello di avvio.
3. In nome modello di avvio, inserire un nome descrittivo per il modello di avvio.
4. In Template version description (Descrizione versione modello), fornire una breve descrizione della versione del modello di avvio.
5. Nella sezione Auto Scaling guidance (Guida di AS), selezionare la casella di controllo affinché Amazon EC2 fornisca indicazioni utili per creare un modello da utilizzare con Auto Scaling.
6. Modificare i parametri di lancio come richiesto. Poiché è stata selezionata l'opzione “Auto Scaling guidance”, alcuni campi sono obbligatori e alcuni campi non sono disponibili. Per informazioni su come configurare i parametri di avvio per Amazon EC2 Auto Scaling, consulta Creare un modello di avvio per un gruppo Auto Scaling e Creare un modello di avvio utilizzando impostazioni avanzate nellaAmazon EC2 Auto Scaling User Guide.
7. Scegli Crea modello di avvio.
8. (Facoltativo) Per creare un gruppo con scalabilità automatica utilizzando questo modello di avvio, nella pagina Next steps (Passaggi successivi) scegli Create Auto Scaling group (Crea gruppo con scalabilità automatica).

Per esempi che mostrano come utilizzare per AWS CLI creare modelli di lancio con varie combinazioni di parametri, consulta Esempi per la creazione e la gestione di modelli di lancio con AWS Command Line Interface (AWS CLI) nella Guida per l'utente di Amazon EC2 Auto Scaling.

Per creare o aggiornare un gruppo Auto Scaling con un modello di avvio utilizzando il AWS CLI

- Utilizzate il update-auto-scaling-groupcomando create-auto-scaling-groupo e specificate il `--launch-template` parametro.

Per ulteriori informazioni sulla creazione o l'aggiornamento di un gruppo Auto Scaling utilizzando un modello di lancio, consulta i seguenti argomenti nella Amazon EC2 Auto Scaling User Guide.

- Crea gruppi di Auto Scaling utilizzando modelli di avvio
- Aggiornare un gruppo Auto Scaling

Utilizzo dei modelli di avvio con Parco istanze EC2

È possibile creare una richiesta Parco istanze EC2 e specificare un modello di avvio nella configurazione dell'istanza. Quando Amazon EC2 soddisfa la richiesta Parco istanze EC2, utilizza i parametri di lancio definiti nel modello di avvio associato. È possibile sovrascrivere alcuni dei parametri specificati nel modello di avvio.

Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

Per creare una flotta EC2 con un modello di lancio utilizzando il AWS CLI

- Utilizzare il comando create-fleet. Utilizzare il parametro `--launch-template-configs` per specificare il modello di avvio ed eventuali sostituzioni per il modello di avvio.

Utilizzo dei modelli di avvio con Parco istanze spot

È possibile creare una richiesta Parco istanze spot e specificare un modello di avvio nella configurazione dell'istanza. Quando Amazon EC2 soddisfa la richiesta di Parco istanze spot, utilizza i parametri di avvio definiti nel modello di avvio associato. È possibile sovrascrivere alcuni dei parametri specificati nel modello di avvio.

Per ulteriori informazioni, consulta Creare una richiesta di parco istanze spot.

Creazione di una richiesta di parco istanze spot con un modello di avvio mediante la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare Request Spot Instances (Richiedi istanze Spot).

4. In Launch parameters (Parametri di avvio), scegli Use a launch template (Utilizza un modello di avvio).
5. Per Launch template (Modello di avvio), scegli un modello di avvio, quindi, dal campo a destra, scegli la versione del modello di avvio.
6. Configura il parco istanze spot selezionando diverse opzioni su questa schermata. Per ulteriori informazioni su queste opzioni, consulta Creare una richiesta di parco istanze spot utilizzando parametri definiti (console).
7. Quando è tutto pronto per la creazione del parco istanze spot, scegli Launch (Avvia).

Per creare una richiesta Spot Fleet con un modello di lancio utilizzando il AWS CLI

- Utilizza il comando request-spot-fleet. Utilizzare il parametro `LaunchTemplateConfigs` per specificare il modello di avvio ed eventuali sostituzioni per il modello di avvio.

Avvio di un'istanza con i parametri di un'istanza esistente

Nella console Amazon EC2 è disponibile l'opzione Launch more like this (Avvia altre come questa) che ti consente di utilizzare l'istanza corrente come base per l'avvio di altre istanze. Questa opzione popola automaticamente la procedura guidata di avvio dell'istanza Amazon EC2 con specifici dettagli di configurazione derivati dall'istanza selezionata.

Considerazioni

- Non cloniamo le istanze, ma replichiamo solamente alcuni dei dettagli di configurazione. Per creare una copia dell'istanza, devi innanzitutto creare un'AMI da tale istanza, quindi avviare altre istanze da tale AMI. Crea un modello di avvio per assicurarti di avviare le istanze utilizzando gli stessi dettagli di avvio.
- L'istanza attuale deve essere nello stato `running`.

Dettagli copiati

I seguenti dettagli di configurazione vengono copiati dall'istanza selezionata alla procedura guidata di avvio dell'istanza:

- ID AMI
- Tipo di istanza

- Zona di disponibilità o VPC e sottorete in cui si trova l'istanza selezionata
- Indirizzo IPv4 pubblico. Se l'istanza selezionata attualmente dispone di un indirizzo IPv4 pubblico, la nuova istanza riceve un indirizzo IPv4 pubblico, indipendentemente dall'impostazione di default dell'indirizzo IPv4 pubblico dell'istanza selezionata. Per ulteriori informazioni sugli indirizzi IPv4 pubblici, consulta Indirizzi IPv4 pubblici.
- Gruppo di collocamento, se applicabile
- Ruolo IAM associato all'istanza, se applicabile
- Impostazione relativa al comportamento dell'arresto (arresto o interruzione)
- Impostazione relativa alla protezione per l'interruzione (true o false)
- CloudWatch monitoraggio (abilitato o disabilitato)
- Impostazione relativa all'ottimizzazione Amazon EBS (true o false)
- Impostazione relativa alla tenancy, in caso di avvio in un VPC (condiviso o dedicato)
- ID kernel e ID disco RAM, se applicabili
- Dati utente, se specificati
- Tag associati all'istanza, se applicabili
- Gruppi di sicurezza associati all'istanza
- [Istanze Windows] Informazioni sull'associazione. Se l'istanza selezionata è associata a un file di configurazione, tale file viene automaticamente associato alla nuova istanza. Se il file di configurazione include una configurazione di aggiunta al dominio, la nuova istanza viene aggiunta a tale dominio. Per ulteriori informazioni sull'aggiunta di un dominio, consulta Aggiunta di un'istanza EC2 Windows in AWS Directory Service Administration Guide.

Dettagli non copiati

I seguenti dettagli di configurazione non vengono copiati dall'istanza selezionata. La procedura guidata applica invece le impostazioni o il comportamento predefiniti:

- Numero di interfacce di rete: il valore predefinito prevede un'interfaccia di rete, ovvero l'interfaccia di rete primaria (eth0).
- Archiviazione: la configurazione di archiviazione di default è determinata dall'AMI e dal tipo di istanza.

Per avviare più istanze come un'istanza esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona un'istanza, quindi scegli Operazioni, Immagini e modelli, Avvia altre come questa.
4. Si apre la procedura guidata dell'istanza di avvio. Puoi apportare le modifiche necessarie alla configurazione dell'istanza selezionando diverse opzioni in questa schermata.

   Quando sei pronto ad avviare l'istanza, scegli Launch instance (Avvia istanza).
5. Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

Avvia un' Marketplace AWS istanza

Puoi abbonarti a un Marketplace AWS prodotto e avviare un'istanza dall'AMI del prodotto utilizzando la procedura guidata di avvio di Amazon EC2. Per ulteriori informazioni sulle AMI pagate, consulta AMI a pagamento. Per annullare la sottoscrizione dopo l'avvio, devi prima terminare tutte le istanze eseguite da tale AMI. Per ulteriori informazioni, consulta Gestisci i tuoi abbonamenti Marketplace AWS.

New console

Per avviare un'istanza Marketplace AWS utilizzando la procedura guidata di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
3. (Facoltativo) in Name and tags (Nome e tag), per Name (Nome), inserire un nome descrittivo per la propria istanza.
4. In Applicazioni e immagini SO (Amazon Machine Image), scegli Sfoglia altre AMI e seleziona la scheda AMI Marketplace AWS). Individua un'AMI idonea sfogliando le categorie oppure utilizzando la funzionalità di ricerca. Scegli Select (Seleziona) per scegliere un prodotto.
5. Si apre una finestra con una panoramica del prodotto selezionato. È possibile visualizzare le informazioni sui prezzi, nonché alte informazioni specificate dal fornitore. Quando sei pronto, scegli uno dei seguenti pulsanti:

   - Abbonati al lancio dell'istanza: l'abbonamento inizia quando scegli Launch instance (al passaggio 10).

- Abbonati ora: l'abbonamento inizia immediatamente. Mentre l'abbonamento è in corso, puoi configurare l'istanza continuando con i passaggi di questa procedura. Se sono presenti problemi con i dettagli della carta di credito, verrà richiesto di aggiornare i dettagli dell'account.

> **Note**
>
> Non è previsto alcun addebito per l'utilizzo del prodotto finché non viene avviata un'istanza mediante l'AMI. Presta attenzione ai prezzi per ogni tipo di istanza supportata quando selezioni un tipo di istanza. Al prodotto potrebbero essere applicate anche tasse aggiuntive.

6. Per Instance type (Tipo di istanza), seleziona un tipo di istanza. Il tipo di istanza definisce la configurazione hardware e le dimensioni dell'istanza da avviare.
7. In Key pair (login) (Coppia di chiavi (login), per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o creane una nuova.
8. In Network settings (Impostazioni di rete),Firewall (security groups) (Firewall [gruppi di sicurezza]), prendi nota del nuovo gruppo di sicurezza creato in base alle specifiche definite dal fornitore per il prodotto. Il gruppo di sicurezza può includere regole che consentono a tutti gli indirizzi IPv4 (`0.0.0.0/0`) l'accesso su SSH (porta 22) su Linux o RDP (porta 3389) su Windows. Consigliamo di modificare queste regole per consentire solo a un indirizzo specifico o a uno specifico intervallo di indirizzi di accedere all'istanza tramite queste porte.
9. Puoi utilizzare gli altri campi sullo schermo per configurare l'istanza e aggiungere storage e tag. Per ulteriori informazioni sulle diverse opzioni configurabili, consulta Avvio di un'istanza utilizzando parametri definiti.
10. Nel pannello Summary (Riepilogo), in Software Image (AMI) (Immagine software [AMI]), verifica dettagli dell'AMI da cui si sta avviando l'istanza. Verifica anche gli altri dettagli di configurazione che hai specificato. Quando si è pronti per avviare l'istanza, scegliere Launch instance (Avvia istanza).
11. A seconda del prodotto a cui è stata eseguita la sottoscrizione, l'avvio dell'istanza può richiedere alcuni minuti. Se hai scelto Abbonati all'avvio dell'istanza nella Fase 5, ti sei abbonato al prodotto prima che l'istanza possa essere lanciata. Se sono presenti problemi con i dettagli della carta di credito, verrà richiesto di aggiornare i dettagli dell'account. Quando viene visualizzata la pagina di conferma dell'avvio, scegli View all instances (Visualizza tutte le istanze) per passare alla pagina Instances (Istanze).

> **Note**
>
> Verrà addebitato il prezzo della sottoscrizione a condizione che l'istanza sia nello stato `running`, anche se inattiva. Se l'istanza viene arrestata, potrebbe continuare a venire addebitato il costo dell'archiviazione.

12. Quando lo stato dell'istanza è `running`, sarà possibile connettersi a tale istanza. A tale scopo, seleziona l'istanza nell'elenco, scegli Connect (Connetti), quindi scegli un'opzione di connessione. Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza di LinuxConnettiti all'istanza Windows .

> **Important**
>
> Controllare attentamente le istruzioni relative all'utilizzo del fornitore perché potrebbe essere necessario utilizzare un nome utente specifico per connettersi all'istanza. Per ulteriori informazioni sull'accesso ai dettagli della sottoscrizione, consulta Gestisci i tuoi abbonamenti Marketplace AWS.

13. Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

Old console

Per avviare un'istanza Marketplace AWS utilizzando la procedura guidata di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di controllo Amazon EC2, selezionare Launch Instance (Avvia istanza).
3. Nella pagina Choose an Amazon Machine Image (AMI) (Scegli immagine macchina Amazon [AMI]) scegliere la categoria Marketplace AWS a sinistra. Individuare un'AMI idonea sfogliando le categorie oppure utilizzando la funzionalità di ricerca. Scegliere Select (Seleziona) per scegliere il prodotto.
4. In una finestra di dialogo viene visualizzata la panoramica del prodotto selezionato. È possibile visualizzare le informazioni sui prezzi, nonché alte informazioni specificate dal fornitore. Al termine, scegliere Continue (Continua).

> **Note**
>
> Non è previsto alcun addebito per l'utilizzo del prodotto finché non viene avviata un'istanza mediante l'AMI. Prestare attenzione ai prezzi per ogni tipo di istanza supportata perché verrà richiesto di selezionare un tipo di istanza nella pagina successiva della procedura guidata. Al prodotto potrebbero essere applicate anche tasse aggiuntive.

5. Nella pagina Choose an Instance Type (Scegli un tipo di istanza), selezionare la configurazione hardware e le dimensioni dell'istanza da avviare. Al termine, scegliere Next: Configure Instance Details (Successivo: Configura i dettagli dell'istanza).
6. Nelle pagine successive della procedura guidata è possibile configurare l'istanza, nonché aggiungere archiviazione e tag. Per ulteriori informazioni sulle diverse opzioni configurabili, consultare Avvio di un'istanza tramite la vecchia procedura guidata di avvio. Scegliere Next (Successivo) fino a raggiungere la pagina Configure Security Group (Configura gruppo di sicurezza).

   La procedura guidata crea un nuovo gruppo di sicurezza in base alle specifiche definite dal fornitore per il prodotto. Il gruppo di sicurezza può includere regole che consentono a tutti gli indirizzi IPv4 (`0.0.0.0/0`) l'accesso su SSH (porta 22) su Linux o RDP (porta 3389) su Windows. Consigliamo di modificare queste regole per consentire solo a un indirizzo specifico o a uno specifico intervallo di indirizzi di accedere all'istanza tramite queste porte.

   Al termine, scegliere Review and Launch (Analizza e avvia).
7. Nella pagina Review Instance Launch (Riconsulta l'avvio dell'istanza) controllare i dettagli dell'AMI da cui si sta avviando l'istanza, nonché gli altri dettagli di configurazione definiti durante la procedura guidata. Al termine, scegliere Launch (Avvia) per selezionare o creare una coppia di chiavi e avviare l'istanza.
8. A seconda del prodotto a cui è stata eseguita la sottoscrizione, l'avvio dell'istanza può richiedere alcuni minuti. Prima di poter avviare l'istanza, è prima necessario effettuare la sottoscrizione al prodotto. Se sono presenti problemi con i dettagli della carta di credito, verrà richiesto di aggiornare i dettagli dell'account. Quando viene visualizzata la pagina di conferma dell'avvio, scegliere View Instances (Visualizza istanze) per passare alla pagina Instances (Istanze).

> **Note**
>
> Verrà addebitato il prezzo della sottoscrizione a condizione che l'istanza sia in esecuzione, anche se inattiva. Se l'istanza viene arrestata, potrebbe continuare a venire addebitato il costo dell'archiviazione.

9. Quando lo stato dell'istanza è `running`, sarà possibile connettersi a tale istanza. A tale scopo, selezionare l'istanza nell'elenco e scegliere Connect (Connetti). Seguire le istruzioni visualizzate nella finestra di dialogo. Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza di LinuxConnettiti all'istanza Windows .

> **Important**
>
> Controllare attentamente le istruzioni relative all'utilizzo del fornitore perché potrebbe essere necessario utilizzare un nome utente specifico per eseguire l'accesso all'istanza. Per ulteriori informazioni sull'accesso ai dettagli della sottoscrizione, consultare Gestisci i tuoi abbonamenti Marketplace AWS.

10. Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

Avvia un'istanza Marketplace AWS AMI utilizzando l'API e la CLI

Per avviare istanze da Marketplace AWS prodotti che utilizzano l'API o gli strumenti da riga di comando, assicurati innanzitutto di essere abbonato al prodotto. Puoi quindi avviare un'istanza con l'ID AMI del prodotto utilizzando i seguenti metodi:

Metodo	Documentazione
AWS CLI	Utilizzare il comando run-instances o per ulteriori informazioni visualizzare il seguente argomento relativo all'avvio di un'istanza.
AWS Tools for Windows PowerShell	Usa il New-EC2Instancecomando o consulta il seguente argomento per ulteriori informazioni: Avvio di un'istanza Amazon EC2 tramite Windows PowerShell
API della query	Usa la RunInstancesrichiesta.

Arresta e avvia le istanze Amazon EC2

Puoi arrestare e avviare la tua istanza se provvista di un volume Amazon EBS come dispositivo root. Quando interrompi un'istanza, questa si spegne. Quando si avvia un'istanza, in genere questa viene migrata su un nuovo computer host sottostante e viene assegnato un nuovo indirizzo IPv4 pubblico.

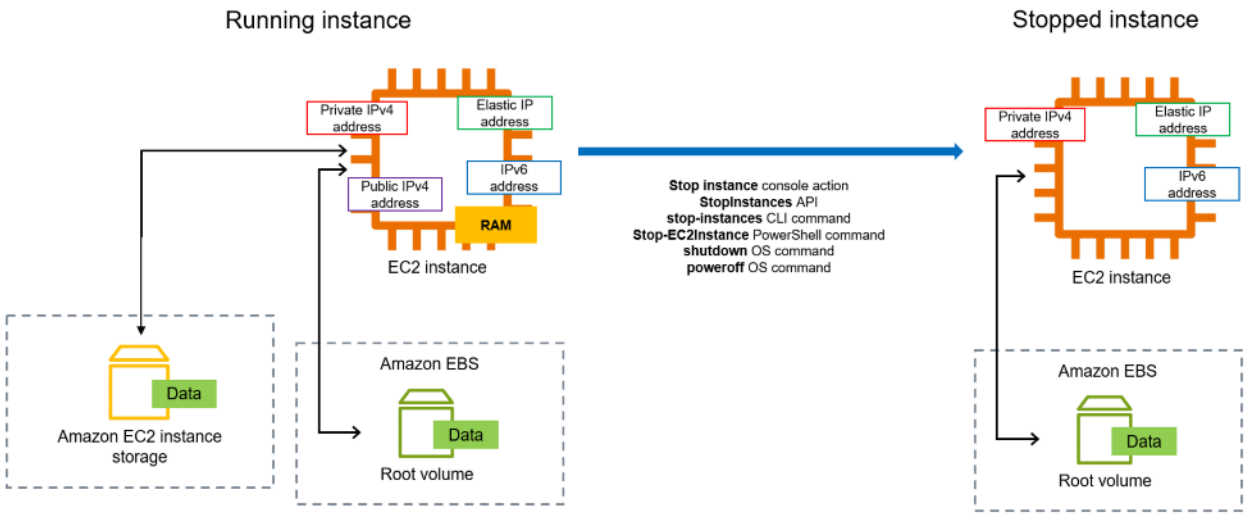
Quando interrompi un'istanza, questa non viene eliminata. Se decidi che non ti occorre più un'istanza, puoi terminarla. Per ulteriori informazioni, consulta Termina le istanze Amazon EC2. Se desideri ibernare un'istanza per salvare il contenuto dalla memoria dell'istanza (RAM), consulta Metti in ibernazione la tua istanza Amazon EC2. Per le distinzioni tra le operazioni relative al ciclo di vita delle istanze, consultare Differenze tra riavvio, arresto, ibernazione e interruzione.

Indice

Come funzionano lo stop and start dell'istanza

Quando si arresta un'istanza, le modifiche vengono registrate a livello di sistema operativo dell'istanza, alcune risorse vengono perse e altre persistono. Quando si avvia un'istanza, le modifiche vengono registrate a livello di istanza.

Il diagramma seguente mostra cosa viene perso e cosa persiste quando un'istanza Amazon EC2 viene arrestata. Quando un'istanza si arresta, perde tutti i volumi di instance store collegati e i dati memorizzati su tali volumi, i dati archiviati nella RAM dell'istanza e l'indirizzo IPv4 pubblico assegnato se all'istanza non è associato un indirizzo IP elastico. Un'istanza conserva gli indirizzi IPv4 privati assegnati, gli indirizzi IP elastici associati all'istanza, qualsiasi indirizzo IPv6 e tutti i volumi Amazon EBS collegati e i dati su tali volumi.



Cosa succede quando arresti un'istanza

Modifiche registrate a livello di sistema operativo

- La richiesta dell'API invia un evento di pressione del pulsante al sistema guest.
- Vari servizi di sistema vengono arrestati a seguito dell'evento di pressione del pulsante. L'arresto graceful viene attivato dall'evento di pressione del pulsante di arresto ACPI dall'hypervisor.
- L'arresto ACPI viene avviato.
- L'istanza viene arrestata quando si esce dal processo di arresto normale. Non c'è un orario di arresto del sistema operativo configurabile.
- Se il sistema operativo dell'istanza non si chiude correttamente entro alcuni minuti, viene eseguito un arresto forzato.
- L'esecuzione dell'istanza viene interrotta.
- Lo stato dell'istanza cambia in `stopping` (arresto in corso) e quindi in `stopped` (arrestata).
- [Dimensionamento automatico] Se la tua istanza è un gruppo con dimensionamento automatico, quando l'istanza è in qualsiasi stato dell'istanza Amazon EC2 diverso da `running` oppure se lo stato del sistema è `impaired`, il Dimensionamento automatico Amazon EC2 considera l'istanza non integra e la sostituisce. Per ulteriori informazioni, consulta Controllo dello stato nelle istanze Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.
- [Istanze Windows] Quando si arresta e si avvia un'istanza Windows, l'agente di avvio esegue attività sull'istanza, come la modifica delle lettere di unità per tutti i volumi Amazon EBS collegati. Per ulteriori informazioni su queste impostazioni predefinite e su come modificarle, consulta. the section called “EC2Launch v2”

Risorse perse

- I dati archiviati nella RAM.
- I dati archiviati nei volumi dell'instance store.
- L'indirizzo IPv4 pubblico assegnato automaticamente ad Amazon EC2 all'istanza all'avvio o all'inizio. Per mantenere un indirizzo IPv4 pubblico che non cambia mai, è possibile associare un indirizzo IP elastico all'istanza.

Risorse che persistono

- Qualsiasi volume Amazon EBS collegato.
- I dati archiviati nei volumi Amazon EBS collegati.
- Gli indirizzi IPv4 privati.
- Gli indirizzi IPv6.
- L'indirizzo IP elastico associato all'istanza. Tieni presente che quando l'istanza viene interrotta, ti verranno addebitati i costi degli indirizzi IP elastici associati.

Per informazioni su cosa succede quando interrompi un'istanza Mac, consultathe section called “Arresta o termina l'istanza Mac”.

Cosa succede quando avvii un'istanza

Modifiche registrate a livello di sistema operativo

- Nella maggior parte dei casi, l'istanza viene migrata in un nuovo computer host sottostante (sebbene in alcuni casi, come quando un'istanza è assegnata a un host in una configurazione del Host dedicato, rimanga sull'host corrente).
- Amazon EC2 assegna un nuovo indirizzo IPv4 pubblico all'istanza se la stessa è configurata per ricevere un indirizzo IPv4 pubblico. Per mantenere un indirizzo IPv4 pubblico che non cambia mai, è possibile associare un indirizzo IP elastico all'istanza.

Testare la risposta dell'applicazione per interromperla e avviarla

È possibile AWS Fault Injection Service utilizzarle per verificare la risposta dell'applicazione all'arresto e all'avvio dell'istanza. Per ulteriori informazioni, consulta la Guida per l'utente AWS Fault Injection Service.

Costi relativi all'arresto e all'avvio dell'istanza

I seguenti costi sono associati all'arresto e all'avvio di un'istanza.

Arresto: non appena lo stato di un'istanza cambia in `shutting-down` o `terminated`, non vengono più addebitati costi per l'istanza. Non ti vengono addebitati i costi di utilizzo o di trasferimento dei dati per un'istanza arrestata. Vengono addebitati costi per archiviare i volumi di archiviazione Amazon EBS.

Avvio: ogni volta che avvii un'istanza arrestata, ti viene addebitato un minimo di un minuto per l'utilizzo. Dopo un minuto, ti vengono addebitati soli i secondi che utilizzi. Ad esempio, se esegui un'istanza per 20 secondi e poi la arresti, ti viene addebitato un minuto di utilizzo. Se esegui un'istanza per 3 minuti e 40 secondi, ti vengono addebitati 3 minuti e 40 secondi di utilizzo.

Arresta e avvia manualmente le istanze

Puoi interrompere e avviare le istanze supportate da Amazon EBS (istanze con dispositivi root EBS). Non puoi interrompere e avviare istanze con il dispositivo root di instance store.

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Prima di interrompere un'istanza, verifica di aver copiato tutti i dati necessari dai volumi dell'Instance Store allo storage persistente, come Amazon EBS o Amazon S3.

Console

Per arrestare e avviare un'istanza supportata da Amazon EBS

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Istanze, quindi seleziona l'istanza.
3. Nella scheda Archiviazione, verifica che il tipo di dispositivo root sia EBS. Altrimenti, non puoi fermare l'istanza.
4. Scegli Instance state (Stato istanza), Stop instance (Arresta istanza). Se questa opzione è disabilitata, l'istanza è già arrestata o il suo dispositivo root è un volume di instance store.
5. Quando viene richiesta la conferma, selezionare Stop (Arresta). Possono essere necessari alcuni minuti per arrestare l'istanza.
6. Per avviare l'istanza arrestata, seleziona l'istanza e scegli Stato istanza, Avvia istanza.

7. Possono essere necessari alcuni minuti affinché l'istanza entri nello stato `running`.
8. Se hai arrestato un'istanza supportata da Amazon EBS e questa appare "bloccata" nello stato `stopping` è possibile forzarne l'arresto. Per ulteriori informazioni, consulta Risoluzione dei problemi di arresto dell'istanza.

Command line

Prerequisiti

Verifica che il dispositivo principale dell'istanza sia un volume EBS. Ad esempio, esegui il AWS CLI comando describe-instances e verifica che non sia così. `RootDeviceType ebs instance-store`

Per arrestare e avviare un'istanza supportata da Amazon EBS

Utilizzare uno dei seguenti comandi:

- AWS CLI—stop-instances e start-instances.
- AWS Tools for PowerShell— e. Stop-EC2InstanceStart-EC2Instance
- Comandi del sistema operativo: è possibile avviare l'arresto utilizzando i comandi shutdown o poweroff. Quando si utilizza un comando del sistema operativo, l'istanza si interrompe per impostazione predefinita. Puoi modificare questo comportamento in modo che l'istanza venga terminata anziché arrestata. Per ulteriori informazioni, consulta Modifica del comportamento di arresto avviato dall'istanza.

[Istanze Linux] L'utilizzo del halt comando del sistema operativo da un'istanza non avvia uno spegnimento. Se si utilizza il comando halt, l'istanza non termina, ma metterà la CPU in stato `HLT`, che sospende il funzionamento della CPU. L'istanza rimane in esecuzione.

Arrestare e avviare automaticamente le istanze

Puoi automatizzare l'arresto e l'avvio delle istanze con i seguenti servizi:

Instance Scheduler attivo AWS

Puoi utilizzare Instance Scheduler on AWS per automatizzare l'avvio e l'arresto delle istanze EC2. Per ulteriori informazioni, consulta Come posso utilizzare Instance Scheduler con per pianificare le istanze EC2? CloudFormation Si noti che sono previsti costi aggiuntivi.

AWS Lambda e una EventBridge regola Amazon

Puoi utilizzare Lambda e una EventBridge regola per interrompere e avviare le istanze in base a una pianificazione. Per ulteriori informazioni, consulta Come si usa Lambda per arrestare e avviare le istanze Amazon EC2 a intervalli regolari?

Amazon EC2 Auto Scaling

Per assicurarti di disporre del numero corretto di istanze Amazon EC2 disponibili per gestire il carico di un'applicazione, crea gruppi con dimensionamento automatico. Amazon EC2 Auto Scaling garantisce che l'applicazione abbia sempre la capacità giusta per gestire la domanda di traffico e consente di risparmiare sui costi avviando le istanze solo quando sono necessarie. Tieni presente che Amazon EC2 Auto Scaling termina, anziché arrestare, le istanze non necessarie. Per configurare i gruppi con dimensionamento automatico, consulta Nozioni di base su Amazon EC2 Auto Scaling.

Trova tutte le istanze in esecuzione e interrotte

Puoi trovare tutte le istanze in esecuzione e interrotte in un'unica pagina utilizzando Amazon EC2 Global View. Regioni AWS Questa funzionalità è particolarmente utile per fare l'inventario e trovare istanze dimenticate. Per informazioni su come usare Global View, consulta Amazon EC2 Global View.

Abilita la protezione dallo stop per la tua istanza

Se desideri che un'istanza non venga arrestata per errore, puoi abilitare la funzionalità di protezione da arresto per tale istanza. La protezione da arresto protegge la tua istanza anche dalla chiusura accidentale.

L'`DisableApiStop`attributo dell'`ModifyInstanceAttribute`API Amazon EC2 controlla se l'istanza può essere interrotta utilizzando la console Amazon EC2, l'API Amazon EC2 o AWS CLI l'API Amazon EC2. Puoi impostare il valore di questo attributo quando avvii l'istanza, mentre l'istanza è in esecuzione oppure mentre l'istanza è arrestata.

Considerazioni

- L'attivazione della protezione da arresto non impedisce di arrestare un'istanza accidentalmente avviando un arresto dall'istanza stessa utilizzando un comando del sistema operativo come shutdown o poweroff.

- L'attivazione della protezione da arresto non AWS impedisce di arrestare l'istanza quando è in corso un evento pianificato per arrestarla.
- L'attivazione della protezione da arresto non impedisce al Dimensionamento automatico Amazon EC2 di terminare un'istanza quando l'istanza non è integra o durante eventi di riduzione orizzontale. Puoi controllare se un gruppo con scalabilità automatica può terminare una determinata istanza durante la riduzione utilizzando la protezione per la riduzione delle istanze.
- La protezione Stop non solo impedisce l'arresto accidentale dell'istanza, ma anche la chiusura accidentale quando si utilizza la console o l'API AWS CLI. Tuttavia, non imposta automaticamente l'attributo `DisableApiTermination`. Tieni presente che quando l'`DisableApiStop`attributo è impostato su`false`, l'impostazione dell'`DisableApiTermination`attributo determina se l'istanza può essere terminata utilizzando la console o l'API AWS CLI. Per ulteriori informazioni, consulta Termina le istanze Amazon EC2.
- Non è possibile abilitare la protezione da arresto per le istanze supportate da un archivio dell'istanza.
- Non è possibile abilitare la protezione da arresto per istanze spot.
- L'API Amazon EC2 segue un modello di consistenza eventuale quando abiliti o disabiliti la protezione da arresto. Ciò significa che il risultato dell'esecuzione dei comandi per impostare l'attributo Protezione da arresto potrebbe non essere immediatamente visibile a tutti i comandi successivi eseguiti. Per ulteriori informazioni, consulta Eventual consistency nella Amazon EC2 Developer Guide.

Attività della protezione da arresto

- Abilitazione della protezione da arresto per un'istanza all'avvio
- Abilitazione della protezione da arresto per un'istanza in esecuzione o arrestata
- Disabilitazione della protezione da arresto per un'istanza in esecuzione o arrestata

Abilitazione della protezione da arresto per un'istanza all'avvio

Puoi abilitare la protezione da arresto per un'istanza al suo avvio utilizzando uno dei metodi descritti di seguito.

Console

Come abilitare la protezione da arresto per un'istanza all'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel pannello di controllo scegliere Avvia istanza.
3. Configura l'istanza tramite la nuova procedura guidata di avvio dell'istanza.
4. Nella procedura guidata, abilita la protezione da arresto scegliendo Abilita per Protezione da arresto in Dettagli avanzati.

AWS CLI

Come abilitare la protezione da arresto per un'istanza all'avvio

Usa il AWS CLI comando run-instances per avviare l'istanza e specifica il parametro. `disable-api-stop`

```
aws ec2 run-instances \
    --image-id ami-a1b2c3d4e5example \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --disable-api-stop \
    ...
```

Abilitazione della protezione da arresto per un'istanza in esecuzione o arrestata

Puoi abilitare la protezione da arresto per un'istanza in esecuzione o arrestata utilizzando uno dei metodi descritti di seguito.

Console

Per abilitare la protezione da arresto per un'istanza in esecuzione o arrestata

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegliere Instances (Istanze).
3. Seleziona l'istanza, quindi scegli Operazioni > Impostazioni dell'istanza > Modifica protezione da arresto.
4. Seleziona la casella di controllo Enable (Abilita), quindi scegli Save (Salva).

AWS CLI

Per abilitare la protezione da arresto per un'istanza in esecuzione o arrestata

Utilizzate il modify-instance-attribute AWS CLI comando e specificate il parametro. `disable-api-stop`

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

Disabilitazione della protezione da arresto per un'istanza in esecuzione o arrestata

Puoi disabilitare la protezione da arresto per un'istanza in esecuzione o arrestata utilizzando uno dei metodi descritti di seguito.

Console

Per disabilitare la protezione da arresto per un'istanza in esecuzione o arrestata

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegliere Instances (Istanze).
3. Seleziona l'istanza, quindi scegli Actions (Operazioni), Instance settings (Impostazioni dell'istanza) e Change stop protection (Modifica protezione da arresto).
4. Deseleziona la casella di controllo Enable (Abilita), quindi scegli Save (Salva).

AWS CLI

Per disabilitare la protezione da arresto per un'istanza in esecuzione o arrestata

Utilizzate il modify-instance-attribute AWS CLI comando e specificate il `no-disable-api-stop` parametro.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-stop
```

Metti in ibernazione la tua istanza Amazon EC2

Quando ibernate un'istanza, Amazon EC2 segnala al sistema operativo di eseguire l'ibernazione (). suspend-to-disk L'ibernazione salva il contenuto della memoria dell'istanza (RAM) nel volume di

root di Amazon Elastic Block Store (Amazon EBS). Amazon EC2 rende persistente il volume di root dell'istanza EBS ed eventuali volumi di dati EBS collegati. Quando l'istanza viene avviata:

- Il volume root EBS viene ripristinato allo stato precedente
- I contenuti RAM vengono ricaricati
- I processi precedentemente in esecuzione vengono ripresi
- I volumi di dati precedentemente collegati vengono collegati nuovamente e l'istanza conserva il proprio ID

Puoi ibernare un'istanza solo se è abilitata per l'ibernazione e soddisfa i prerequisiti di ibernazione.

Se un'istanza o un'applicazione impiega molto tempo per eseguire il bootstrap e creare un footprint di memoria per diventare pienamente produttiva, puoi utilizzare l'ibernazione per inizializzare l'istanza. Per inizializzare l'istanza, è necessario:

1. Avviarla con l'ibernazione abilitata.
2. Portarla nello stato desiderato.
3. Puoi ibernarla in modo che sia pronta per essere ripresa nello stato desiderato quando necessario.

Non sono previsti addebiti per l'utilizzo di un'istanza ibernata, finché questa si trova nello stato `stopped`, né per il trasferimento dei dati, se il contenuto della RAM viene trasferito al volume root EBS. È previsto l'addebito per l'archiviazione di tutti i volumi EBS, compresa l'archiviazione dei contenuti RAM.

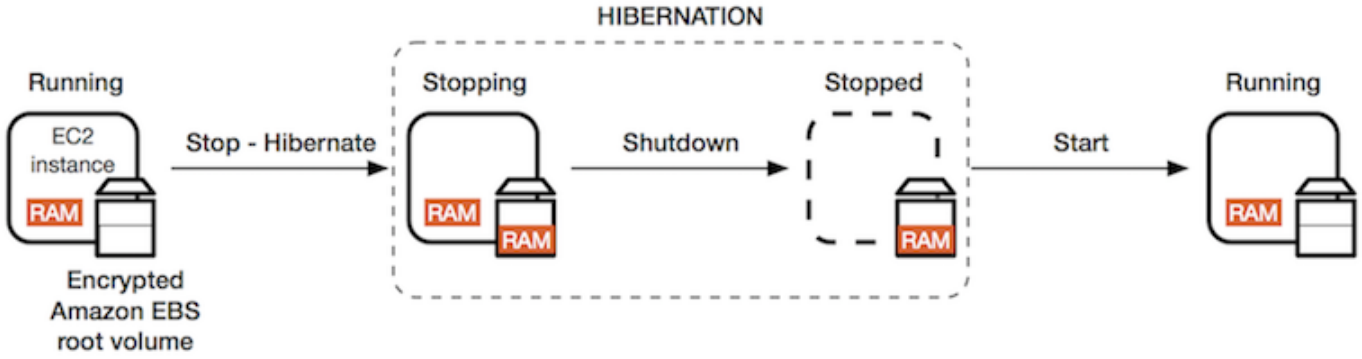
Se non hai più bisogno di un'istanza, puoi terminarla in qualsiasi momento, anche quando si trova nello stato `stopped` (ibernata). Per ulteriori informazioni, consulta Termina le istanze Amazon EC2.

Indice

- Risoluzione dei problemi di ibernazione delle istanze Amazon EC2

Come funziona l'ibernazione delle istanze Amazon EC2

Il diagramma seguente mostra una panoramica di base del processo di ibernazione per le istanze EC2.



Cosa succede quando ibernate un'istanza

Quando ibernate un'istanza, accade quanto segue:

- L'istanza passa allo stato `stopping`. Amazon EC2 segnala al sistema operativo di eseguire l'ibernazione (). suspend-to-disk L'ibernazione blocca tutti i processi, salva il contenuto della memoria RAM nel volume root EBS, quindi esegue la normale chiusura del sistema.
- Una volta completata la chiusura, l'istanza passa allo stato `stopped`.
- Tutti i volumi EBS restano collegati all'istanza e i rispettivi dati vengono conservati, incluso il contenuto salvato della RAM.
- Tutti i volumi di instance store Amazon EC2 rimangono collegati all'istanza, ma i dati sui volumi di instance store vengono persi.
- Quando lo stato dell'istanza è `stopped`, puoi modificare determinati attributi dell'istanza, compreso il tipo o la dimensione dell'istanza.
- Nella maggior parte dei casi, all'avvio l'istanza migra su un nuovo computer host sottostante. Questo è anche quello che accade quando si arresta e avvia un'istanza.
- Quando l'istanza viene avviata, il sistema operativo legge il contenuto della RAM dal volume root EBS prima di sbloccare i processi per riprendere il proprio stato.
- L'istanza mantiene i suoi indirizzi IPv4 privati e tutti gli indirizzi IPv6. Quando l'istanza viene avviata, l'istanza continua a mantenere i relativi indirizzi IPv4 privati e gli eventuali indirizzi IPv6.

- Amazon EC2 rilascia l'indirizzo IPv4 pubblico. Quando l'istanza viene avviata, Amazon EC2 le assegna un nuovo indirizzo IPv4 pubblico.
- L'istanza mantiene gli indirizzi IP elastici associati. Ti verranno addebitati gli indirizzi IP elastici associati a un'istanza ibernata.

Per ulteriori informazioni sulla differenza tra ibernare e riavviare, arrestare o terminare un'istanza, consulta Differenze tra riavvio, arresto, ibernazione e interruzione.

Limitazioni

- Quando iberni un'istanza, i dati presenti sui volumi dell'instance store vengono persi.
- (Istanze Linux) Non è possibile ibernare un'istanza Linux con più di 150 GB di RAM.
- (Istanze Windows) Non è possibile ibernare un'istanza Windows con più di 16 GB di RAM.
- Se si crea uno snapshot o un'AMI da un'istanza che è ibernata o ha attivato la modalità di ibernazione, potrebbe non essere possibile connettersi a una nuova istanza avviata dall'AMI o da un'AMI creata da uno snapshot.
- (Solo istanze spot) Se l'istanza spot viene messa in ibernazione da Amazon EC2, solo Amazon EC2 può riprenderla. Se l'istanza spot viene messa in ibernazione da te (ibernazione avviata dall'utente), puoi riprendere l'istanza in autonomia. Un'istanza spot ibernata può essere ripresa solo se la capacità è disponibile e il prezzo spot è inferiore o uguale al prezzo massimo specificato.
- Non è possibile ibernare un'istanza che si trova in un gruppo Auto Scaling o viene utilizzata da Amazon ECS. Se l'istanza si trova in un gruppo Auto Scaling e si prova a ibernarla, il servizio Amazon EC2 Auto Scaling contrassegna l'istanza arrestata come non integra, pertanto potrebbe terminarla e avviare un'istanza sostitutiva. Per ulteriori informazioni, consulta Health checks for instances in an Auto Scaling group nella Amazon EC2 Auto Scaling User Guide.
- Non è possibile ibernare un'istanza configurata per l'avvio in modalità UEFI con UEFI Secure Boot abilitato.
- Se si iberna un'istanza che è stata lanciata in un Prenotazione di capacità, il Prenotazione di capacità non garantisce che l'istanza ibernata possa riprendere dopo aver provato ad avviarla.
- Non è possibile ibernare un'istanza che utilizza un kernel inferiore a 5.10 se è abilitata la modalità FIPS (Federal Information Processing Standard).
- Non è possibile mantenere un'istanza ibernata per più di 60 giorni. Per prolungare il periodo di ibernazione oltre i 60 giorni, è necessario avviare l'istanza ibernata, arrestarla e avviarla.
- Aggiorniamo costantemente la nostra piattaforma con upgrade e patch di sicurezza che possono entrare in conflitto con le istanze ibernate. Ti avvisiamo in caso di aggiornamenti critici che

richiedono un avvio per le istanze ibernate per potere eseguire la chiusura o il riavvio per applicare gli upgrade e le patch di sicurezza necessari.

Considerazioni sull'ibernazione di un'istanza spot

- Se l'istanza spot viene messa in ibernazione da te, puoi riavviarla a condizione che la capacità sia disponibile e il prezzo spot sia inferiore o uguale al prezzo massimo specificato.
- Se Amazon EC2 mette in ibernazione l'istanza spot:
  - Solo Amazon EC2 può riprendere l'istanza.
  - Amazon EC2 riprende l'istanza spot ibernata quando la capacità diventa disponibile con un prezzo spot pari o inferiore al prezzo massimo specificato.
  - Due minuti prima che Amazon EC2 metta in ibernazione l'istanza spot, riceverai un avviso di interruzione.

  Per ulteriori informazioni, consulta Interruzioni dell'istanza spot.
- Esistono diversi modi per abilitare l'ibernazione per un'istanza spot. Per ulteriori informazioni, consulta Specificare il comportamento di interruzione.

Prerequisiti per l'ibernazione delle istanze Amazon EC2

Puoi abilitare il supporto per l'ibernazione per un'istanza On-Demand o un'istanza Spot al momento del lancio. Non è possibile abilitare l'ibernazione su un'istanza esistente, indipendentemente dal fatto che sia in esecuzione o interrotta. Per ulteriori informazioni, consulta Abilita l'ibernazione dell'istanza.

Requisiti per ibernare un'istanza

- Regioni AWS
- AMI
- Famiglie di istanze
- Dimensioni RAM dell'istanza
- Tipo di volume root
- Dimensione del volume principale
- Crittografia del volume principale
- Tipi di volume EBS
- Richieste di istanza spot

Regioni AWS

È possibile utilizzare l'ibernazione con tutte le istanze. Regioni AWS

AMI

È necessario utilizzare un'AMI HVM che supporti l'ibernazione. Le seguenti AMI supportano l'ibernazione:

AMI Linux

- AMI AL2023 rilasciata il 20.09.2023 o successivamente
- AMI Amazon Linux 2 rilasciata il 29.08.2019 o successivamente
- AMI Amazon Linux 2018.03 rilasciata il 16.11.2018 o successivamente
- AMI CentOS versione 8[1] (la configurazione aggiuntiva è obbligatoria)
- AMI Fedora versione 34 o successiva[1] (la configurazione aggiuntiva è obbligatoria)
- AMI Red Hat Enterprise Linux (RHEL) 9[1] (la configurazione aggiuntiva è obbligatoria)
- AMI Red Hat Enterprise Linux (RHEL) 8[1] (la configurazione aggiuntiva è obbligatoria)
- AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish) rilasciata con numero di serie 20230303 o successivo [2]
- AMI Ubuntu 20.04 LTS (Focal Fossa) AMI rilasciata con numero di serie 20210820 o successivo[2]
- AMI Ubuntu 18.04 LTS (Bionic Beaver) AMI rilasciata con numero di serie 20190722.1 o successivo [2] [4]
- AMI Ubuntu 16.04 LTS (Xenial Xerus) AMI [2] [3] [4] (la configurazione aggiuntiva è obbligatoria)

[1] Per CentOS, Fedora e Red Hat Enterprise Linux, l'ibernazione è supportata solo su istanze basate su Nitro.

[2] Suggeriamo di disabilitare KASLR sulle istanze con 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver) e Ubuntu 16.04 LTS (Xenial Xerus). Per ulteriori informazioni, consulta Disabilitazione di KASLR su un'istanza (solo Ubuntu).

[3] Per Ubuntu 16.04 LTS - (Xenial Xerus) AMI, l'ibernazione non è supportata su tipi di istanza `t3.nano`. Nessuna patch sarà resa disponibile perché Ubuntu (Xenial Xerus) ha terminato il supporto nell'aprile 2021. Per utilizzare i tipi di istanza `t3.nano`, consigliamo di eseguire l'aggiornamento alle AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa) ooppure Ubuntu 18.04 LTS (Bionic Beaver).

[4] Il supporto per Ubuntu 18.04 LTS (Bionic Beaver) e Ubuntu 16.04 LTS (Xenial Xerus) ha raggiunto la fine del ciclo di vita.

Per configurare la tua AMI per il supporto dell'ibernazione, consulta Configurare un'AMI Linux per supportare l'ibernazione.

Il supporto per altre versioni di Ubuntu e altri sistemi operativi sarà disponibile a breve.

AMI Windows

- AMI Windows Server 2022 rilasciata il 13.09.2023 o successivamente
- AMI Windows Server 2019 rilasciata il 11.09.2019 o successivamente
- AMI Windows Server 2016 rilasciata il 11.09.2019 o successivamente
- AMI Windows Server 2012 R2 rilasciata il 11.09.2019 o successivamente
- AMI Windows Server 2012 rilasciata il 11.09.2019 o successivamente

Famiglie di istanze

È necessario utilizzare una famiglia di istanze che supporti l'ibernazione.

- Uso generale: M3, M4, M5, M5a, M5ad, M5d, M6i, M6iD, M7i, M7i-Flex, T2, T3, T3a
- Elaborazione ottimizzata: C3, C4, C5, C5d, C6i, C6iD, C7a, C7i, C7i-Flex
- Memoria ottimizzata: R3, R4, R5, R5a, R5ad, R5d, R7a, R7i, R7iz
- Archiviazione ottimizzata: I3, I3en

Istanze Nitro: le istanze bare metal non sono supportate.

Per visualizzare i tipi di istanza disponibili che supportano l'ibernazione in una Regione specifica

I tipi di istanza disponibili variano in base alla regione. Per visualizzare i tipi di istanza disponibili che supportano l'ibernazione in una regione, utilizzate il comando con il parametro. describe-instance-types`--region` Includere il parametro `--filters` per assegnare i risultati ai tipi di istanza che supportano l'ibernazione e il parametro `--query` per assegnare l'output al valore di `InstanceType`.

```
aws ec2 describe-instance-types --filters Name=hibernation-supported,Values=true --
query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Output di esempio

```
c3.2xlarge
c3.4xlarge
c3.8xlarge
c3.large
c3.xlarge
c4.2xlarge
c4.4xlarge
c4.8xlarge
...
```

Dimensioni RAM dell'istanza

Istanze Linux: devono pesare meno di 150 GB.

Istanze Windows: possono contenere fino a 16 GB. Per ibernare un'istanza Windows T3 o T3a, consigliamo almeno 1 GB di RAM.

Tipo di volume root

Il volume root deve essere un volume EBS e non un volume instance store.

Dimensione del volume principale

Il volume root deve essere sufficientemente grande da memorizzare il contenuto della RAM e consentire l'utilizzo previsto, ad esempio il sistema operativo o le applicazioni. Se abiliti l'ibernazione, lo spazio viene allocato sul volume root al lancio per archiviare la RAM.

Crittografia del volume principale

Il volume root deve essere crittografato per garantire la protezione dei contenuti sensibili presenti in memoria al momento dell'ibernazione. Quando vengono spostati al volume root EBS, i dati della RAM sono sempre crittografati. La crittografia del volume root viene applicata al lancio dell'istanza.

Utilizzare una delle tre opzioni seguenti per garantire che il volume root sia un volume EBS crittografato:

- Crittografia EBS predefinita: puoi abilitare la crittografia EBS per impostazione predefinita per garantire che tutti i nuovi volumi EBS creati nell'account AWS siano crittografati. In questo modo è possibile abilitare l'ibernazione per le istanze senza specificare l'intento di crittografia all'avvio delle istanze. Per ulteriori informazioni, consulta Abilitare la crittografia per impostazione predefinita.

- Crittografia a "fase singola" EBS: puoi avviare le stanze EC2 supportate da EBS e crittografate da un'AMI non crittografata e abilitarne al contempo l'ibernazione. Per ulteriori informazioni, consulta Utilizzo della crittografia con le AMI EBS-backed.
- AMI crittografata: puoi abilitare la crittografia EBS utilizzando un'AMI crittografata per avviare l'istanza. Se l'AMI non dispone di una snapshot root crittografata, è possibile copiarla in una nuova AMI e richiederne la crittografia. Per ulteriori informazioni, consulta Crittografia di un'immagine non crittografata durante la copia e Copiare un'AMI.

Tipi di volume EBS

I volumi EBS devono utilizzare uno dei seguenti tipi di volume EBS:

- Scopo generico (SSD) (`gp2` e `gp3`)
- IOPS con provisioning (SSD) (`io1` e `io2`)

Se scegli un tipo di volume SSD IOPS con provisioning, per ottenere prestazioni ottimali per l'ibernazione devi eseguire il provisioning del volume EBS con l'IOPS appropriato. Per ulteriori informazioni, consulta i tipi di volume di Amazon EBS nella Guida per l'utente di Amazon EBS.

Richieste di istanza spot

Per le istanze Spot, si applicano i seguenti requisiti:

- Il tipo di richiesta di istanza spot deve essere `persistent`.
- Non è possibile specificare un gruppo di avvio nella richiesta di istanza spot.

Configurare un'AMI Linux per supportare l'ibernazione

Le seguenti AMI Linux supportano l'ibernazione, ma per ibernare un'istanza lanciata con una di queste AMI, è necessaria una configurazione aggiuntiva prima di poter ibernare l'istanza.

Una configurazione aggiuntiva è richiesta per:

- AMI Amazon Linux 2 versione minima rilasciata il 29/08/2019 o successivamente
- Amazon Linux 2 rilasciato prima del 29.08.2019
- Amazon Linux rilasciato prima del 16.11.2018
- CentOS versione 8 o successiva
- Fedora versione 34 o successive

- Red Hat Enterprise Linux versione 8 o 9
- Ubuntu 20.04 LTS (Focal Fossa) rilasciata prima del numero di serie 20210820
- Ubuntu 18.04 (Bionic Beaver) rilasciata prima del numero seriale 20190722.1
- Ubuntu 16.04 (Xenial Xerus)

Per ulteriori informazioni, consulta Update instance software on your Amazon Linux 2.

Nessuna configurazione aggiuntiva è richiesta per le AMI seguenti perché sono già configurate per supportare l'ibernazione:

- AMI AL2023 rilasciata il 20.09.2023 o successivamente
- AMI Amazon Linux 2 versione completa rilasciata il 29/08/2019 o successivamente
- AMI Amazon Linux 2018.03 rilasciata il 16.11.2018 o successivamente
- AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish) rilasciata con numero di serie 20230303 o successivo
- Ubuntu 20.04 LTS (Focal Fossa) AMI rilasciata con numero di serie 20210820 o successivo
- Ubuntu 18.04 LTS (Bionic Beaver) AMI rilasciata con numero seriale 20190722.1 o successivo

AMI Amazon Linux 2 versione minima rilasciata il 29/08/2019 o successivamente

Per configurare un'AMI Amazon Linux 2 versione minima rilasciata il 29/08/2019 o successivamente per il supporto dell'ibernazione

1. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Riavvia il servizio .

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Amazon Linux 2 rilasciato prima del 29.08.2019

Per configurare un'AMI Amazon Linux 2 rilasciata prima del 29.08.2019 per il supporto dell'ibernazione

1. Aggiornare il kernel a `4.14.138-114.102` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

4. Verificare che il kernel sia aggiornato alla versione `4.14.138-114.102` o successiva.

```
[ec2-user ~]$ uname -a
```

5. Arrestare l'istanza e creare un'AMI. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.

Amazon Linux rilasciato prima del 16.11.2018

Per configurare un'AMI Amazon Linux rilasciata prima del 16.11.2018 per il supporto dell'ibernazione

1. Aggiornare il kernel a `4.14.77-70.59` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

4. Verificare che il kernel sia aggiornato alla versione `4.14.77-70.59` o successiva.

```
[ec2-user ~]$ uname -a
```

5. Arrestare l'istanza e creare un'AMI. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.

CentOS versione 8 o successiva

Per configurare un'AMI CentOS versione 8 o successiva per il supporto dell'ibernazione

1. Aggiornare il kernel a `4.18.0-305.7.1.el8_4.x86_64` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il repository EPEL (Extra Packages for Enterprise Linux) Fedora.

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Attivare l'agente di ibernazione perché venga lanciato all'avvio.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

6. Verificare che il kernel sia aggiornato alla versione `4.18.0-305.7.1.el8_4.x86_64` o successiva.

```
[ec2-user ~]$ uname -a
```

Fedora versione 34 o successive

Per configurare un'AMI Fedora versione 34 o successiva per il supporto dell'ibernazione

1. Aggiornare il kernel a `5.12.10-300.fc34.x86_64` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Attivare l'agente di ibernazione perché venga lanciato all'avvio.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

5. Verificare che il kernel sia aggiornato alla versione `5.12.10-300.fc34.x86_64` o successiva.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux versione 8 o 9

Per configurare un'AMI Red Hat Enterprise Linux 8 o 9 per supportare l'ibernazione

1. Aggiornare il kernel a `4.18.0-305.7.1.el8_4.x86_64` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il repository EPEL (Extra Packages for Enterprise Linux) Fedora.

   Versione 8 RHEL:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   Versione 9 RHEL:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

3. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Attivare l'agente di ibernazione perché venga lanciato all'avvio.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

6. Verificare che il kernel sia aggiornato alla versione `4.18.0-305.7.1.el8_4.x86_64` o successiva.

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 LTS (Focal Fossa) rilasciata prima del numero di serie 20210820

Configurazione di un Ubuntu 20.04 LTS (Focal Fossa) AMI rilasciata prima del numero di serie 20210820 a supporto dell'ibernazione

1. Aggiorna il linux-aws-kernel file alla versione precedente `5.8.0-1038.40` o successiva e grub2 alla `2.04-1ubuntu26.13` versione successiva.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

3. Verificare che il kernel sia aggiornato alla versione `5.8.0-1038.40` o successiva.

```
[ec2-user ~]$ uname -a
```

4. Confermare che la versione grub2 sia aggiornata alla versione `2.04-1ubuntu26.13` o successiva.

```
[ec2-user ~]$ dpkg --list | grep grub2-common
```

Ubuntu 18.04 (Bionic Beaver) rilasciata prima del numero seriale 20190722.1

Per configurare un'AMI Ubuntu 18.04 LTS rilasciata prima del numero seriale 20190722.1 per il supporto dell'ibernazione

1. Aggiornare il kernel a `4.15.0-1044` o versione successiva.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

4. Verificare che il kernel sia aggiornato alla versione `4.15.0-1044` o successiva.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xerus)

Per configurare Ubuntu 16.04 LTS in modo che supporti l'ibernazione, è necessario installare il pacchetto linux-aws-hwe kernel versione 4.15.0-1058-aws o successiva e l'agente ec2-hibinit-agent.

> **Important**
>
> Il pacchetto kernel `linux-aws-hwe` è supportato da Canonical. Il supporto standard per Ubuntu 16.04 LTS è terminato nell'aprile 2021 e il pacchetto non riceve più aggiornamenti regolari. Tuttavia, riceverà ulteriori aggiornamenti della sicurezza fino al termine del supporto per la manutenzione estesa della sicurezza nel 2024. Per ulteriori informazioni, consulta Amazon EC2 Hibernation per Ubuntu 16.04 LTS ora disponibile sul blog Canonical Ubuntu. Ti consigliamo di eseguire l'aggiornamento a Ubuntu 20.04 LTS (Focal Fossa) AMI o Ubuntu 18.04 LTS (Bionic Beaver) AMI.

Per configurare un'AMI Ubuntu 16.04 LTS e supportare l'ibernazione

1. Aggiornare il kernel a `4.15.0-1058-aws` o versione successiva.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

4. Verificare che il kernel sia aggiornato alla versione `4.15.0-1058-aws` o successiva.

```
[ec2-user ~]$ uname -a
```

Abilita l'ibernazione per un'istanza Amazon EC2

Per ibernare un'istanza, devi prima abilitarla per l'ibernazione durante l'avvio dell'istanza.

> **Important**
>
> Non è possibile abilitare o disabilitare l'ibernazione di un'istanza dopo averla avviata.

Argomenti

- Abilitazione dell'ibernazione per le istanze on demand
- Abilitazione dell'ibernazione per le istanze spot
- Verificare se un'istanza è abilitata per l'ibernazione

Abilitazione dell'ibernazione per le istanze on demand

Utilizza uno dei seguenti metodi per abilitare l'ibernazione per le istanze on demand.

New console

Abilitazione dell'ibernazione per un'istanza on demand

1. Segui la procedura per l'avvio di un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per abilitare l'ibernazione.
2. Per abilitare l'ibernazione, configura i seguenti campi nella procedura guidata di avvio dell'istanza:

   a. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), seleziona un'AMI che supporta l'ibernazione. Per ulteriori informazioni, consulta AMI.

   b. In Instance type (Tipo di istanza), seleziona un tipo di istanza supportato. Per ulteriori informazioni, consulta Famiglie di istanze.

   c. In Configure storage (Configura lo storage), scegli Advanced (Avanzate) a destra e specifica le informazioni seguenti per il volume root:

      - Per Dimensione (GiB), immettere la dimensione del volume EBS principale. Il volume deve essere sufficientemente grande per memorizzare il contenuto della RAM e soddisfare l'utilizzo previsto.
      - Per Volume Type (Tipo di volume), seleziona un tipo di volume EBS supportato: SSD per scopo generico (`gp2` e `gp3`) o SSD con capacità di IOPS allocata (`io1` e `io2`).
      - Per Encrypted (Crittografato), scegli Yes (Sì). Se la crittografia è stata abilitata per impostazione predefinita in questa AWS regione, è selezionata l'opzione Sì.
      - Per KMS key (Chiave KMS), seleziona la chiave di crittografia per il volume. Se è stata abilitata la crittografia per impostazione predefinita in questa AWS regione, viene selezionata la chiave di crittografia predefinita.

      Per ulteriori informazioni sui prerequisiti per il volume radice, consulta Prerequisiti per l'ibernazione delle istanze Amazon EC2.

   d. Espandi Advanced details (Dettagli avanzati) e in Stop - Hibernate behavior (Comportamento di arresto/ibernazione) scegli Enable (Abilita).

3. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Old console

Abilitazione dell'ibernazione per un'istanza on demand

1. Seguire la procedura Avvio di un'istanza tramite la vecchia procedura guidata di avvio.
2. Nella pagina Choose an Amazon Machine Image (AMI) (Scegli Amazon Machine Image [AMI]) selezionare un'AMI che supporti l'ibernazione. Per ulteriori informazioni sulle AMI supportate, consulta Prerequisiti per l'ibernazione delle istanze Amazon EC2.
3. Nella pagina Choose an Instance Type (Scegli il tipo di istanza) selezionare un tipo di istanza supportato e scegliere Next: Configure Instance Details (Successivo: Configura i dettagli dell'istanza). Per ulteriori informazioni sui tipi di istanza supportati, consulta Prerequisiti per l'ibernazione delle istanze Amazon EC2.
4. Nella pagina Configure Instance Details (Configurazione dettagli istanza), per Stop - Hibernate Behavior (Comportamento di interruzione/ibernazione), selezionare la casella di controllo Enable hibernation as an additional stop behavior (Abilita ibernazione come comportamento di arresto aggiuntivo).
5. Nella pagina Add storage (Aggiungi archiviazione) per il volume root, specificare le informazioni seguenti:

   - Per Dimensione (GiB), immettere la dimensione del volume EBS principale. Il volume deve essere sufficientemente grande per memorizzare il contenuto della RAM e soddisfare l'utilizzo previsto.
   - Per Tipo di volume, selezionare un tipo di volume EBS supportato (SSD per uso generale (`gp2` e `gp3`) o SSD con capacità di IOPS allocata (`io1` e `io2`).
   - Per Crittografia, selezionare la chiave di crittografia per il volume. Se la crittografia è abilitata per impostazione predefinita in questa AWS regione, viene selezionata la chiave di crittografia predefinita.

   Per ulteriori informazioni sui prerequisiti per il volume radice, consulta Prerequisiti per l'ibernazione delle istanze Amazon EC2.
6. Continuare come richiesto dalla procedura guidata. Dopo avere esaminato le opzioni nella pagina Rivedere l'avvio dell'istanza, scegliere Launch (Avvia). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la vecchia procedura guidata di avvio.

AWS CLI

Abilitazione dell'ibernazione per un'istanza on demand

Utilizzare il comando run-instances per avviare un'istanza. Specificare i parametri del volume principale EBS utilizzando il parametro `--block-device-mappings file://mapping.json` e abilitare l'ibernazione utilizzando il parametro `--hibernation-options Configured=true`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

Specifica quanto segue nel file `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> Il valore per `DeviceName` deve corrispondere al nome del dispositivo root associato all'AMI. Per trovare il nome del dispositivo root, utilizza il comando describe-images.
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```
>
> Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, puoi ometterla`"Encrypted": true`.

PowerShell

Per abilitare l'ibernazione per un'istanza On-Demand utilizzando il AWS Tools for Windows PowerShell

Utilizzate il New-EC2Instancecomando per avviare un'istanza. Specificare il volume principale EBS definendo innanzitutto la mappatura dei dispositivi a blocchi e quindi aggiungendolo al comando mediante il parametro `-BlockDeviceMappings`. Abilitare l'ibernazione utilizzando il parametro `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
            -ImageId ami-0abcdef1234567890 `
            -InstanceType m5.large `
            -BlockDeviceMappings $ebs_encrypt `
            -HibernationOptions_Configured $true `
            -MinCount 1 `
            -MaxCount 1 `
            -KeyName MyKeyPair
```

> **Note**
>
> Il valore per `DeviceName` deve corrispondere al nome del dispositivo radice associato all'AMI. Per trovare il nome del dispositivo root, usa il Get-EC2Imagecomando.
>
> ```
> Get-EC2Image -ImageId ami-0abcdef1234567890
> ```
>
> Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, puoi omettere la `Encrypted = $true` mappatura dei dispositivi a blocchi.

Abilitazione dell'ibernazione per le istanze spot

Utilizza uno dei seguenti metodi per abilitare l'ibernazione per le istanze spot. Per informazioni su come ibernare un'istanza spot in fase di interruzione, consulta la pagina Interruzioni dell'istanza spot.

Console

È possibile utilizzare la procedura guidata di avvio dell'istanza nella console Amazon EC2 per abilitare l'ibernazione per un'istanza spot.

Abilitazione dell'ibernazione per un'istanza spot

1. Segui la procedura per richiedere un'istanza spot utilizzando la procedura guidata di avvio di un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per abilitare l'ibernazione.
2. Per abilitare l'ibernazione, configura i seguenti campi nella procedura guidata di avvio dell'istanza:

   a. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), seleziona un'AMI che supporta l'ibernazione. Per ulteriori informazioni, consulta AMI.

   b. In Instance type (Tipo di istanza), seleziona un tipo di istanza supportato. Per ulteriori informazioni, consulta Famiglie di istanze.

   c. In Configure storage (Configura lo storage), scegli Advanced (Avanzate) a destra e specifica le informazioni seguenti per il volume root:

      - Per Dimensione (GiB), immettere la dimensione del volume EBS principale. Il volume deve essere sufficientemente grande per memorizzare il contenuto della RAM e soddisfare l'utilizzo previsto.
      - Per Volume Type (Tipo di volume), seleziona un tipo di volume EBS supportato: SSD per scopo generico (`gp2` e `gp3`) o SSD con capacità di IOPS allocata (`io1` e `io2`).
      - Per Encrypted (Crittografato), scegli Yes (Sì). Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, è selezionato Sì.
      - Per KMS key (Chiave KMS), seleziona la chiave di crittografia per il volume. Se è stata abilitata la crittografia per impostazione predefinita in questa AWS regione, viene selezionata la chiave di crittografia predefinita.

      Per ulteriori informazioni sui prerequisiti per il volume radice, consulta Prerequisiti per l'ibernazione delle istanze Amazon EC2.

   d. Espandi Dettagli avanzati e, oltre ai campi per la configurazione di un'istanza spot, procedi come segue:

i. Per Tipo di richiesta, scegli Persistente.

ii. Per Comportamento di interruzione, scegli Iberna. In alternativa, per Comportamento di arresto/ibernazione, scegli Abilita. Entrambi i campi abilitano l'ibernazione sull'istanza spot. È necessario configurarne solo uno.

3. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

AWS CLI

È possibile abilitare l'ibernazione per un'istanza spot utilizzando il comando run-instances della AWS CLI .

Abilitazione dell'ibernazione per un'istanza spot tramite il parametro **`hibernation-options`**

Utilizza il comando run-instances per richiedere un'istanza spot. Specificare i parametri del volume principale EBS utilizzando il parametro `--block-device-mappings file://mapping.json` e abilitare l'ibernazione utilizzando il parametro `--hibernation-options Configured=true`. Il tipo di richiesta spot (`SpotInstanceType`) deve essere `persistent`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c4.xlarge \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
    --instance-market-options
        {
           "MarketType":"spot",
           "SpotOptions":{
              "MaxPrice":"1",
              "SpotInstanceType":"persistent"
            }
        }
```

Specifica i parametri del volume root EBS in `mapping.json` nel modo seguente.

```
[
```

```
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> Il valore per `DeviceName` deve corrispondere al nome del dispositivo root associato all'AMI. Per trovare il nome del dispositivo root, utilizza il comando describe-images.
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```
>
> Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, puoi ometterla`"Encrypted": true`.

PowerShell

Per abilitare l'ibernazione per un'istanza Spot utilizzando il AWS Tools for Windows PowerShell

Utilizza il New-EC2Instancecomando per richiedere un'istanza Spot. Specificare il volume principale EBS definendo innanzitutto la mappatura dei dispositivi a blocchi e quindi aggiungendolo al comando mediante il parametro `-BlockDeviceMappings`. Abilitare l'ibernazione utilizzando il parametro `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
            -ImageId ami-0abcdef1234567890 `
            -InstanceType m5.large `
            -BlockDeviceMappings $ebs_encrypt `
```

```
            -HibernationOptions_Configured $true `
            -MinCount 1 `
            -MaxCount 1 `
            -KeyName MyKeyPair `
            -InstanceMarketOption @(
                  MarketType = spot;
                  SpotOptions @{
                  MaxPrice = 1;
                  SpotInstanceType = persistent}
               )
```

> **Note**
>
> Il valore per `DeviceName` deve corrispondere al nome del dispositivo radice associato all'AMI. Per trovare il nome del dispositivo root, usa il Get-EC2Imagecomando.
>
> ```
> Get-EC2Image -ImageId ami-0abcdef1234567890
> ```
>
> Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, puoi omettere la `Encrypted = $true` mappatura dei dispositivi a blocchi.

Esistono diversi modi per abilitare l'ibernazione per un'istanza spot. Per ulteriori informazioni, consulta Specificare il comportamento di interruzione.

Verificare se un'istanza è abilitata per l'ibernazione

Utilizza le seguenti istruzioni per vedere se un'istanza è abilitata per l'ibernazione.

Console

Per vedere se un'istanza è abilitata per l'ibernazione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza e, nella scheda Details (Dettagli) nella sezione Instance details (Dettagli istanza) controllare Stop-hibernate behavior (Comportamento di interruzione/ibernazione). Enabled (Abilitata) indica che l'istanza è abilitata per l'ibernazione.

AWS CLI

Per vedere se un'istanza è abilitata per l'ibernazione

Utilizzare il comando describe-instances e specificare il parametro `--filters "Name=hibernation-options.configured,Values=true"` per filtrare le istanze abilitate per l'ibernazione.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

Il campo seguente nell'output indica che l'istanza è abilitata per l'ibernazione.

```
"HibernationOptions": {
    "Configured": true
}
```

PowerShell

Per vedere se un'istanza è abilitata per l'ibernazione tramite AWS Tools for Windows PowerShell

Utilizzate il Get-EC2Instancecomando e specificate il `-Filter @{ Name="hibernation-options.configured"; Value="true"}` parametro per filtrare le istanze abilitate per l'ibernazione.

```
(Get-EC2Instance -Filter @{Name="hibernation-options.configured";
 Value="true"}).Instances
```

L'output elenca le istanze EC2 abilitate per l'ibernazione.

Disabilitazione di KASLR su un'istanza (solo Ubuntu)

Per eseguire l'ibernazione su un'istanza avviata di recente con Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver) rilasciata con numero di serie 20190722.1 o versione successiva, o Ubuntu 20.04 LTS (Focal Fossa) rilasciata con numero di serie 20210820 o versione successiva, consigliamo di disabilitare KASLR (Kernel Address Space Layout Randomization). In Ubuntu 16.04 LTS o Ubuntu 18.04 LTS, o Ubuntu 20.04 LTS, KASLR è abilitato per impostazione predefinita.

KASLR è una funzionalità di sicurezza standard del kernel di Linux che consente di mitigare l'esposizione e le ramificazioni di vulnerabilità di accesso alla memoria non ancora scoperte

riproducendo in maniera casuale il valore di base dell'indirizzo del kernel. Con KASLR abilitato, c'è la possibilità che l'istanza non venga riavviata dopo l'ibernazione.

Per ulteriori informazioni su KASLR, consultare Funzionalità di Ubuntu.

Per disabilitare KASLR su un'istanza avviata con Ubuntu

1. Connettersi all'istanza tramite SSH. Per ulteriori informazioni, consulta the section called "Connessione via SSH da macOS o Linux".
2. Aprire il file `/etc/default/grub.d/50-cloudimg-settings.cfg` con un editor a scelta. Modificare la riga `GRUB_CMDLINE_LINUX_DEFAULT` per collegare l'opzione `nokaslr`, come mostrato nell'esempio seguente.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295 nokaslr"
```

3. Salvare il file e uscire dall'editor.
4. Eseguire il comando riportato di seguito per ricreare la configurazione di grub.

```
[ec2-user ~]$ sudo update-grub
```

5. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

6. Esegui il comando seguente per confermare che `nokaslr` è stato aggiunto.

```
[ec2-user ~]$ cat /proc/cmdline
```

   L'output del comando deve includere l'opzione `nokaslr`.

Ibernazione di un'istanza Amazon EC2

È possibile avviare l'ibernazione su un'istanza on demand o su un'istanza spot se l'istanza è supportata da EBS, è abilitata per l'ibernazione e soddisfa i prerequisiti di ibernazione. Se l'ibernazione di un'istanza non riesce, si verifica una normale chiusura.

Console

Ibernazione di un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona un'istanza e scegli Instance state (Stato istanza), Hibernate instance (Sospendi istanza). Se Hibernate instance (Sospendi istanza) è disabilitato, l'istanza è già sospesa o arrestata oppure non può essere sospesa. Per ulteriori informazioni, consulta Prerequisiti per l'ibernazione delle istanze Amazon EC2.
4. Quando viene richiesta la conferma scegli Hibernate (Sospendi). Possono essere necessari alcuni minuti per ibernare l'istanza. Lo stato dell'istanza diventa prima Stopping (in arresto), quindi passa a Stopped (arrestata) una volta ibernata l'istanza.

AWS CLI

Ibernazione di un'istanza supportata da EBS

Utilizzare il comando stop-instances e specificare il parametro `--hibernate`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

Per ibernare un'istanza utilizzando AWS Tools for Windows PowerShell

Utilizzate il Stop-EC2Instancecomando e specificate il `-Hibernate $true` parametro.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

Console

Per vedere se è stata avviata l'ibernazione per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e, nella scheda Dettagli, nella sezione Dettagli istanza, verifica il valore di Messaggio transizione stato.

   Cliente. UserInitiatedHibernate: L'ibernazione avviata dall'utente indica che è stata avviata l'ibernazione sull'istanza On-Demand o sull'istanza Spot.

AWS CLI

Per vedere se è stata avviata l'ibernazione per un'istanza

Utilizzare il comando describe-instances e specificare il filtro `state-reason-code` per vedere le istanze su cui è stata avviata l'ibernazione.

```
aws ec2 describe-instances \
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

Il campo seguente nell'output indica che l'ibernazione è stata avviata per l'istanza on demand o l'istanza spot.

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

Per vedere se è stata avviata l'ibernazione per un'istanza tramite AWS Tools for Windows PowerShell

Utilizza il Get-EC2Instancecomando e specifica il `state-reason-code` filtro per visualizzare le istanze in cui è stata avviata l'ibernazione.

```
Get-EC2Instance `
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

L'output elenca le istanze EC2 su cui l'ibernazione è stata avviata.

Avvia un'istanza Amazon EC2 ibernata

Avvia un'istanza ibernata avviandola come faresti con un'istanza arrestata.

> **Note**
>
> Per le istanze spot, se l'istanza è stata messa in ibernazione da Amazon EC2, solo Amazon EC2 può riprenderla. Puoi riprendere un'istanza spot ibernata solo se l'hai ibernata tu. Le istanze spot possono essere riprese solo se la capacità è disponibile e il prezzo spot è inferiore o uguale al prezzo massimo specificato.

Console

Per riavviare un'istanza ibernata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona un'istanza sospesa e scegli Instance state (Stato istanza), Start instance (Avvia istanza). Possono essere necessari alcuni minuti affinché l'istanza entri nello stato `running`. In questo periodo di tempo le verifiche dello stato mostrano l'istanza come non riuscita, fino a quando questa non viene avviata.

AWS CLI

Per riavviare un'istanza ibernata

Utilizzare il comando start-instances:

```
aws ec2 start-instances \
    --instance-ids i-1234567890abcdef0
```

PowerShell

Per avviare un'istanza ibernata utilizzando AWS Tools for Windows PowerShell

Utilizza il comando Start-EC2Instance.

```
Start-EC2Instance `
    -InstanceId i-1234567890abcdef0
```

Risoluzione dei problemi di ibernazione delle istanze Amazon EC2

Utilizza queste informazioni per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'ibernazione di un'istanza.

Problemi di ibernazione

- Non si riesce a eseguire l'ibernazione immediatamente dopo il lancio
- Il passaggio da stopping a stopped richiede troppo tempo e lo stato della memoria non viene ripristinato dopo l'avvio
- L'istanza è bloccata nello stato di arresto
- Impossibile avviare l'istanza spot subito dopo l'ibernazione
- Ripristino delle istanze spot non riuscito

Non si riesce a eseguire l'ibernazione immediatamente dopo il lancio

Se provi a ibernare un'istanza troppo presto dopo il lancio, ricevi un errore.

È necessario attendere circa due minuti per le istanze Linux e circa cinque minuti per le istanze Windows dopo l'avvio prima di andare in ibernazione.

Il passaggio da **`stopping`** a **`stopped`** richiede troppo tempo e lo stato della memoria non viene ripristinato dopo l'avvio

Se l'istanza che stai ibernando impiega troppo tempo per passare dallo stato `stopping` allo stato `stopped` e lo stato della memoria non viene ripristinato dopo l'avvio, è possibile che l'ibernazione non sia stata configurata in modo appropriato.

Istanze Linux

Verifica il log di sistema dell'istanza e cerca i messaggi correlati all'ibernazione. Per accedere al registro di sistema, connettiti all'istanza o usa il get-console-outputcomando. Trova le righe del log che iniziano con `hibinit-agent`. Se le righe del log indicano un errore o se mancano, molto probabilmente c'è stato un errore di configurazione dell'ibernazione al lancio.

Ad esempio, il messaggio seguente indica che il volume root dell'istanza non è abbastanza grande: `hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Se l'ultima riga del log registro da `hibinit-agent` è `hibinit-agent: Running: swapoff /swap`, l'ibernazione è stata configurata correttamente.

Se non vedi log relativi a questi processi, è possibile che l'AMI non supporti l'ibernazione. Per informazioni sulle AMI supportate, vedi Prerequisiti per l'ibernazione delle istanze Amazon EC2. Se hai usato la tua AMI Linux, assicurati di aver seguito le istruzioni perConfigurare un'AMI Linux per supportare l'ibernazione.

Windows Server 2016 e versioni successive

Verifica il log di avvio EC2 e cerca i messaggi correlati all'ibernazione. Per accedere al log di avvio EC2, connettersi all'istanza da configurare e aprire il file `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` in un editor di testo. Se utilizzi EC2Launch v2, apri `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Per impostazione predefinita, Windows nasconde i file e le cartelle in `C:\ProgramData`. Per visualizzare le directory e i file di avvio EC2, digitare il percorso in Windows Explorer risorse o modificare le proprietà della cartella per visualizzare i file e le cartelle nascosti.

Individuare le righe di log per l'ibernazione. Se le righe del log indicano un errore o se mancano, molto probabilmente c'è stato un errore di configurazione dell'ibernazione al lancio.

Ad esempio, il seguente messaggio indica che l'ibernazione non è stata configurata: `Message: Failed to enable hibernation.` se il messaggio di errore include valori ASCII decimali, puoi convertire i valori ASCII in testo semplice per leggere il messaggio di errore completo.

Se la riga del log contiene `HibernationEnabled: true`, l'ibernazione è stata configurata correttamente.

Windows Server 2012 R2 e versione precedente

Verifica il log di configurazione EC2 e cerca i messaggi correlati all'ibernazione. Per accedere al log di configurazione EC2, connettersi all'istanza da configurare e aprire il file `C:\Program Files`

`\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` in un editor di testo. Trovare le righe del log che iniziano con `SetHibernateOnSleep`. Se le righe del log indicano un errore o se mancano, molto probabilmente c'è stato un errore di configurazione dell'ibernazione al lancio.

Ad esempio, il messaggio seguente indica che il volume root dell'istanza non è abbastanza grande: `SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Se la riga del log è `SetHibernateOnSleep: HibernationEnabled: true`, l'ibernazione è stata configurata correttamente.

Dimensione dell'istanza di Windows

Se usi un'istanza Windows T3 o T3a con meno di 1 GB di RAM, prova ad aumentare le dimensioni dell'istanza a un'istanza con almeno 1 GB di RAM.

L'istanza è bloccata nello stato di arresto

Se hai ibernato un'istanza e questa appare bloccata nello stato `stopping`, puoi forzarne l'arresto. Per ulteriori informazioni, consulta Risoluzione dei problemi di arresto dell'istanza.

Impossibile avviare l'istanza spot subito dopo l'ibernazione

Se provi ad avviare un'istanza spot entro due minuti dall'ibernazione, potresti ricevere il seguente errore:

`You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.`

Attendi circa due minuti per le istanze Linux e circa cinque minuti per le istanze Windows, quindi riprova ad avviare l'istanza.

Ripristino delle istanze spot non riuscito

Se l'istanza spot è stata ibernata correttamente ma non è stato possibile riattivarla e invece è stata riavviata (un nuovo riavvio in cui lo stato di ibernazione non viene mantenuto), è possibile che i dati dell'utente contenessero lo script seguente:

```
/usr/bin/enable-ec2-spot-hibernation
```

Rimuovi questo script dal campo Dati utente nel modello di avvio, quindi richiedi una nuova istanza spot.

Tieni presente che anche se l'istanza non è stata ripristinata senza che lo stato di ibernazione fosse mantenuto, potrà comunque essere avviata nello stesso modo in cui è stata avviata dallo stato `stopped`.

Riavvio dell'istanza

Il riavvio di un'istanza equivale al riavvio di un sistema operativo. Nella maggior parte dei casi, sono necessari pochi minuti per riavviare l'istanza.

Quando riavvii un'istanza, mantiene quanto segue:

- Nome DNS pubblico (IPv4)
- Indirizzo IPv4 privato
- Indirizzo IPv4 pubblico
- Indirizzo IPv6 (se applicabile)
- Tutti i dati presenti nei volumi dell'archivio dell'istanza

A differenza dell'arresto e avvio, il riavvio di un'istanza non comporta l'inizio di un nuovo periodo di fatturazione (con un addebito minimo di un minuto).

È possibile pianificare il riavvio di un'istanza per gli interventi di manutenzione necessari, ad esempio per applicare gli aggiornamenti che richiedono un riavvio. Non è necessario alcun intervento da parte tua. Ti consigliamo di attendere l'inizio del riavvio nell'intervallo di tempo pianificato. Per ulteriori informazioni, consulta Eventi pianificati per le istanze.

Ti consigliamo di utilizzare la console Amazon EC2, uno strumento a riga di comando oppure l'API Amazon EC2 per riavviare l'istanza anziché eseguire il comando di riavvio del sistema operativo dall'interno dell'istanza. Se utilizzi la console Amazon EC2, uno strumento a riga di comando o l'API Amazon EC2 per riavviare l'istanza, verrà eseguito un riavvio a freddo se l'istanza non si arresta entro alcuni minuti. Se utilizzi AWS CloudTrail, l'utilizzo di Amazon EC2 per riavviare l'istanza crea anche un record API relativo al momento in cui l'istanza è stata riavviata.

Istanze Windows

Se Windows sta installando aggiornamenti sull'istanza, consigliamo di non riavviare o arrestare l'istanza utilizzando la console Amazon EC2 o la riga di comando fino alla completa installazione di tutti gli aggiornamenti. Quando utilizzi la console Amazon EC2 o la riga di comando per riavviare

o arrestare l'istanza, sussiste il rischio che l'istanza venga riavviata a freddo. Un riavvio a freddo durante l'installazione degli aggiornamenti potrebbe rendere instabile l'istanza.

Console

Per riavviare un'istanza utilizzando la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare l'istanza e scegliere Instance state (Stato istanza), Reboot instance (Riavvia istanza).

   In alternativa, selezionare l'istanza e scegliere Actions (Operazioni),Manage instance state (Gestisci lo stato dell'istanza). Nella schermata visualizzata, scegliere Reboot (Riavvio), quindi Change state (Modifica stato).
4. Scegliere Reboot (Riavvia) quando viene richiesta la conferma.

   L'istanza rimane in stato di `running`.

Command line

Per riavviare un'istanza

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- reboot-instances (AWS CLI)
- Restart-EC2Instance (AWS Tools for Windows PowerShell)

Esecuzione di un esperimento di iniezione di guasti controllati

È possibile AWS Fault Injection Service utilizzarlo per verificare la risposta dell'applicazione al riavvio dell'istanza. Per ulteriori informazioni, consulta la Guida per l'utente AWS Fault Injection Service.

Termina le istanze Amazon EC2

Puoi eliminare un'istanza quando non è più necessaria. Questa operazione viene definita interruzione dell'istanza. Appena lo stato di un'istanza cambia in `shutting-down` o `terminated`, vengono bloccati i rispettivi addebiti.

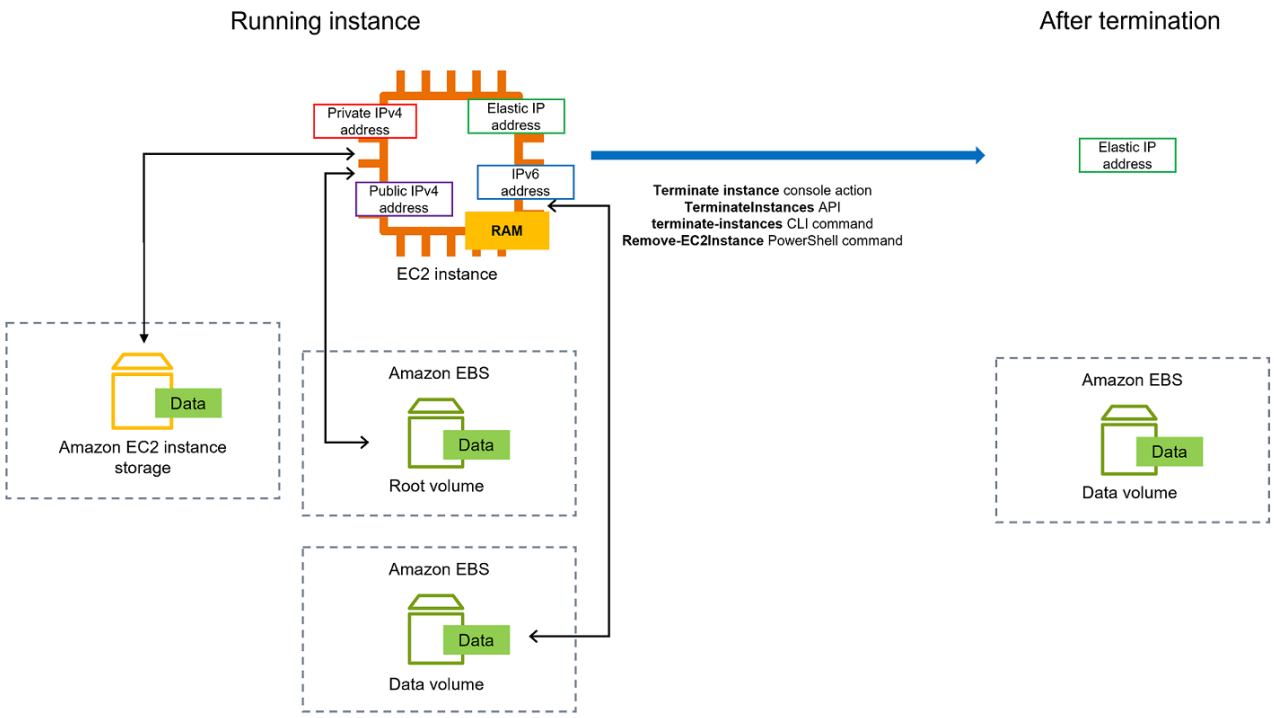
Dopo averla interrotta, non è più possibile connettersi a un'istanza o avviarla. Puoi tuttavia avviare istanze aggiuntive utilizzando la stessa AMI. Se preferisci interrompere o ibernare un'istanza, consulta o. Arresta e avvia le istanze Amazon EC2 Metti in ibernazione la tua istanza Amazon EC2 Per ulteriori informazioni, consulta Differenze tra riavvio, arresto, ibernazione e interruzione.

Indice

Come funziona la chiusura dell'istanza

Quando si termina un'istanza, le modifiche vengono registrate a livello di sistema operativo dell'istanza, alcune risorse vengono perse e altre persistono.

Il diagramma seguente mostra cosa viene perso e cosa persiste quando un'istanza Amazon EC2 viene terminata. Quando un'istanza termina, i dati su ogni istanza archiviano i volumi e i dati archiviati nella RAM dell'istanza vengono cancellati. Tutti gli indirizzi IP elastici associati all'istanza vengono scollegati. Per i volumi Amazon EBS e i dati su tali volumi, il risultato dipende dall'impostazione Delete on termination per il volume. Per impostazione predefinita, il volume principale viene eliminato e i volumi di dati vengono conservati.



Considerazioni

- Quando un'istanza viene interrotta, i dati disponibili sui volumi instance store a essa associati vengono eliminati.
- Per impostazione di default, i volumi dispositivo root Amazon EBS vengono eliminati quando l'istanza viene interrotta. Tuttavia, qualsiasi volume EBS aggiuntivo collegato all'avvio oppure qualsiasi volume EBS collegato a un'istanza esistente rimane persistente anche dopo l'interruzione dell'istanza. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.

> **Note**
>
> Continueranno a essere addebitati i costi per volumi che non vengono eliminati al momento della terminazione dell'istanza.

- Per evitare che un'istanza venga interrotta accidentalmente da qualcuno, abilita la protezione dalla terminazione.
- Per controllare se un'istanza si arresta o termina quando l'arresto viene avviato dall'istanza, modifica il comportamento di arresto avviato dall'istanza.

- Se esegui uno script durante la terminazione dell'istanza, si potrebbe verificare una terminazione anomala dell'istanza stessa perché non esiste alcun modo per garantire l'esecuzione degli script di arresto. Amazon EC2 cerca di arrestare un'istanza correttamente ed eseguire gli eventuali script di arresto del sistema. Tuttavia, alcuni eventi, ad esempio un errore hardware, potrebbero impedire l'esecuzione di questi script di arresto del sistema.

Cosa accade se si termina un'istanza

Modifiche registrate a livello di sistema operativo

- La richiesta dell'API invia un evento di pressione del pulsante al sistema guest.
- Vari servizi di sistema vengono arrestati a seguito dell'evento di pressione del pulsante. L'arresto corretto del sistema è fornito da systemd (Linux) o dal processo di sistema (Windows). L'arresto graceful viene attivato dall'evento di pressione del pulsante di arresto ACPI dall'hypervisor.
- L'arresto ACPI viene avviato.
- L'istanza verrà chiusa al termine del processo di arresto gradito. Non c'è un orario di arresto del sistema operativo configurabile. L'istanza rimane visibile nella console per un breve periodo, trascorso il quale la relativa voce viene eliminata automaticamente.

Risorse perse

- I dati archiviati in un volume di archivio dell'istanza.
- I dati archiviati in volumi dispositivo root Amazon EBS, se l'attributo `DeleteOnTermination` è impostato su vero.

Risorse che persistono

- I dati archiviati su volumi Amazon EBS collegati al momento del lancio o dopo il lancio di un'istanza.

Testare la risposta dell'applicazione alla terminazione dell'istanza

Puoi utilizzarle AWS Fault Injection Service per testare la risposta dell'applicazione quando l'istanza viene terminata. Per ulteriori informazioni, consulta la Guida per l'utente AWS Fault Injection Service.

Terminare un'istanza

Puoi terminare un'istanza in qualsiasi momento.

Console

Per interrompere un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona l'istanza e scegli Instance state (Stato istanza), Terminate instance (Termina istanza).
4. Quando viene richiesta la conferma, seleziona Terminate (Interrompi).
5. Dopo aver terminato un'istanza, questa rimane visibile per un breve periodo, con uno stato di. `terminated`

   Se la terminazione fallisce o se un'istanza terminata è visibile per più di qualche ora, vedi. L'istanza terminata rimane visualizzata

Command line

Per interrompere un'istanza utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- terminate-instances (AWS CLI)
- Remove-EC2Instance (AWS Tools for Windows PowerShell)

Risoluzione dei problemi relativi alla terminazione delle istanze

Il richiedente deve avere il permesso di chiamare. `ec2:TerminateInstances` Per ulteriori informazioni, consulta Esempi di politiche per l'utilizzo delle istanze.

Se termini l'istanza e avvii un'altra istanza, molto probabilmente hai configurato la scalabilità automatica tramite una caratteristica come Parco istanze EC2 o Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Istanze avviate o terminate automaticamente.

Non puoi terminare un'istanza se la protezione dalla terminazione è attivata. Per ulteriori informazioni, consulta Protezione dalla terminazione.

Se lo stato dell'istanza è `shutting-down` per un periodo più lungo del previsto, l'istanza deve essere cancellata (terminata) da processi automatizzati all'interno del servizio Amazon EC2. Per ulteriori informazioni, consulta Ritardo della terminazione dell'istanza.

Abilitare la protezione da cessazione

Per impedire che un'istanza venga interrotta per errore, è possibile abilitare la funzionalità di protezione da cessazione per tale istanza. L'`DisableApiTermination`attributo controlla se l'istanza può essere terminata utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o l'API. Per impostazione predefinita, la protezione dalla terminazione è disabilitata per l'istanza, il che significa che l'istanza può essere terminata utilizzando l'API AWS Management Console, AWS CLI, o. È possibile impostare il valore di questo attributo all'avvio di un'istanza, mentre l'istanza è in esecuzione oppure mentre l'istanza è arrestata (per le istanze supportate da Amazon EBS).

L'attributo `DisableApiTermination` non impedisce di interrompere un'istanza mediante l'inizializzazione dell'arresto dall'istanza stessa (utilizzando un comando del sistema operativo per l'arresto del sistema) quando l'attributo `InstanceInitiatedShutdownBehavior` è impostato. Per ulteriori informazioni, consulta Modifica del comportamento di arresto avviato dall'istanza.

Considerazioni

- L'attivazione della protezione dalla terminazione non AWS impedisce di terminare l'istanza quando è in corso un evento pianificato per terminare l'istanza.
- L'attivazione della protezione da cessazione non impedisce al Dimensionamento automatico Amazon EC2 di terminare un'istanza quando l'istanza non è integra o durante eventi di riduzione orizzontale. È possibile controllare se un gruppo con dimensionamento automatico può terminare una determinata istanza durante la riduzione utilizzando la protezione per la riduzione delle istanze. È possibile controllare se un gruppo con dimensionamento automatico può terminare istanze non integre sospendendo il processo di dimensionamento ReplaceUnhealthy.
- Non è possibile abilitare la protezione da interruzione per Istanze spot.

Per abilitare la protezione da interruzione per un'istanza all'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel pannello di controllo, scegliere Launch Instance (Avvia istanza) ed eseguire le istruzioni visualizzate nella procedura guidata.
3. Nella pagina Configure Instance Details (Configura i dettagli dell'istanza), selezionare la casella di controllo Enable termination protection (Abilita protezione da interruzione).

Per abilitare la protezione da interruzione per un'istanza in esecuzione o arrestata

1. Selezionare l'istanza, scegliere Actions (Operazioni), Instance Settings (Impostazioni istanza) e quindi scegliere Change Termination Protection (Modifica protezione da interruzione).
2. Scegliere Yes, Enable (Sì, abilita).

Per disabilitare la protezione da interruzione per un'istanza in esecuzione o arrestata

1. Selezionare l'istanza, scegliere Actions (Operazioni), Instance Settings (Impostazioni istanza) e quindi scegliere Change Termination Protection (Modifica protezione da interruzione).
2. Scegliere Yes, Disable (Sì, disabilita).

Per abilitare o disabilitare la protezione da interruzione utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Termina più istanze con la protezione dalla terminazione

Se si interrompono più istanze in più zone di disponibilità nella stessa richiesta e una o più delle istanze specificate sono abilitate per la protezione dalla terminazione, la richiesta ha esito negativo con i seguenti risultati:

- Le istanze specificate nella stessa zona di disponibilità dell'istanza protetta non vengono terminate.
- Le istanze specificate che si trovano in zone di disponibilità diverse, in cui non sono protette altre istanze specificate, vengono terminate correttamente.

Esempio

Supponiamo di avere le seguenti quattro istanze in due zone di disponibilità.

Istanza	Zona di disponibilità	Protezione da cessazione
Istanza 1	COME A	`Disabled`
Istanza 2		`Disabled`
Istanza 3	AZ B	`Enabled`
Istanza 4		`Disabled`

Se si tenta di terminare tutte queste istanze nella stessa richiesta, la richiesta segnala un errore con i seguenti risultati:

- L'istanza 1 e l'istanza 2 vengono terminate con successo perché nessuna delle due istanze è abilitata per la protezione dalla terminazione.
- L'istanza 3 e l'istanza 4 non riescono a terminare perché l'istanza 3 è abilitata per la protezione dalla terminazione.

Modifica del comportamento di arresto avviato dall'istanza

Per impostazione predefinita, quando si avvia un arresto da un'istanza supportata da Amazon EBS (utilizzando un comando come shutdown o poweroff), l'istanza viene arrestata. Puoi modificare questo comportamento in modo che l'istanza venga terminata invece di modificare l'attributo `InstanceInitiatedShutdownBehavior` per l'istanza. Puoi modificare questo attributo mentre l'istanza è in esecuzione o quando è arrestata.

Il comando halt non avvia un arresto. Se utilizzato, l'istanza non sarà terminata; al contrario, la CPU verrà messa in stato `HLT` e l'istanza rimarrà in esecuzione.

> **Note**
>
> L'attributo `InstanceInitiatedShutdownBehavior` si applica solo quando si esegue un arresto dal sistema operativo dell'istanza stessa. Non si applica quando si interrompe un'istanza utilizzando l'API `StopInstances` o la console Amazon EC2.

Puoi modificare l'attributo `InstanceInitiatedShutdownBehavior` utilizzando la console Amazon EC2 o la riga di comando.

Console

Modifica del comportamento di arresto avviato dall'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Scegliere Actions (Operazioni), Instance settings (Impostazioni istanza), Change shutdown behavior (Cambia comportamento di arresto).

   Il comportamento di arresto mostra il comportamento corrente.
5. Per modificare il comportamento, in Comportamento di arresto, scegli Arresta o Termina.
6. Selezionare Salva.

Command line

Modifica del comportamento di arresto avviato dall'istanza

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Conservare i dati quando un'istanza viene terminata

A seconda del caso d'uso, potresti voler conservare i dati nel volume di archivio dell'istanza o in un volume Amazon EBS quando l'istanza Amazon EC2 viene terminata. I dati presenti in un volume di archivio dell'istanza non vengono conservati quando un'istanza viene terminata. Se devi conservare i dati archiviati su un volume di archivio dell'istanza oltre la durata dell'istanza, devi copiarli manualmente su un'archiviazione più persistente, come un volume Amazon EBS, un bucket Amazon S3 o un file system Amazon EFS. Per ulteriori informazioni, consulta Opzioni di archiviazione per le istanze Amazon EC2.

Per i dati presenti in volumi Amazon EBS, Amazon EC2 utilizza il valore dell'attributo `DeleteOnTermination` di ciascun volume Amazon EBS collegato per determinare se conservare o eliminare il volume.

Il valore predefinito per l'attributo `DeleteOnTermination` differisce a seconda che il volume sia il volume root dell'istanza o un volume non root collegato all'istanza.

Volume root

Per impostazione predefinita, quando si avvia un'istanza, l'`DeleteOnTermination`attributo per il volume principale di un'istanza è impostato su. `true` Pertanto, il comportamento di default prevede l'eliminazione del volume root di un'istanza quando l'istanza viene interrotta.

Volume non root

Per impostazione predefinita, quando si collega un volume EBS non root a un'istanza, il relativo `DeleteOnTermination` attributo è impostato su. `false` Pertanto, il comportamento di default prevede la conservazione di questi volumi.

> **Note**
>
> Una volta interrotta l'istanza, puoi creare uno snapshot del volume conservato e collegarlo a un'altra istanza. È necessario eliminare un volume per evitare di incorrere in ulteriori addebiti.

L'attributo `DeleteOnTermination` può essere impostato dal creatore di un'AMI o dalla persona che lancia un'istanza. Quando l'attributo viene modificato dal creatore di un'AMI o dalla persona che lancia un'istanza, la nuova impostazione sostituisce l'impostazione predefinita originale dell'AMI. Si consiglia di verificare l'impostazione predefinita dell'attributo `DeleteOnTermination` dopo il lancio di un'istanza con un'AMI.

Per verificare se un volume Amazon EBS verrà eliminato al momento della terminazione dell'istanza, visualizzare i dettagli del volume nel riquadro dei dettagli dell'istanza. Nella scheda archiviazione (Archiviazione), in Block devices (Dispositivi a blocchi), scorrere verso destra per visualizzare l'impostazione per il volume Delete on termination (Elimina al termine).

- Se l'impostazione è Sì, il volume sarà eliminato al momento della terminazione dell'istanza.

- Se l'impostazione è No, il volume non sarà eliminato al momento della terminazione dell'istanza. Continueranno a essere addebitati i costi per volumi che non vengono eliminati al momento della terminazione dell'istanza.

Modifica il volume root in modo che persista all'avvio

Utilizzando la console puoi modificare l'attributo `DeleteOnTermination` all'avvio di un'istanza. Per modificare questo attributo per un'istanza in esecuzione, devi utilizzare la riga di comando.

Utilizza uno dei metodi seguenti per modificare il volume root per renderlo persistente all'avvio.

Console

Per modificare il volume root di un'istanza per renderlo persistente all'avvio utilizzando la console

1. Segui la procedura di avvio di un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per modificare il volume root per renderlo persistente.
2. In Archiviazione (volumi), espandi le informazioni relative al volume root.
3. In Elimina al termine, scegli No
4. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Command line

Per modificare il volume root di un'istanza per renderlo persistente all'avvio utilizzando la riga di comando

Quando avvii un'istanza supportata da EBS, puoi utilizzare uno dei seguenti comandi per modificare il volume dispositivo root e renderlo persistente. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- run-instances (AWS CLI)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Nelle mappature dei dispositivi a blocchi per i volumi che desideri mantenere, includi `--DeleteOnTermination` e specifica `false`.

Ad esempio, per mantenere un volume aggiungi la seguente opzione al comando `run-instances`:

```
--block-device-mappings file://mapping.json
```

In `mapping.json`, specifica il nome del dispositivo, ad esempio `/dev/sda1` o `/dev/xvda` e per `--DeleteOnTermination` specifica `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Modifica il volume root di un'istanza in esecuzione in modo che rimanga

Puoi utilizzare uno dei seguenti comandi per modificare il volume dispositivo root di un'istanza supportata da EBS in esecuzione e renderlo persistente. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Ad esempio, utilizza il seguente comando:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

In `mapping.json`, specifica il nome del dispositivo, ad esempio `/dev/sda1` o `/dev/xvda` e per `--DeleteOnTermination` specifica `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
```

```
      "DeleteOnTermination": false
    }
  }
]
```

Ritiro dell'istanza

È pianificato il ritiro di un'istanza quando AWS rileva un guasto irreparabile dell'hardware sottostante che ospita l'istanza. Il dispositivo root dell'istanza determina il comportamento del ritiro dell'istanza:

- Se il dispositivo root dell'istanza è un volume Amazon EBS, l'istanza viene arrestata e puoi avviarla di nuovo in qualsiasi momento. L'avvio di un'istanza arrestata ne comporta la migrazione in un nuovo hardware.
- Se il dispositivo principale dell'istanza è un volume di Instance Store, l'istanza viene terminata e non può essere riutilizzata.

Per ulteriori informazioni sui tipi di eventi relativi alle istanze, consulta Eventi pianificati per le istanze.

Indice

Identificazione delle istanze pianificate per il ritiro

Se l'istanza è pianificata per il ritiro, riceverai un'e-mail prima dell'evento con l'ID dell'istanza e la data del ritiro. È inoltre possibile verificare la presenza di istanze pianificate per il ritiro utilizzando la console Amazon EC2 o la riga di comando.

> **Important**
>
> Se un'istanza è pianificata per il ritiro, è consigliabile intervenire il prima possibile perché l'istanza potrebbe non essere raggiungibile. (La notifica e-mail che ricevi indica quanto segue: "A causa di questa degradazione, l'istanza potrebbe già essere irraggiungibile"). Per ulteriori informazioni sull'azione consigliata da intraprendere, consulta Check if your instance is reachable.

Modi per identificare le istanze programmate per il ritiro

- Notifiche e-mail
- Identificazione della console

Notifiche e-mail

Se l'istanza è pianificata per il ritiro, riceverai un'e-mail prima dell'evento con l'ID dell'istanza e la data del ritiro.

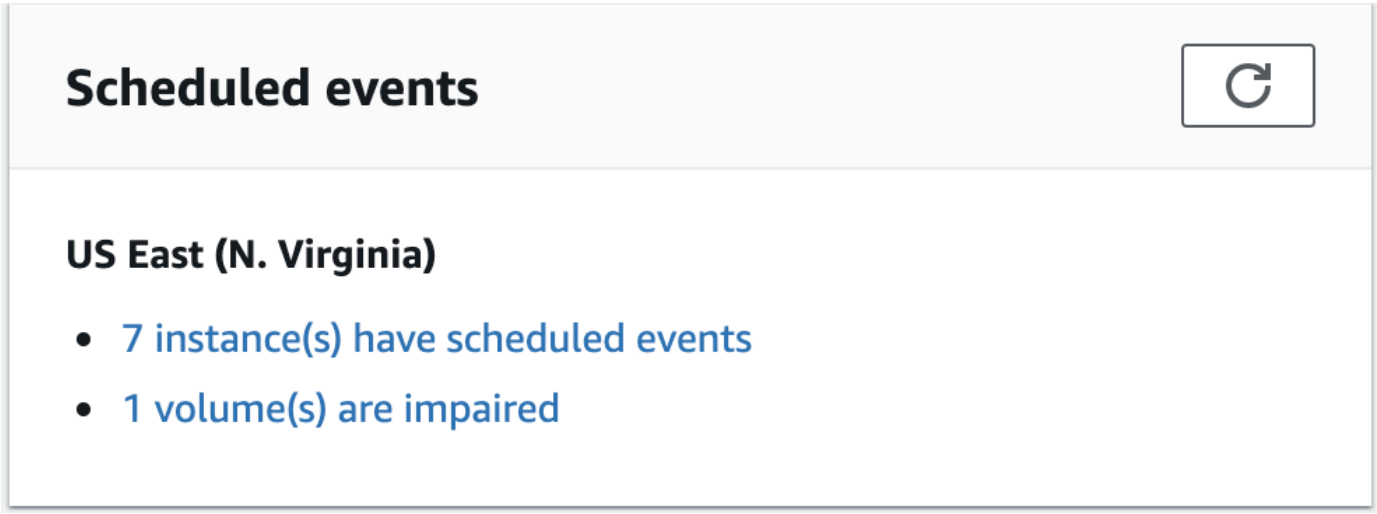
L'e-mail viene inviata al titolare dell'account principale e al referente operativo. Per ulteriori informazioni, consulta Aggiunta, modifica o rimozione di contatti alternativi nella Guida per l'utente di AWS Billing .

Identificazione della console

Se si tratta di un account e-mail che non verifichi regolarmente, puoi utilizzare la console Amazon EC2 o la riga di comando per determinare se alcune istanze sono pianificate per il ritiro.

Per identificare le istanze pianificate per il ritiro utilizzando la console

1. Aprire la console Amazon EC2.
2. Nel riquadro di navigazione scegliere EC2 Dashboard (Pannello di controllo EC2). In Scheduled events (Eventi pianificati), è possibile visualizzare gli eventi associati a istanze e volumi Amazon EC2, organizzati per regione.



3. Se nell'elenco viene visualizzata un'istanza con un evento pianificato, selezionare il relativo collegamento sotto il nome della regione per passare alla pagina Events (Eventi).

4. Nella pagina Events (Eventi) sono elencate tutte le risorse e i relativi eventi associati. Per visualizzare le istanze pianificate per il ritiro, selezionare Instance resources (Risorse istanze) nel primo elenco di filtri, quindi Instance stop or retirement (Ritiro o arresto istanze) nel secondo elenco di filtri.
5. Se i risultati dei filtri indicano che un'istanza è pianificata per il ritiro, selezionarla e annotare la data e l'ora riportata nel campo Start time (Ora di avvio) nel riquadro dei dettagli. Questa è la data di ritiro dell'istanza.

Per identificare le istanze pianificate per il ritiro utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- describe-instance-status (AWS CLI)
- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)

Azioni da intraprendere su istanze supportate da EBS programmate per il ritiro

Per conservare i dati sull'istanza pianificata per il ritiro, è possibile eseguire una delle seguenti operazioni. È essenziale che tu esegua questa operazione prima della data di ritiro dell'istanza per evitare tempi di inattività imprevisti o la perdita dei dati.

Per le istanze Linux, se non sei sicuro che la tua istanza sia supportata da EBS o dall'instance store, consulta. Volumi root per le tue istanze Amazon EC2

Controlla se la tua istanza è raggiungibile

Quando si riceve una notifica che l'istanza è pianificata per il ritiro, si consiglia di eseguire le seguenti azioni il prima possibile:

- Controlla se la tua istanza è raggiungibile collegandoti a o eseguendo il ping all'istanza.
- Se l'istanza è raggiungibile, è consigliabile pianificare di arrestare/avviare l'istanza in un momento appropriato prima della data di ritiro programmata, quando l'impatto è minimo. Per ulteriori informazioni su arresto e avvio dell'istanza e sulle conseguenze previste in caso di arresto dell'istanza, ad esempio effetti sugli indirizzi IP pubblici, privati ed elastici associati all'istanza, consulta Arresta e avvia le istanze Amazon EC2. Si noti che i dati sui volumi instance store vengono persi quando si arresta e si avvia l'istanza.

- Se l'istanza non è raggiungibile, è necessario intraprendere un'azione immediata ed eseguire un arresto/avvio per recuperare l'istanza.
- In alternativa, se si desidera terminare l'istanza, pianificare di farlo il prima possibile in modo da interrompere gli addebiti per l'istanza.

Creare un backup dell'istanza

Crea un'AMI EBS-backed dalla tua istanza in modo da avere un backup. Per garantire l'integrità dei dati, arrestare l'istanza prima di creare l'AMI. Puoi attendere la data di ritiro pianificato (quando l'istanza viene arrestata) oppure arrestare manualmente l'istanza prima della data di ritiro. Puoi avviare di nuovo l'istanza in qualsiasi momento. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.

Avviare un'istanza sostitutiva

Dopo aver creato un'AMI dall'istanza, è possibile utilizzare l'AMI per avviare un'istanza sostitutiva. Dalla console Amazon EC2, seleziona la tua nuova AMI, quindi scegli Launch instance from AMI. Configura i parametri per la tua istanza, quindi scegli Launch instance. Per ulteriori informazioni su ciascun campo, consultare Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Azioni da intraprendere per istanze supportate dall'instance store pianificate per il ritiro

Per conservare i dati sull'istanza pianificata per il ritiro, è possibile eseguire una delle seguenti operazioni. È essenziale che tu esegua questa operazione prima della data di ritiro dell'istanza per evitare tempi di inattività imprevisti o la perdita dei dati.

> **Warning**
>
> Al raggiungimento della relativa data di scadenza, la tua istanza supportata da instance store viene interrotta e non sarai più in grado di recuperare l'istanza o i relativi dati in essa archiviati. Indipendentemente dal dispositivo root dell'istanza, i dati sui volumi instance store vanno perduti quando l'istanza viene ritirata, anche se sono collegati a un'istanza supportata da EBS.

Controlla se la tua istanza è raggiungibile

Quando si riceve una notifica che l'istanza è pianificata per il ritiro, si consiglia di eseguire le seguenti azioni il prima possibile:

- Controlla se la tua istanza è raggiungibile collegandoti a o eseguendo il ping all'istanza.
- Se la tua istanza è irraggiungibile, probabilmente c'è molto poco che può essere fatto per recuperare la tua istanza. Per ulteriori informazioni, consultaRisoluzione di problemi relativi a un'istanza irraggiungibile. AWS interromperà l'istanza alla data prevista per il pensionamento, quindi, nel caso di un'istanza irraggiungibile, potrà terminare immediatamente l'istanza autonomamente.

Avviare un'istanza sostitutiva

Crea un'AMI supportata da instance store dalla tua istanza utilizzando gli strumenti AMI, come descritto in Creazione di un'AMI Linux supportata da un instance store. Dalla console Amazon EC2, seleziona la tua nuova AMI, quindi scegli Launch instance from AMI. Configura i parametri per la tua istanza, quindi scegli Launch instance. Per ulteriori informazioni su ciascun campo, consultare Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Converti la tua istanza in un'istanza supportata da EBS

Trasferire i dati in un volume EBS, acquisire uno snapshot del volume e quindi creare AMI dallo snapshot. Puoi avviare un'istanza di sostituzione dalla nuova AMI. Per ulteriori informazioni, consulta Conversione dell'AMI supportata da instance store in un'AMI Amazon EBS-backed.

Resilienza delle istanze

> **Important**
>
> Le seguenti informazioni si applicano alla configurazione delle funzionalità relative al ripristino su istanze integre. Se al momento riscontri difficoltà di accesso alla tua istanza, consulta Risoluzione dei problemi relativi alle istanze EC2.

Nel caso in cui si AWS determini che un'istanza non è disponibile a causa di un problema hardware sottostante, è possibile configurare due meccanismi, ad esempio la resilienza in grado di ripristinare la disponibilità: il ripristino automatico semplificato e il ripristino basato sulle CloudWatch azioni di Amazon. Questo processo è chiamato ripristino dell'istanza.

Almeno un meccanismo deve essere configurato o abilitato in anticipo con risorse supportate affinché si verifichi il processo di ripristino dell'istanza. Per impostazione predefinita, il ripristino automatico semplificato è abilitato per le istanze supportate al momento dell'avvio.

Argomenti

Panoramica del ripristino delle istanze

Di seguito sono riportati alcuni esempi di problemi hardware sottostanti che potrebbero richiedere il ripristino dell'istanza:

- Perdita di connettività di rete
- Perdita di alimentazione elettrica del sistema
- Problemi di software sull'host fisico
- Problemi hardware sull'host fisico che incidono sulla raggiungibilità della rete

Un'istanza recuperata è identica all'istanza originale, inclusa la sua:

- ID istanza
- Indirizzi IP pubblici, privati ed elastici
- Metadati delle istanze
- Gruppo di posizionamento
- Volumi EBS allegati
- Zona di disponibilità

Un ripristino riuscito dell'istanza verrà visualizzato dall'istanza come un riavvio non pianificato. In altre parole, il contenuto archiviato nella memoria volatile andrà perso, i dati dell'archivio delle istanze verranno cancellati e l'operatività del sistema operativo ricomincerà da zero.

Per contribuire alla protezione dalla perdita di dati, si consiglia di creare regolarmente backup di dati importanti. Per ulteriori informazioni sulle best practice di backup e ripristino per le istanze Amazon EC2, consulta Best practice for Amazon EC2.

Alternative di ripristino delle ist

Le seguenti alternative al ripristino delle istanze possono essere prese in considerazione quando soddisfano il caso d'uso delle istanze.

Gruppi Auto Scaling

È possibile utilizzare i gruppi Auto Scaling per consentire di raggruppare una raccolta di istanze ai fini della scalabilità e della disponibilità. Nel caso in cui un'istanza all'interno di un gruppo Auto Scaling diventi non disponibile, l'istanza verrà automaticamente sostituita (non recuperata) dal gruppo Auto Scaling. Per ulteriori informazioni, consulta Cos'è Amazon EC2 Auto Scaling? nella Guida per l'utente di Amazon EC2 Auto Scaling.

Amazon EBS Multi-Attacchi

Puoi configurare Amazon EBS Multi-Attach per le tue istanze per consentire la connessione di più istanze allo stesso volume EBS. Se combinato con un software appropriato, ciò consente di abilitare il clustering ad alta disponibilità. Per un esempio di configurazione con istanze Linux, consulta Storage cluster semplificato: volumi abilitati per GFS2 su Amazon EBS Multi-Attach sullo Storage Blog. AWS

Configura il ripristino basato sulle azioni CloudWatch

> **Important**
>
> - Le seguenti informazioni si applicano alla configurazione delle funzionalità relative al ripristino su istanze integre. Se al momento riscontri difficoltà di accesso alla tua istanza, consulta Risoluzione dei problemi relativi alle istanze EC2.
> - Affinché il carico di lavoro funzioni correttamente dopo il corretto ripristino dell'istanza, l'istanza deve avviarsi e accettare il traffico senza richiedere l'intervento manuale.

Puoi configurare il ripristino basato sulle CloudWatch azioni di Amazon per aggiungere azioni di ripristino agli CloudWatch allarmi Amazon. CloudWatch il ripristino basato sulle azioni funziona con la `StatusCheckFailed_System` metrica. CloudWatch il ripristino basato sull'azione fornisce la granularità dei tempi di risposta al to-the-minute ripristino e notifiche Amazon Simple Notification Service (Amazon SNS) delle azioni e dei risultati del ripristino. Queste opzioni di configurazione consentono tentativi di ripristino più rapidi con un controllo più granulare sulla risposta agli eventi di

errore del controllo dello stato del sistema rispetto al ripristino automatico semplificato. Per ulteriori informazioni sulle CloudWatch opzioni disponibili, consulta Controlli di stato per le istanze.

Il ripristino basato sulle CloudWatch azioni di Amazon non funziona durante gli eventi di servizio in AWS Health Dashboard. Per ulteriori informazioni, consulta the section called “Risoluzione dei problemi di ripristino basati sulle CloudWatch azioni”.

Argomenti

- Requisiti e limitazioni per il ripristino basato sull' CloudWatch azione
- Configura il ripristino basato sulle CloudWatch azioni
- Risoluzione dei problemi di ripristino basati sulle CloudWatch azioni

Requisiti e limitazioni per il ripristino basato sull' CloudWatch azione

CloudWatch il ripristino basato sull'azione può tentare di ripristinare un'istanza se:

- È nello `running` stato. Per ulteriori informazioni, consulta the section called “Ciclo di vita dell'istanza”.
- Utilizza `default` (On-Demand) o locazione dell'`dedicate`distanza. Per ulteriori informazioni, consulta the section called “Opzioni di acquisto delle istanze”.
- È di un tipo di istanza per cui Amazon EC2 ha capacità disponibile. In alcune situazioni, ad esempio interruzioni significative, la capacità disponibile non sarà sufficiente e alcuni tentativi di ripristino potrebbero fallire.
- Non utilizza la tenancy dell'`dedicate`distanza. Per gli host dedicati di Amazon EC2, puoi utilizzare il ripristino automatico degli host dedicati per ripristinare automaticamente le istanze non integre.
- Non utilizza un Elastic Fabric Adapter.
- Non è membro di un gruppo Auto Scaling.
- Al momento non è sottoposto a un evento di manutenzione programmato.
- Utilizza uno dei seguenti tipi di istanza:
  - Uso generico: A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Elaborazione ottimizzata: C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-Flex

- Memoria ottimizzata: R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6i | R6in | R7a | R7g | R7i | R7iZ | R8g | u-3tb1 | u-6tb1 | u-9tb1 | u-12tb1 | u-18tb1 | u-24tb1 | u7-12tb | u7in-16tb | u7in-24tb | u7in-32tb | X1 | X1e | X2iEzN
- Calcolo accelerato: G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
- Elaborazione ad alte prestazioni: HPC6a | HPC7a | HPC7g
- Istanze in metallo: uno qualsiasi dei tipi precedenti con istanze in metallo delle stesse dimensioni.

- Dispone di volumi di archiviazione delle istanze e utilizza uno dei seguenti tipi di istanza: M3 | C3 | R3 | X1 | X1e | X2idn | X2iedn

> **Warning**
>
> - I dati sui volumi dell'Instance Store andranno persi se l'istanza viene interrotta. Per ulteriori informazioni sull'arresto di un'istanza, consultathe section called “Arresto e avvio dell'istanza”.
> - In caso di errore nel controllo dello stato del sistema, i dati mappati del dispositivo di archiviazione e blocco dell'istanza potrebbero andare persi. Per questi tipi di istanze, puoi prendere in considerazione l'utilizzo the section called “Abilitare la protezione da cessazione” di.
>
> Ti consigliamo di creare regolarmente backup di dati importanti. Per informazioni sulle best practice di backup e ripristino per Amazon EC2, consulta Best practice for Amazon EC2.

Puoi anche usare AWS Management Console o the AWS CLI per visualizzare i tipi di istanza che supportano il ripristino basato sulle CloudWatch azioni.

Console

Per visualizzare i tipi di istanze che supportano il ripristino basato sulle CloudWatch azioni di Amazon

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Instance Types (Tipi di istanza).

3. Nella barra del filtro, inserisci Auto Recovery support: true (Supporto per il ripristino automatico: vero). In alternativa, quando si immettono i caratteri e viene visualizzato il nome del filtro, è possibile selezionarlo.

   La tabella dei tipi di istanza mostra tutti i tipi di istanza che supportano il ripristino basato sulle CloudWatch azioni di Amazon.

AWS CLI

Per visualizzare i tipi di istanze che supportano il ripristino basato sulle CloudWatch azioni di Amazon

Utilizza il comando describe-instance-types.

```
aws ec2 describe-instance-types --filters Name=auto-recovery-supported,Values=true
--query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Configura il ripristino basato sulle CloudWatch azioni

CloudWatch il ripristino basato sulle azioni funziona con la `StatusCheckFailed_System` metrica. CloudWatch il ripristino basato sull'azione viene configurato tramite la CloudWatch console. Per configurare il ripristino basato sulle CloudWatch azioni, consulta Aggiungere azioni di ripristino agli CloudWatch allarmi nella Amazon CloudWatch User Guide.

Risoluzione dei problemi di ripristino basati sulle CloudWatch azioni

I seguenti problemi possono causare il fallimento del ripristino dell'istanza con il ripristino basato sulle CloudWatch azioni:

- CloudWatch il ripristino basato sull'azione non funziona durante gli eventi di servizio in AWS Health Dashboard. Potresti non ricevere notifiche di errore di ripristino per tali eventi. Per le informazioni più recenti sulla disponibilità del servizio, consulta la pagina sullo stato di integrità del servizio.
- Capacità insufficiente temporanea dell'hardware sostitutivo.
- L'istanza ha raggiunto l'indennità giornaliera massima per i tentativi di ripristino. Successivamente, l'istanza potrebbe venire ritirata se il ripristino automatico ha esito negativo e se un deterioramento dell'hardware viene considerato la causa radice dell'errore originale della verifica dello stato del sistema.

Se l'errore di controllo dello stato del sistema dell'istanza persiste nonostante più tentativi di ripristino, consulta Risoluzione dei problemi delle istanze con controlli dello stato non riusciti per ulteriori indicazioni.

Configura il ripristino automatico semplificato

> **Important**
>
> - Le seguenti informazioni si applicano alla configurazione delle funzionalità relative al ripristino su istanze integre. Se al momento riscontri difficoltà di accesso alla tua istanza, consulta Risoluzione dei problemi relativi alle istanze EC2.
> - Affinché il carico di lavoro funzioni correttamente dopo il corretto ripristino dell'istanza, l'istanza deve avviarsi e accettare il traffico senza richiedere l'intervento manuale.

Per impostazione predefinita, il ripristino automatico semplificato monitora tutte le istanze in esecuzione supportate. Nel caso in cui venga rilevato un errore di controllo dello stato del sistema, il ripristino automatico semplificato tenta di ripristinare l'integrità dell'istanza. Il ripristino automatico semplificato non funziona durante gli eventi di servizio in. AWS Health Dashboard Per ulteriori informazioni, consulta the section called “Risoluzione dei problemi di ripristino automatico semplificati”.

Quando si verifica un evento di ripristino automatico semplificato, si riceverà un AWS Health Dashboard evento. Per configurare le notifiche per questi eventi, consulta la Guida introduttiva Notifiche all'utente AWS nella Guida per l'Notifiche all'utente AWS utente. Puoi anche utilizzare EventBridge le regole di Amazon per monitorare gli eventi di ripristino automatico semplificati utilizzando i seguenti codici evento:

- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`: eventi con esito positivo
- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`: eventi con esito negativo

Per ulteriori informazioni, consulta EventBridge le regole di Amazon.

Argomenti

- Requisiti e limitazioni per il ripristino automatico semplificato
- Configura il ripristino automatico semplificato
- Risoluzione dei problemi di ripristino automatico semplificati

Requisiti e limitazioni per il ripristino automatico semplificato

Il ripristino automatico semplificato tenterà di ripristinare un'istanza se:

- È nello `running` stato. Per ulteriori informazioni, consulta the section called “Ciclo di vita dell'istanza”.
- Usi `default` (su richiesta) o `dedicated` locazione. Per ulteriori informazioni, consulta the section called “Opzioni di acquisto delle istanze”.
- È di un tipo di istanza per cui Amazon EC2 ha capacità disponibile. In alcune situazioni, ad esempio interruzioni significative, la capacità disponibile non sarà sufficiente e alcuni tentativi di ripristino potrebbero fallire.
- Non utilizza la `host` locazione. Per gli host dedicati di Amazon EC2, puoi utilizzare il ripristino automatico degli host dedicati per ripristinare automaticamente le istanze non integre.
- Non utilizza un Elastic Fabric Adapter.
- Non è una dimensione dell'`metal`istanza.
- Non è membro di un gruppo Auto Scaling.
- Al momento non è sottoposto a un evento di manutenzione programmato.
- Non dispone di volumi di Instance Store.
- Utilizza uno dei seguenti tipi di istanza:
  - Uso generico: A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Elaborazione ottimizzata: C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-Flex
  - Memoria ottimizzata: R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6i | R6in | R7a | R7g | R7i | R7iZ | R8g | u-3tb1 | u-6tb1 | u-9tb1 | u-12tb1 | u-18tb1 | u-24tb1 | u7-12tb | u7in-16tb | u7in-24tb | u7in-32tb | X1 | X1e | X2iEzN
  - Calcolo accelerato: G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
  - Elaborazione ad alte prestazioni: HPC6a | HPC7a | HPC7g

⚠ Warning

- I dati sui volumi dell'archivio delle istanze andranno persi se l'istanza viene interrotta. Per ulteriori informazioni sull'arresto di un'istanza, consultathe section called “Arresto e avvio dell'istanza”.

- In caso di errore nel controllo dello stato del sistema, i dati mappati del dispositivo di archiviazione e blocco dell'istanza potrebbero andare persi. Per questi tipi di istanze, puoi prendere in considerazione l'utilizzo the section called “Abilitare la protezione da cessazione” di.

Ti consigliamo di creare regolarmente backup di dati importanti. Per informazioni sulle best practice di backup e ripristino per Amazon EC2, consulta Best practice for Amazon EC2.

Configura il ripristino automatico semplificato

Il ripristino automatico semplificato è abilitato per impostazione predefinita all'avvio di un'istanza supportata. È possibile impostare il comportamento di ripristino automatico `disabled` durante o dopo l'avvio dell'istanza. La `default` configurazione non consente il ripristino automatico semplificato per un tipo di istanza non supportato.

Console

Per disabilitare il ripristino automatico semplificato durante l'avvio dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze), quindi seleziona Launch instance (Avvia istanza).
3. Nella sezione Advanced details (Dettagli avanzati), per Instance auto-recovery (Ripristino automatico dell'istanza) seleziona Disabled (Disabilitato).
4. Configura le impostazioni di avvio dell'istanza rimanenti secondo necessità e quindi avvia l'istanza.

Disabilitare il recupero automatico semplificato per un'istanza in esecuzione o arrestata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Actions (Operazioni), Instance Settings (Impostazioni istanza), Change auto-recovery behavior (Modifica comportamento di ripristino automatico).
4. Selezionare Off (Disattiva), quindi Save (Salva URL).

Come impostare il comportamento di ripristino automatico come **`default`** (di default) per un'istanza in esecuzione o arrestata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Actions (Operazioni), Instance Settings (Impostazioni istanza), Change auto-recovery behavior (Modifica comportamento di ripristino automatico).
4. Scegli Predefinito (attivo), quindi Salva.

AWS CLI

Disabilitare il ripristino automatico semplificato all'avvio

Utilizzare il comando run-instances.

```
aws ec2 run-instances \
--image-id ami-1a2b3c4d \
--instance-type t2.micro \
--key-name MyKeyPair \
--maintenance-options AutoRecovery=Disabled \
  [...]
```

Disabilitare il recupero automatico semplificato per un'istanza in esecuzione o arrestata

Utilizza il comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery disabled
```

Come impostare il comportamento di ripristino automatico come **`default`** (di default) per un'istanza in esecuzione o arrestata

Utilizza il comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery default
```

Risoluzione dei problemi di ripristino automatico semplificati

I seguenti problemi possono causare il fallimento del ripristino dell'istanza con il ripristino automatico semplificato:

- Il ripristino automatico semplificato non funziona durante gli eventi di servizio in. AWS Health Dashboard Potresti non ricevere notifiche di errore di ripristino per tali eventi. Per le informazioni più recenti sulla disponibilità del servizio, consulta la pagina sullo stato di integrità del servizio.
- Capacità insufficiente temporanea dell'hardware sostitutivo.
- L'istanza ha raggiunto l'indennità giornaliera massima per i tentativi di ripristino. Successivamente, l'istanza potrebbe venire ritirata se il ripristino automatico ha esito negativo e se un deterioramento dell'hardware viene considerato la causa radice dell'errore originale della verifica dello stato del sistema.

Se l'errore di controllo dello stato del sistema dell'istanza persiste nonostante più tentativi di ripristino, consulta Risoluzione dei problemi delle istanze con controlli dello stato non riusciti per ulteriori indicazioni.

Utilizzo dei metadati delle istanze

I metadati dell'istanza sono dati relativi all'istanza che puoi utilizzare per configurare o gestire un'istanza in esecuzione. I metadati dell'istanza sono suddivisi in categorie, ad esempio, nome host, eventi e gruppi di sicurezza.

Puoi anche utilizzare i metadati dell'istanza per accedere ai dati utente specificati quando un'istanza viene avviata. Ad esempio, puoi specificare i parametri per configurare l'istanza o includere un semplice script. Puoi anche creare AMI generiche e utilizzare i dati utente per modificare i file di configurazione forniti al momento dell'avvio. Ad esempio, se gestisci server Web per diverse piccole imprese, tutte possono utilizzare la stessa AMI generica e recuperare il contenuto da un bucket Amazon S3 specificato nei dati utente al momento del lancio. Per aggiungere un nuovo cliente in qualsiasi momento, crea un bucket per il cliente, aggiungi il relativo contenuto e avvia l'AMI con il nome bucket univoco fornito al codice nel dati utente. Se avvii più istanze utilizzando la stessa `RunInstances` chiamata, i dati utente sono disponibili per tutte le istanze della prenotazione. Ogni istanza che fa parte della stessa prenotazione ha un `ami-launch-index` numero univoco, in modo da poter scrivere codice che controlli il funzionamento delle istanze. Ad esempio, il primo host potrebbe scegliere se stesso come nodo originale in un cluster. Per un esempio dettagliato di lancio di un'AMI, consultaEsempio Linux: valore dell'indice di lancio AMI.

Le istanze EC2 possono inoltre includere dati dinamici, ad esempio un documento di identità dell'istanza generato all'avvio dell'istanza. Per ulteriori informazioni, consulta Categorie dei dati dinamici.

> **Important**
>
> Anche se puoi accedere ai metadati dell'istanza e ai dati utente solo dall'interno dell'istanza stessa, i dati non sono protetti mediante metodi di autenticazione o crittografia. Chiunque disponga dell'accesso diretto all'istanza, e potenzialmente qualsiasi software in esecuzione sull'istanza, può visualizzare i propri metadati. Pertanto, è opportuno non memorizzare dati sensibili, ad esempio password o chiavi di crittografia di lunga durata, come dati utente.

Indice

Usa IMDSv2

Puoi accedere ai metadati dell'istanza da un'istanza in esecuzione utilizzando uno dei metodi seguenti:

- Servizio di metadati dell'istanza Versione 1 (IMDSv1): un metodo di richiesta/risposta
- Servizio di metadati dell'istanza Versione 2 (IMDSv2): un metodo orientato alla sessione

Per impostazione predefinita, puoi utilizzare IMDSv1 o IMDSv2 oppure entrambi.

Puoi configurare il servizio di metadati dell'istanza (IMDS) su ogni istanza in modo che il codice locale o gli utenti utilizzino IMDSv2. Quando specifichi l'utilizzo di IMDSv2, IMDSv1 non funziona più. Per informazioni su come configurare l'istanza per l'utilizzo di IMDSv2, consulta Configura le opzioni dei metadati dell'istanza.

Le intestazioni `PUT` o `GET` sono esclusive di IMDSv2. Se queste intestazioni sono presenti nella richiesta, la richiesta è destinata a IMDSv2. Se non sono presenti intestazioni, si presume che la richiesta sia destinata a IMDSv1.

Per un'analisi approfondita di IMDSv2, consulta Aggiungere protezione in profondità contro firewall aperti, proxy inversi e vulnerabilità SSRF con miglioramenti al servizio di metadati dell'istanza EC2.

Per recuperare i metadati dell'istanza, vedere Recupero dei metadati dell'istanza.

Argomenti

- Funzionamento di Servizio di metadati dell'istanza Versione 2
- Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2
- Utilizzo di un SDK AWS supportato

Funzionamento di Servizio di metadati dell'istanza Versione 2

IMDSv2 utilizza richieste orientate alla sessione. Con richieste orientate alla sessione, puoi creare un token di sessione che definisce la durata della sessione, che può essere compresa tra un minimo di un secondo e un massimo di sei ore. Durante la specifica della durata, puoi utilizzare lo stesso token di sessione per le richieste successive. Al termine della durata specificata, è necessario creare un nuovo token di sessione da utilizzare per richieste future.

> **Note**
>
> Negli esempi riportati in questa sezione viene utilizzato l'indirizzo IPv4 del servizio di metadati dell'istanza (IMDS): `169.254.169.254`. Se si recuperano i metadati per le istanze EC2 tramite l'indirizzo IPv6, accertarsi invece di abilitare e utilizzare l'indirizzo IPv6: `[fd00:ec2::254]`. L'indirizzo IPv6 del servizio di metadati dell'istanza (IMDS) è compatibile con i comandi IMDSv2. L'indirizzo IPv6 è accessibile solo su istanze create sul sistema AWS Nitro e in una sottorete supportata da IPv6 (dual stack o solo IPv6).

Gli esempi seguenti utilizzano uno script di shell e IMDSv2 per recuperare gli elementi di metadati dell'istanza di primo livello. Ogni esempio:

- Crea un token di sessione della durata di sei ore (21.600 secondi) utilizzando la richiesta PUT
- Memorizza l'intestazione del token di sessione in una variabile denominata `TOKEN` (istanze Linux) o `token` (istanze Windows)
- Richiede gli elementi di metadati di livello superiore utilizzando il token

Esempio per Linux

È possibile eseguire due comandi separati o combinarli.

Comandi separati

Innanzitutto, generare un token utilizzando il comando riportato di seguito.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"`
```

Quindi, utilizzare il token per generare elementi di metadati di primo livello utilizzando il seguente comando.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/
```

Comandi combinati

È possibile memorizzare il token e combinare i comandi. L'esempio seguente combina i due comandi precedenti e memorizza l'intestazione del token di sessione in una variabile denominata TOKEN.

> **Note**
>
> Se si verifica un errore nella creazione del token, invece di un token valido nella variabile viene memorizzato un messaggio di errore e il comando avrà esito negativo.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Dopo aver creato un token, puoi riutilizzarlo finché non scade. Nel comando di esempio seguente, che ottiene l'ID dell'AMI utilizzata per avviare l'istanza, viene riutilizzato il token memorizzato in `$TOKEN` nell'esempio precedente.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/ami-id
```

Esempio per Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

Dopo aver creato un token, puoi riutilizzarlo finché non scade. Nel comando di esempio seguente, che ottiene l'ID dell'AMI utilizzata per avviare l'istanza, viene riutilizzato il token memorizzato in `$token` nell'esempio precedente.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
-Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Quando utilizzi IMDSv2 per richiedere i metadati dell'istanza, la richiesta deve includere quanto segue:

1. Utilizza una richiesta PUT per inizializzare una sessione al servizio di metadati dell'istanza. La richiesta PUT restituisce un token che deve essere incluso nelle richieste GET successive al servizio di metadati dell'istanza. Il token è obbligatorio per accedere ai metadati utilizzando IMDSv2.
2. Includi il token in tutte le richieste GET inviate all'IMDS. Quando l'uso del token è impostato su `required`, le richieste senza una token valido o con un token scaduto ricevono un codice di errore HTTP `401 - Unauthorized`.
   - Il token è una chiave specifica dell'istanza. Il token non è valido su altre istanze EC2 e verrà rifiutato se si tenta di utilizzarlo all'esterno dell'istanza su cui è stato generato.
   - La richiesta PUT deve includere un'intestazione che specifica il Time To Live (TTL) per il token, in secondi, fino a un massimo di sei ore (21.600 secondi). Il token rappresenta una sessione logica. Il TTL specifica la durata di validità del token e, pertanto, la durata della sessione.

- Dopo che un token scade, per continuare ad accedere ai metadati dell'istanza, è necessario creare una nuova sessione utilizzando un altro PUT.
- Puoi scegliere di riutilizzare un token o creare un nuovo token con ogni richiesta. Per un piccolo numero di richieste, potrebbe essere più semplice generare e utilizzare immediatamente un token ogni volta che devi accedere al servizio di metadati dell'istanza (IMDS). Per maggior efficienza, tuttavia, puoi specificare una durata maggiore per il token e riutilizzarlo, piuttosto che dover riscrivere una richiesta PUT ogni volta che devi richiedere metadati dell'istanza. Non esiste un limite effettivo al numero di token simultanei, ciascuno dei quali rappresenta la propria sessione. Tuttavia, IMDSv2 è ancora vincolato ai normali limiti di connessione e limitazione (della larghezza di banda della rete) di IMDS. Per ulteriori informazioni, consulta Throttling delle query.

Nei metodi HTTP GET e HEAD sono consentite richieste dei metadati dell'istanza IMDSv2. Le richieste PUT vengono rifiutate se contengono un'intestazione X-Forwarded-For.

Per impostazione predefinita, la risposta alle richieste PUT dispone di un limite di hop della risposta (time-to-live) di 1 a livello del protocollo IP. Se hai bisogno di un limite di hop maggiore, puoi regolarlo usando il comando. modify-instance-metadata-options AWS CLI Ad esempio, potrebbe essere necessario un limite di hop maggiore per la compatibilità con le versioni precedenti dei servizi container in esecuzione sull'istanza. Per ulteriori informazioni, consulta Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti.

Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2

Se scegli di eseguire la migrazione a IMDSv2, ti consigliamo di utilizzare gli strumenti e il percorso di transizione seguenti.

Argomenti

- Strumenti per semplificare la transizione a IMDSv2
- Percorso consigliato per richiedere IMDSv2

Strumenti per semplificare la transizione a IMDSv2

Se il software utilizza IMDSv1, gli strumenti seguenti consentono di riconfigurare il software per utilizzare IMDSv2.

AWS software

Le versioni più recenti degli AWS CLI AWS SDK supportano IMDSv2. Per utilizzare IMDSv2, accertati che le istanze EC2 dispongano delle versioni più recenti della CLI e degli SDK. Per informazioni sull'aggiornamento della CLI, consulta Installazione, aggiornamento e disinstallazione di AWS CLI nella Guida per l'utente di AWS Command Line Interface .

Tutti i pacchetti software Amazon Linux 2 e Amazon Linux 2023 supportano iMDSv2. In Amazon Linux 2023, iMDSv1 è disabilitato per impostazione predefinita.

Per le versioni AWS SDK minime che supportano IMDSv2, consulta. Utilizzo di un SDK AWS supportato

IMDS Packet Analyzer

IMDS Packet Analyzer è uno strumento open source che identifica e registra le chiamate IMDSv1 dalla fase di avvio dell'istanza. Questo strumento può aiutare a identificare il software che effettua chiamate IMDSv1 sulle istanze EC2, consentendoti di individuare esattamente cosa devi aggiornare per preparare le tue istanze al solo utilizzo di IMDSv2. Puoi eseguire IMDS Packet Analyzer da una riga di comando o installarlo come servizio. Per ulteriori informazioni, vedere IMDS Packet Analyzer su. GitHub

CloudWatch

IMDSv2 utilizza sessioni supportate da token, mentre IMDSv1 no. La `MetadataNoToken` CloudWatch metrica tiene traccia del numero di chiamate all'Instance Metadata Service (IMDS) che utilizzano IMDSv1. Monitorando questo parametro a zero, puoi determinare se e quando tutto il software è stato aggiornato per utilizzare IMDSv2.

Dopo aver disabilitato IMDSv1, puoi utilizzare la `MetadataNoTokenRejected` CloudWatch metrica per tenere traccia del numero di volte in cui una chiamata IMDSv1 è stata tentata e rifiutata. Monitorando questa metrica, puoi verificare se il tuo software deve essere aggiornato per utilizzare IMDSv2.

Per ulteriori informazioni, consulta Parametri dell'istanza.

Aggiornamenti alle API e alle CLI di EC2

Per le nuove istanze, puoi utilizzare l'RunInstancesAPI per avviare nuove istanze che richiedono l'uso di IMDSv2. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.

Per le istanze esistenti, puoi utilizzare l'ModifyInstanceMetadataOptionsAPI per richiedere l'uso di IMDSv2. Per ulteriori informazioni, consulta Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti.

Per richiedere l'utilizzo di IMDSv2 in tutte le nuove istanze avviate dai gruppi Auto Scaling, i gruppi Auto Scaling possono utilizzare un modello di avvio o una configurazione di avvio. Quando crei un modello di avvio o una configurazione di avvio, devi configurare i parametri `MetadataOptions` per richiedere l'utilizzo di IMDSv2. Il gruppo con scalabilità automatica avvia le nuove istanza tramite il nuovo modello di avvio o configurazione di avvio, senza coinvolgere le istanze esistenti. Per le istanze esistenti in un gruppo Auto Scaling, è possibile utilizzare l'API per richiedere ModifyInstanceMetadataOptionsl'uso di IMDSv2 sulle istanze esistenti oppure terminare le istanze e il gruppo Auto Scaling lancerà nuove istanze sostitutive con le impostazioni delle opzioni dei metadati dell'istanza definite nel nuovo modello di avvio o nella nuova configurazione di avvio.

Usa un'AMI che configura IMDSv2 per impostazione predefinita

Quando avvii un'istanza, puoi configurarla automaticamente per l'uso di IMDSv2 per impostazione predefinita (il parametro `HttpTokens` è impostato su `required`) avviandola con un'AMI configurata con il parametro `ImdsSupport` impostato su `v2.0`. È possibile impostare il `ImdsSupport` parametro su `v2.0` quando si registra l'AMI utilizzando il comando CLI register-image oppure modificare un'AMI esistente utilizzando il comando CLI. modify-image-attribute Per ulteriori informazioni, consulta Configurazione dell'AMI.

Policy IAM e SCP

È possibile utilizzare una policy IAM o una policy di controllo dei AWS Organizations servizi (SCP) per controllare gli utenti nel modo seguente:

- Non è possibile avviare un'istanza utilizzando l'RunInstancesAPI a meno che l'istanza non sia configurata per utilizzare IMDSv2.
- Impossibile modificare un'istanza in esecuzione utilizzando l'ModifyInstanceMetadataOptionsAPI per riattivare IMDSv1.

La policy IAM o SCP deve contenere le chiavi di condizione IAM indicate di seguito:

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Se un parametro nell'API o nella CLI non corrisponde allo stato specificato nella policy che contiene la chiave di condizione, la chiamata dell'API o della CLI non riesce e viene restituita la risposta `UnauthorizedOperation`.

Inoltre, puoi scegliere un livello aggiuntivo di protezione per imporre la modifica da IMDSv1 a IMDSv2. A livello di gestione degli accessi rispetto alle API richiamate tramite le credenziali EC2 Role, puoi utilizzare una nuova chiave di condizione nelle policy IAM o AWS Organizations nelle policy di controllo dei servizi (SCP). In particolare, utilizzando la chiave di condizione della policy `ec2:RoleDelivery` con il valore `2.0` nelle policy IAM, le chiamate dell'API effettuate con le credenziali del ruolo EC2 ottenute da IMDSv1 riceveranno una risposta `UnauthorizedOperation`. Lo stesso può essere ottenuto su scala più ampia con tale condizione richiesta da un SCP. Ciò assicura che le credenziali distribuite tramite IMDSv1 non possano di fatto essere utilizzate per chiamare API perché le eventuali chiamate API che non corrispondono alla condizione specificata riceveranno un errore `UnauthorizedOperation`.

Per esempi di policy IAM, consulta Utilizzo dei metadati delle istanze. Per ulteriori informazioni sulle SCP, consulta Service Control Policies (Policy di controllo dei servizi) nella Guida per l'utente di AWS Organizations .

Percorso consigliato per richiedere IMDSv2

Utilizzando gli strumenti precedenti, ti consigliamo di seguire questo percorso per eseguire la transizione a IMDSv2.

Fase 1: all'inizio

Aggiorna gli SDK, le CLI e il software che utilizza credenziali del ruolo sulle istanze EC2 a versioni compatibili con IMDSv2. Per informazioni sull'aggiornamento della CLI, consulta Aggiornamento all'ultima versione della AWS CLI nella Guida per l'utente di AWS Command Line Interface .

Quindi, modifica il software che accede direttamente ai metadati dell'istanza (in altre parole, che non utilizza un SDK) utilizzando le richieste IMDSv2. Puoi utilizzare IMDS Packet Analyzer per identificare il software da modificare per utilizzare le richieste IMDSv2.

Fase 2: monitoraggio dell'avanzamento della transizione

Tieni traccia dei progressi della transizione utilizzando la metrica. CloudWatch `MetadataNoToken` Tale parametro mostra il numero di chiamate IMDSv1 al servizio di metadati dell'istanza (IMDS) nelle istanze. Per ulteriori informazioni, consulta Parametri dell'istanza.

Fase 3: quando l'utilizzo di IMDSv1 è pari a zero

Quando la CloudWatch metrica `MetadataNoToken` registra un utilizzo pari a zero per IMDSv1, le istanze sono pronte per la transizione completa all'utilizzo di IMDSv2. In questa fase, puoi fare quanto segue:

- Account predefinito

  È possibile impostare IMDSv2 in modo che sia obbligatorio come account predefinito. All'avvio di un'istanza, la configurazione dell'istanza viene automaticamente impostata sui valori predefiniti dell'account.

  Per impostare l'account predefinito, procedi come segue:

  - Console Amazon EC2: nella dashboard EC2, in Attributi dell'account, protezione dei dati e sicurezza, per le impostazioni predefinite IMDS, imposta il servizio di metadati dell'istanza su Enabled e la versione dei metadati solo su V2 (token richiesto). Per ulteriori informazioni, consulta Imposta IMDSv2 come predefinito per l'account.
  - AWS CLI: utilizzate il comando modify-instance-metadata-defaultsCLI e specificate `--http-tokens required` e. `--http-put-response-hop-limit 2`

- Nuove istanze

  Quando avvii una nuova istanza, puoi effettuare le operazioni seguenti:

  - Console di Amazon EC2: nella procedura guidata di avvio dell'istanza, imposta Metadata accessible (Metadati accessibili) su Enabled (Abilitato) e Metadata version (Versione metadati) su V2 only (token required) (Solo V2 [token richiesto]). Per ulteriori informazioni, consulta Configurazione dell'istanza all'avvio.
  - AWS CLI: utilizzate il comando CLI run-instances e specificate che IMDSv2 è obbligatorio.

- Istanze esistenti

  Per le istanze esistenti, procedi come indicato di seguito:

  - Console Amazon EC2: seleziona l'istanza nella pagina Istanze, scegli Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza e, per IMDSv2, scegli Obbligatorio. Per ulteriori informazioni, consulta Richiesta dell'uso di IMDSv2.
  - AWS CLI: utilizzare il comando modify-instance-metadata-optionsCLI per specificare che deve essere utilizzato solo IMDSv2.

Puoi modificare le opzioni dei metadati dell'istanza nelle istanze in esecuzione, senza dover riavviare le istanze dopo aver apportato le modifiche.

Fase 4: verifica se le istanze hanno eseguito la transizione a IMDSv2

Puoi verificare se alcune istanze non sono ancora configurate per l'utilizzo di IMDSv2, in altre parole, se IMDSv2 è ancora configurato come `optional`. Se alcune istanze sono ancora configurate come `optional`, puoi modificare le opzioni dei metadati dell'istanza per rendere IMDSv2 `required` ripetendo la fase 3 precedente.

Per filtrare le istanze:

- Console Amazon EC2: nella pagina Istanze, filtra le istanze utilizzando il filtro IMDSv2 = facoltativo. Per ulteriori informazioni sul filtro, consulta Filtrare le risorse mediante la console. Puoi anche vedere se IMDSv2 è obbligatorio o facoltativo per ogni istanza: nella finestra Preferenze, attiva IMDSv2 per aggiungere la colonna IMDSv2 alla tabella Istanze.
- AWS CLI: utilizza il comando CLI describe-instances e filtra per `metadata-options.http-tokens = optional`, come mostrato:

```
aws ec2 describe-instances --filters "Name=metadata-options.http-
tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --output
 text
```

Fase 5: quando tutte le istanze hanno eseguito la transizione a IMDSv2

Le chiavi di condizione `ec2:MetadataHttpTokensec2:MetadataHttpPutResponseHopLimit`, e `ec2:MetadataHttpEndpoint` IAM possono essere utilizzate per controllare l'uso delle ModifyInstanceMetadataOptionsAPI RunInstancese delle CLI corrispondenti. Se viene creata una policy e un parametro nella chiamata API non corrisponde allo stato specificato nella policy utilizzando la chiave di condizione, la chiamata all'API o alla CLI non va a buon e viene restituita la risposta `Unauthorized0peration`. Per esempi di policy IAM, consulta Utilizzo dei metadati delle istanze.

Inoltre, dopo aver disabilitato IMDSv1, puoi utilizzare la `MetadataNoTokenRejected` CloudWatch metrica per tenere traccia del numero di volte in cui una chiamata IMDSv1 è stata tentata e rifiutata. Se, dopo aver disabilitato IMDSv1, il software non funziona correttamente e la

`MetadataNoTokenRejected` metrica registra le chiamate IMDSv1, è probabile che questo software debba essere aggiornato per utilizzare IMDSv2.

Utilizzo di un SDK AWS supportato

Per utilizzare IMDSv2, le istanze EC2 devono utilizzare una versione SDK che supporti l'utilizzo di IMDSv2. AWS Le versioni più recenti di tutti gli SDK supportano l'utilizzo di IMDSv2. AWS

> **Important**
>
> Ti consigliamo di rimanere al passo con i nuovi rilasci degli SDK per poter usufruire delle funzionalità, degli aggiornamenti di sicurezza e delle dipendenze sottostanti più recenti. L'uso continuato di una versione SDK non supportata è sconsigliato ed è a tua discrezione. Per ulteriori informazioni, consulta la pagina Policy di manutenzione degli SDK e degli strumenti AWS nella Guida di riferimento degli SDK e degli strumenti AWS .

Le seguenti sono le versioni minime che supportano l'uso di IMDSv2:

- AWS CLI - 1.16.289
- AWS Tools for Windows PowerShell – 4,0.1.0
- AWS SDK for .NET - 3.3.634.1
- AWS SDK for C++ - 1.7.229
- AWS SDK for Go - 1.25.38
- AWS SDK per Go v2 — 0.19.0
- AWS SDK for Java - 1.11.678
- AWS SDK for Java 2.x - 2.10.21
- AWS SDK per in Node.js — 2.722.0 JavaScript
- AWS SDK for PHP - 3.147.7
- AWS SDK per Python (Botocore) — 1.13.25
- AWS SDK for Python (Boto3) - 1.12.6
- AWS SDK for Ruby - 3.79.0

Configura le opzioni dei metadati dell'istanza

Il servizio di metadati dell'istanza (IMDS) viene eseguito localmente su ogni istanza EC2. Le opzioni relative ai metadati dell'istanza si riferiscono a un insieme di configurazioni che controllano l'accessibilità e il comportamento dell'IMDS su un'istanza EC2.

Puoi configurare le seguenti opzioni di metadati dell'istanza su ogni istanza:

Servizio di metadati delle istanze (IMDS): | `enabled` `disabled`

> È possibile abilitare o disabilitare l'IMDS su un'istanza. Se disabilitato, tu o qualsiasi codice non sarete in grado di accedere ai metadati dell'istanza sull'istanza.
>
> L'IMDS ha due endpoint su un'istanza: IPv4 (`169.254.169.254`) e IPv6 (). `[fd00:ec2::254]` Quando si abilita l'IMDS, l'endpoint IPv4 viene abilitato automaticamente. Se desideri abilitare l'endpoint IPv6, devi farlo in modo esplicito.

Endpoint IPv6 IMDS: | `enabled` `disabled`

> È possibile abilitare in modo esplicito l'endpoint IMDS IPv6 su un'istanza. Quando l'endpoint IPv6 è abilitato, l'endpoint IPv4 rimane abilitato. L'endpoint IPv6 è supportato solo su istanze create sul sistema AWS Nitro e in una sottorete supportata da IPv6 (dual stack o solo IPv6).

Versione **`IMDSv1 or IMDSv2 (token optional)`** dei metadati: | `IMDSv2 only (token required)`

> Quando si richiedono i metadati dell'istanza, le chiamate IMDSv2 richiedono un token. Le chiamate IMDSv1 non richiedono un token. È possibile configurare un'istanza per consentire le chiamate IMDSv1 o IMDSv2 (dove un token è facoltativo) o per consentire solo le chiamate IMDSv2 (dove è richiesto un token).

Limite dell'hop di risposta ai metadati: — 1 `64`

> Il limite di hop è il numero di hop di rete che la risposta PUT è autorizzata a effettuare. È possibile impostare il limite di hop su un minimo 1 e un massimo di`64`. In un ambiente contenitore, consigliamo di impostare il limite di hop su`2`. Per ulteriori informazioni, consulta Considerazioni.

Accesso ai tag nei metadati dell'istanza: | `enabled` `disabled`

> È possibile abilitare o disabilitare l'accesso ai tag dell'istanza dai metadati dell'istanza. Per ulteriori informazioni, consulta Utilizzo dei tag dell'istanza nei metadati dell'istanza.

Dove configurare le opzioni dei metadati dell'istanza

Le opzioni dei metadati delle istanze possono essere configurate a diversi livelli, come segue:

- Account: è possibile impostare valori predefiniti per le opzioni dei metadati dell'istanza a livello di account per ciascuna di esse. Regione AWS All'avvio di un'istanza, le opzioni dei metadati dell'istanza vengono impostate automaticamente sui valori a livello di account. Puoi modificare questi valori al momento del lancio. I valori predefiniti a livello di account non influiscono sulle istanze esistenti.
- AMI: è possibile impostare il `imds-support` parametro su `v2.0` quando si registra o si modifica un AMI. Quando un'istanza viene avviata con questa AMI, la versione dei metadati dell'istanza viene impostata automaticamente su IMDSv2 e il limite di hop è impostato su 2.
- Istanza: puoi modificare tutte le opzioni dei metadati dell'istanza su un'istanza all'avvio, ignorando le impostazioni predefinite. È inoltre possibile modificare le opzioni dei metadati dell'istanza dopo l'avvio su un'istanza in esecuzione o interrotta. Tieni presente che le modifiche possono essere limitate da una policy IAM o SCP.

Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze e Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti.

Ordine di precedenza, ad esempio le opzioni relative ai metadati

Il valore per ogni opzione di metadati dell'istanza viene determinato all'avvio dell'istanza, seguendo un ordine gerarchico di precedenza. La gerarchia, con la precedenza più alta nella parte superiore, è la seguente:

- Precedenza 1: configurazione dell'istanza all'avvio: i valori possono essere specificati nel modello di avvio o nella configurazione dell'istanza. Tutti i valori qui specificati sostituiscono i valori specificati a livello di account o nell'AMI.
- Precedenza 2: Impostazioni dell'account: se un valore non è specificato all'avvio dell'istanza, viene determinato dalle impostazioni a livello di account (impostate per ciascuna di esse). Regione AWS Le impostazioni a livello di account includono un valore per ogni opzione di metadati o non indicano alcuna preferenza.
- Precedenza 3: configurazione AMI: se un valore non è specificato all'avvio dell'istanza o a livello di account, viene determinato dalla configurazione AMI. Questo vale solo per gli eventi `HttpTokens` e `HttpPutResponseHopLimit`.

Ogni opzione di metadati viene valutata separatamente. L'istanza può essere configurata con una combinazione di configurazione diretta dell'istanza, impostazioni predefinite a livello di account e configurazione dall'AMI.

È possibile modificare il valore di qualsiasi opzione di metadati dopo l'avvio su un'istanza in esecuzione o interrotta, a meno che le modifiche non siano limitate da una policy IAM o SCP.

Determinare i valori per le opzioni di metadati — Esempio 1

In questo esempio, un'istanza EC2 viene lanciata in una regione in cui `HttpPutResponseHopLimit` è impostata a `1` livello di account. L'AMI specificato è `ImdsSupport` impostato su`v2.0`. Nessuna opzione di metadati viene specificata direttamente sull'istanza al momento del lancio. L'istanza viene avviata con le seguenti opzioni di metadati:

```
"MetadataOptions": {
    ...
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 1,
    ...
```

Questi valori sono stati determinati come segue:

- Nessuna opzione di metadati specificata all'avvio: durante l'avvio dell'istanza, i valori specifici per le opzioni di metadati non venivano forniti né nei parametri di avvio dell'istanza né nel modello di avvio.
- Le impostazioni dell'account hanno la precedenza successiva: in assenza di valori specifici specificati all'avvio, le impostazioni a livello di account all'interno della Regione hanno la precedenza. Ciò significa che vengono applicati i valori predefiniti configurati a livello di account. In questo caso, `HttpPutResponseHopLimit` era impostato su`1`.
- Le impostazioni AMI hanno l'ultima priorità: in assenza di un valore specifico specificato all'avvio o a livello di account per `HttpTokens` (la versione dei metadati dell'istanza), viene applicata l'impostazione AMI. In questo caso, l'impostazione AMI ha `ImdsSupport: v2.0` determinato che `HttpTokens` era impostata su`required`. Tieni presente che, sebbene l'impostazione AMI `ImdsSupport: v2.0` sia progettata per essere impostata`HttpPutResponseHopLimit: 2`, è stata sostituita dall'impostazione a livello di account`HttpPutResponseHopLimit: 1`, che ha la precedenza maggiore.

Determinare i valori per le opzioni relative ai metadati — Esempio 2

In questo esempio, l'istanza EC2 viene avviata con le stesse impostazioni del precedente Esempio 1, ma `HttpTokens` impostata `optional` direttamente sull'istanza al momento dell'avvio. L'istanza viene avviata con le seguenti opzioni di metadati:

```
"MetadataOptions": {
    ...
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    ...
```

Il valore di `HttpPutResponseHopLimit` è determinato nello stesso modo dell'Esempio 1. Tuttavia, il valore per `HttpTokens` è determinato come segue: le opzioni di metadati configurate sull'istanza al momento del lancio hanno la precedenza. Anche se l'AMI è stata configurata con `ImdsSupport: v2.0` (in altre parole, `HttpTokens` è impostata su`required`), il valore specificato nell'istanza all'avvio (`HttpTokens`impostato su`optional`) aveva la precedenza.

Imposta la versione dei metadati dell'istanza

Quando viene avviata un'istanza, il valore per la versione dei metadati dell'istanza è o`IMDSv1 or IMDSv2 (token optional)`. `IMDSv2 only (token required)`

All'avvio dell'istanza, è possibile specificare manualmente il valore per la versione dei metadati o utilizzare il valore predefinito. Se specificate manualmente il valore, esso sostituisce qualsiasi valore predefinito. Se si sceglie di non specificare manualmente il valore, questo verrà determinato da una combinazione di impostazioni predefinite, come indicato nella tabella seguente.

La tabella mostra come la versione dei metadati per un'istanza all'avvio (indicata dalla configurazione dell'istanza risultante nella colonna 4) è determinata dalle impostazioni ai diversi livelli di configurazione. L'ordine di precedenza va da sinistra a destra, dove la prima colonna ha la precedenza più alta, come segue:

- Colonna 1: parametro di avvio: rappresenta l'impostazione sull'istanza specificata manualmente all'avvio.
- Colonna 2: Livello di account predefinito: rappresenta l'impostazione dell'account.
- Colonna 3: AMI predefinito: rappresenta l'impostazione sull'AMI.

Parametro di avvio	Livello di account predefinito	AMI predefinito	Configurazione dell'istanza risultante
Solo V2 (token richiesto)	Nessuna preferenza	Solo V2	Solo V2
Solo V2 (token richiesto)	Solo V2	Solo V2	Solo V2
Solo V2 (token richiesto)	V1 o V2	Solo V2	Solo V2
V1 o V2 (token opzionale)	Nessuna preferenza	Solo V2	V1 o V2
V1 o V2 (token opzionale)	Solo V2	Solo V2	V1 o V2
V1 o V2 (token opzionale)	V1 o V2	Solo V2	V1 o V2
Non impostato	Nessuna preferenza	Solo V2	Solo V2
Non impostato	Solo V2	Solo V2	Solo V2
Non impostato	V1 o V2	Solo V2	V1 o V2
Solo V2 (token richiesto)	Nessuna preferenza	null	Solo V2
Solo V2 (token richiesto)	Solo V2	null	Solo V2
Solo V2 (token richiesto)	V1 o V2	null	Solo V2
V1 o V2 (token opzionale)	Nessuna preferenza	null	V1 o V2

Parametro di avvio	Livello di account predefinito	AMI predefinito	Configurazione dell'istanza risultante
V1 o V2 (token opzionale)	Solo V2	null	V1 o V2
V1 o V2 (token opzionale)	V1 o V2	null	V1 o V2
Non impostato	Nessuna preferenza	null	V1 o V2
Non impostato	Solo V2	null	Solo V2
Non impostato	V1 o V2	null	V1 o V2

Utilizza le chiavi di condizione IAM per limitare le opzioni dei metadati delle istanze

Puoi utilizzare le chiavi delle condizioni IAM in una policy IAM o in SCP come segue:

- Consentire il lancio di un'istanza solo se è configurata per richiedere l'uso di IMDSv2
- Limitare il numero di hop consentiti
- Disattivazione dell'accesso ai metadati dell'istanza

Attività

- Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze
- Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti

> **Note**
>
> È opportuno procedere con cautela e condurre test accurati prima di apportare qualsiasi modifica. Prendi nota di quanto segue:
>
> - Se imponi l'uso di IMDSv2, applicazioni o agenti che utilizzano IMDSv1 per l'accesso ai metadati dell'istanza verranno interrotti.
> - Se disattivi tutto l'accesso ai metadati dell'istanza, applicazioni o agenti il cui funzionamento si basa sull'accesso ai metadati dell'istanza verranno interrotti.

- Per IMDSv2, devi utilizzare `/latest/api/token` durante il recupero del token.
- (Solo Windows) Se la PowerShell versione in uso è precedente alla 4.0, è necessario eseguire l'aggiornamento a Windows Management Framework 4.0 per richiedere l'uso di IMDSv2.

Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze

È possibile configurare le seguenti opzioni di metadati delle istanze per le nuove istanze.

Opzioni

- Richiesta dell'uso di IMDSv2
- Abilita gli endpoint IMDS IPv4 e IPv6
- Disattivazione dell'accesso ai metadati dell'istanza

Richiesta dell'uso di IMDSv2

È possibile utilizzare i seguenti metodi per richiedere l'uso di IMDSv2 sulle nuove istanze.

Richiesta di IMDSv2

- Imposta IMDSv2 come predefinito per l'account
- Configurazione dell'istanza all'avvio
- Configurazione dell'AMI
- Utilizzo di una policy IAM

Imposta IMDSv2 come predefinito per l'account

È possibile impostare la versione predefinita per l'Instance Metadata Service (IMDS) a livello di account per ciascuno di essi. Regione AWS Ciò significa che quando si avvia una nuova istanza, la versione dei metadati dell'istanza viene automaticamente impostata sul valore predefinito a livello di account. Tuttavia, è possibile sovrascrivere manualmente il valore all'avvio o dopo l'avvio. Per ulteriori informazioni su come le impostazioni a livello di account e le sostituzioni manuali influiscono su un'istanza, consulta. Ordine di precedenza, ad esempio le opzioni relative ai metadati

> **Note**
>
> L'impostazione dell'impostazione predefinita a livello di account non ripristina le istanze esistenti. Ad esempio, se si imposta l'impostazione predefinita a livello di account su IMDSv2, le eventuali istanze esistenti impostate su IMDSv1 non vengono influenzate. Se si desidera modificare il valore sulle istanze esistenti, è necessario modificare manualmente il valore sulle istanze stesse.

È possibile impostare l'account predefinito per la versione dei metadati dell'istanza su IMDSv2 in modo che tutte le nuove istanze nell'account vengano avviate con IMDSv2 e IMDSv1 vengano disabilitate. Con questo account predefinito, quando si avvia un'istanza, i valori predefiniti per l'istanza sono i seguenti:

- Console: la versione dei metadati è impostata solo su V2 (è richiesto il token) e il limite dell'hop di risposta dei metadati è impostato su 2.
- AWS CLI: `HttpTokens` è impostato su `required` ed `HttpPutResponseHopLimit` è impostato su. 2

> **Note**
>
> Prima di impostare l'account predefinito su IMDSv2, assicurati che le tue istanze non dipendano da IMDSv1. Per ulteriori informazioni, consulta Percorso consigliato per richiedere IMDSv2.

Console

Per impostare IMDSv2 come predefinito per l'account per la regione specificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione scegliere EC2 Dashboard (Pannello di controllo EC2).
4. In Attributi dell'account, scegli Protezione e sicurezza dei dati.
5. Accanto alle impostazioni predefinite IMDS, scegli Gestisci.

6. Nella pagina Gestisci le impostazioni predefinite IMDS, procedi come segue:

   a. Ad esempio, servizio di metadati, scegli Abilitato.

   b. Per Metadata version (Versione metadati), seleziona V2 only (token required) (Solo V2 [token richiesto]).

   c. Per il limite dell'hop di risposta ai metadati, specifica 2 se le istanze ospiteranno contenitori. Altrimenti, seleziona Nessuna preferenza. Quando non viene specificata alcuna preferenza, all'avvio il valore predefinito è 2 se l'AMI richiede IMDSv2; in caso contrario, il valore predefinito è 1.

   d. Scegli Aggiorna.

AWS CLI

Per impostare IMDSv2 come predefinito per l'account per la regione specificata

Usa il modify-instance-metadata-defaultscomando e specifica la regione in cui modificare le impostazioni a livello di account IMDS. Includi `--http-tokens` set to `required` e `--http-put-response-hop-limit` imposta 2 se le tue istanze ospiteranno contenitori. Altrimenti, specifica di non `-1` indicare alcuna preferenza. Quando viene specificata `-1` (nessuna preferenza), all'avvio, il valore predefinito è 2 se l'AMI richiede IMDSv2; in caso contrario, il valore predefinito è. 1

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-put-response-hop-limit 2
```

Output previsto

```
{
    "Return": true
}
```

Per visualizzare le impostazioni predefinite dell'account per le opzioni dei metadati dell'istanza per la regione specificata

Utilizzate il get-instance-metadata-defaultscomando e specificate la regione.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Output di esempio

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 2
    }
}
```

PowerShell

Per impostare IMDSv2 come predefinito per l'account per la regione specificata

Usa il Edit-EC2InstanceMetadataDefaultcomando e specifica la regione in cui modificare le impostazioni a livello di account IMDS. Includi `-HttpToken` set to `required` e `-HttpPutResponseHopLimit` imposta 2 se le tue istanze ospiteranno contenitori. Altrimenti, specifica di non `-1` indicare alcuna preferenza. Quando viene specificata `-1` (nessuna preferenza), all'avvio, il valore predefinito è 2 se l'AMI richiede IMDSv2; in caso contrario, il valore predefinito è. 1

```
Edit-EC2InstanceMetadataDefault `
    -Region us-east-1 `
    -HttpToken required `
    -HttpPutResponseHopLimit 2
```

Output previsto

```
True
```

Per visualizzare le impostazioni predefinite dell'account per le opzioni dei metadati dell'istanza per la regione specificata

Utilizzate il Get-EC2InstanceMetadataDefaultcomando e specificate la regione.

```
Get-EC2InstanceMetadataDefault -Region us-east-1 | Format-List
```

Output di esempio

```
HttpEndpoint            :
HttpPutResponseHopLimit : 2
HttpTokens              : required
InstanceMetadataTags    :
```

Configurazione dell'istanza all'avvio

Quando avvii un'istanza, puoi configurare l'istanza in modo che richieda l'uso di IMDSv2 configurando i campi seguenti:

- Console di Amazon EC2: imposta Metadata version (Versione metadati) su V2 only (token required) (Solo V2 [token richiesto]).
- AWS CLI: imposta `HttpTokens` su `required`.

Quando specifichi che IMDSv2 è obbligatorio, devi abilitare anche l'endpoint del servizio di metadati dell'istanza (IMDS) impostando Metadati accessibili su Abilitato (console) o `HttpEndpoint` su `enabled` (AWS CLI).

In un ambiente contenitore, quando è richiesto IMDSv2, si consiglia di impostare il limite di hop su. 2 Per ulteriori informazioni, consulta Considerazioni.

New console

Per richiedere l'uso di IMDSv2 su una nuova istanza

- Quando avvii una nuova istanza nella console Amazon EC2, espandi Advanced details (Dettagli avanzati) e procedi come segue:
  - Per Metadata accessible (Metadati accessibili), scegli Enabled (Abilitato).
  - Per Metadata version (Versione metadati), seleziona V2 only (token required) (Solo V2 [token richiesto]).
  - (Ambiente contenitore) Per il limite dell'hop di risposta ai metadati, scegliete 2.

  Per ulteriori informazioni, consulta Dettagli avanzati.

Old console

Per richiedere l'uso di IMDSv2 su una nuova istanza

- Quando si avvia una nuova istanza nella console Amazon EC2, selezionare le opzioni seguenti nella pagina Configure Instance Details (Configura i dettagli dell'istanza:
  - In Advanced Details (Dettagli avanzati), per Metadata accessible (Metadati accessibili), selezionare Enabled (Abilitato).
  - Per Metadata version (Versione metadati), selezionare V2 (token required) (V2 [token richiesto]).

Per ulteriori informazioni, consulta Fase 3: configurare i dettagli dell'istanza.

AWS CLI

Per richiedere l'uso di IMDSv2 su una nuova istanza

L'esempio run-instances avvia un'istanza `c6i.large` con `--metadata-options` impostato su `HttpTokens=required`. Quando si specifica un valore per `HttpTokens`, è necessario impostare `HttpEndpoint` anche su `enabled`. Poiché l'intestazione del token sicuro è impostata su `required` per le richieste di recupero dei metadati, l'istanza deve utilizzare IMDSv2 quando si richiedono i metadati dell'istanza.

In un ambiente contenitore, quando è richiesto IMDSv2, consigliamo di impostare il limite di hop su with. 2 `HttpPutResponseHopLimit=2`

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
 ...
    --metadata-options
 "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

Per richiedere l'uso di IMDSv2 su una nuova istanza

Il seguente esempio di New-EC2Instancecmdlet avvia un'`c6i.large`istanza con `MetadataOptions_HttpEndpoint` set to e il parametro to. `enabled`

`MetadataOptions_HttpTokens` `required` Quando si specifica un valore per `HttpTokens`, è necessario impostare `HttpEndpoint` anche su `enabled`. Poiché l'intestazione del token sicuro è impostata su `required` per le richieste di recupero dei metadati, l'istanza deve utilizzare IMDSv2 quando si richiedono i metadati dell'istanza.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpTokens required
```

AWS CloudFormation

Per specificare le opzioni di metadati utilizzate da un'istanza AWS CloudFormation, consultate la AWS::EC2::LaunchTemplate MetadataOptionsproprietà nella Guida per l'utente.AWS CloudFormation

Configurazione dell'AMI

Quando registri una nuova AMI o modifichi un'AMI esistente, puoi impostare il parametro `imds-support` su `v2.0`. Per le istanze avviate da questa AMI, Metadata version (Versione metadati) sarà impostato su V2 only (token required) (Solo V2 [token richiesto]) (console) o `HttpTokens` sarà impostato su `required` (AWS CLI). Con queste impostazioni, l'istanza richiede l'uso di IMDSv2 quando vengono chiesti i metadati dell'istanza.

Tieni presente che quando imposti `imds-support` su `v2.0`, anche per le istanze avviate da questa AMI Metadata response hop limit (Limite hop risposta metadati) (console) o `http-put-response-hop-limit` (AWS CLI) sarà impostato su 2.

> **Important**
>
> Non utilizzate questo parametro a meno che il software AMI non supporti IMDSv2. Dopo aver impostato il valore su `v2.0`, non è possibile annullare l'operazione. L'unico modo per "reimpostare" l'AMI consiste nel creare una nuova AMI dallo snapshot sottostante.

Per configurare una nuova AMI per IMDSv2

Utilizza uno dei seguenti metodi per configurare una nuova AMI per IMDSv2.

AWS CLI

L'esempio register-image seguente registra un'AMI utilizzando lo snapshot specificato di un volume root EBS come dispositivo `/dev/xvda`. Specifica `v2.0` per il parametro `imds-support`, in modo che le istanze avviate da tale AMI richiedano l'utilizzo di IMDSv2 quando si richiedono i metadati dell'istanza.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0123456789example} \
    --architecture x86_64 \
    --imds-support v2.0
```

PowerShell

Il seguente esempio di Register-EC2Imagecmdlet registra un AMI utilizzando l'istantanea specificata di un volume root EBS come dispositivo. `/dev/xvda` Specifica `v2.0` per il parametro `ImdsSupport`, in modo che le istanze avviate da tale AMI richiedano l'utilizzo di IMDSv2 quando si richiedono i metadati dell'istanza.

```
Import-Module AWS.Tools.EC2  # Required for Amazon.EC2.Model object creation.
Register-EC2Image `
    -Name 'my-image' `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping  (
    New-Object `
        -TypeName Amazon.EC2.Model.BlockDeviceMapping `
        -Property @{
        DeviceName = '/dev/xvda';
        EBS        = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property
 @{
                SnapshotId = 'snap-0123456789example';
                VolumeType = 'gp3'
                } )
        }  ) `
    -Architecture X86_64 `
    -ImdsSupport v2.0
```

Per configurare un'AMI esistente per IMDSv2

Utilizza uno dei metodi seguenti per configurare una nuova AMI per IMDSv2.

AWS CLI

L'modify-image-attributeesempio seguente modifica un AMI esistente solo per IMDSv2. Specifica `v2.0` per il parametro `imds-support`, in modo che le istanze avviate da tale AMI richiedano l'utilizzo di IMDSv2 quando si richiedono i metadati dell'istanza.

```
aws ec2 modify-image-attribute \
    --image-id ami-0123456789example \
    --imds-support v2.0
```

PowerShell

Il seguente esempio di Edit-EC2ImageAttributecmdlet modifica un AMI esistente solo per IMDSv2. Specifica `v2.0` per il parametro `imds-support`, in modo che le istanze avviate da tale AMI richiedano l'utilizzo di IMDSv2 quando si richiedono i metadati dell'istanza.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ImdsSupport 'v2.0'
```

Utilizzo di una policy IAM

Puoi creare una policy IAM che impedisce agli utenti di avviare nuove istanze a meno che non richiedano IMDSv2 sulla nuova istanza.

Uso forzato di IMDSv2 su tutte le nuove istanze tramite una policy IAM

Per garantire che tutti gli utenti possano avviare solo istanze che richiedono l'uso di IMDSv2 durante la richiesta di metadati dell'istanza, puoi specificare che la condizione per richiedere IMDSv2 deve essere soddisfatta prima di poter avviare un'istanza. Per un esempio di policy IAM, consulta Utilizzo dei metadati delle istanze.

Abilita gli endpoint IMDS IPv4 e IPv6

L'IMDS ha due endpoint su un'istanza: IPv4 () e IPv6 (). `169.254.169.254` `[fd00:ec2::254]` Quando si abilita l'IMDS, l'endpoint IPv4 viene abilitato automaticamente. L'endpoint IPv6 rimane disabilitato anche se si avvia un'istanza in una sottorete solo IPv6. Per abilitare l'endpoint IPv6, è necessario farlo in modo esplicito. Quando si abilita l'endpoint IPv6, l'endpoint IPv4 rimane abilitato.

È possibile abilitare l'endpoint IPv6 all'avvio dell'istanza o dopo.

Requisiti per l'abilitazione dell'endpoint IPv6

- Il tipo di istanza selezionato è basato sul sistema Nitro.AWS
- La sottorete selezionata supporta IPv6, dove la sottorete è dual stack o solo IPv6.

Utilizza uno dei seguenti metodi per avviare un'istanza con l'endpoint IMDS IPv6 abilitato.

New console

Per abilitare l'endpoint IMDS IPv6 all'avvio dell'istanza

- Avvia l'istanza nella console di Amazon EC2 con le opzioni specificate di seguito in Advanced details (Dettagli avanzati):
  - Per l'endpoint IPv6 dei metadati, scegli Abilitato.

Per ulteriori informazioni, consulta Dettagli avanzati.

AWS CLI

Per abilitare l'endpoint IPv6 IMDS all'avvio dell'istanza

L'esempio run-instances seguente avvia un'istanza `c6i.large` con l'endpoint IPv6 abilitato per IMDS. Per abilitare l'endpoint IPv6, per il parametro `--metadata-options` specifica `HttpProtocolIpv6=enabled`. Quando si specifica un valore per `HttpProtocolIpv6`, è necessario impostare `HttpEndpoint` anche su `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Per abilitare l'endpoint IPv6 IMDS all'avvio dell'istanza

Il seguente esempio di New-EC2Instancecmdlet avvia un'`c6i.large`istanza con l'endpoint IPv6 abilitato per l'IMDS. Per abilitare l'endpoint IPv6, specifica

`MetadataOptions_HttpProtocolIpv6` come `enabled`. Quando si specifica un valore per `MetadataOptions_HttpProtocolIpv6`, è necessario impostare `MetadataOptions_HttpEndpoint` anche su `enabled`.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpProtocolIpv6 enabled
```

Disattivazione dell'accesso ai metadati dell'istanza

È possibile disattivare l'accesso ai metadati dell'istanza disabilitando l'IMDS all'avvio di un'istanza. È possibile attivare l'accesso in un secondo momento riabilitando l'IMDS. Per ulteriori informazioni, consulta Attivazione dell'accesso ai metadati dell'istanza.

Important

È possibile scegliere di disabilitare l'IMDS all'avvio o dopo l'avvio. Se disabiliti l'IMDS all'avvio, quanto segue potrebbe non funzionare:

- Potresti non disporre dell'accesso SSH all'istanza. La `public-keys/0/openssh-key`, che è la chiave SSH pubblica dell'istanza, non sarà accessibile perché normalmente la chiave viene fornita dai metadati dell'istanza EC2 e l'accesso avviene tramite gli stessi.
- I dati utente EC2 non saranno disponibili e non verranno eseguiti all'avvio dell'istanza. I dati utente EC2 sono ospitati sull'IMDS. Se disabiliti l'IMDS, disattivi di fatto l'accesso ai dati utente.

Per accedere a questa funzionalità, è possibile riabilitare l'IMDS dopo l'avvio.

New console

Disattivazione dell'accesso ai metadati dell'istanza all'avvio

- Avvia l'istanza nella console di Amazon EC2 con le opzioni specificate di seguito in Advanced details (Dettagli avanzati):

- Per Metadata accessible (Metadati accessibili), scegli Disabled (Disabilitato).

Per ulteriori informazioni, consulta Dettagli avanzati.

Old console

Disattivazione dell'accesso ai metadati dell'istanza all'avvio

- Avvia l'istanza nella console di Amazon EC2 con l'opzione seguente selezionata nella pagina Configura dettagli istanza:
  - In Advanced Details (Dettagli avanzati), per Metadata accessible (Metadati accessibili), selezionare Disabled (Disabilitato).

Per ulteriori informazioni, consulta Fase 3: configurare i dettagli dell'istanza.

AWS CLI

Disattivazione dell'accesso ai metadati dell'istanza all'avvio

Avvia l'istanza con `--metadata-options` impostato su `HttpEndpoint=disabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

PowerShell

Disattivazione dell'accesso ai metadati dell'istanza all'avvio

Il seguente esempio di New-EC2InstanceCmdlet avvia un'istanza con set to. `MetadataOptions_HttpEndpoint` `disabled`

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint disabled
```

AWS CloudFormation

Per specificare le opzioni relative ai metadati per un'istanza che utilizza AWS CloudFormation, consultate la AWS::EC2::LaunchTemplate MetadataOptionsproprietà nella Guida per l'utente.AWS CloudFormation

Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti

Puoi modificare le opzioni dei metadati dell'istanza per le istanze esistenti.

Puoi inoltre creare una policy IAM che impedisce agli utenti di modificare le opzioni dei metadati dell'istanza in istanze esistenti. Per controllare quali utenti possono modificare le opzioni dei metadati dell'istanza, specifica una politica che impedisca a tutti gli utenti diversi dagli utenti con un ruolo specifico di utilizzare l'ModifyInstanceMetadataOptionsAPI. Per un esempio di policy IAM, consulta Utilizzo dei metadati delle istanze.

Esegui una query sulle opzioni dei metadati dell'istanza per le istanze esistenti

Puoi eseguire una query sulle opzioni dei metadati dell'istanza per le istanze esistenti utilizzando uno dei seguenti metodi.

Console

Esecuzione di query sulle opzioni dei metadati dell'istanza per un'istanza esistente tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Verifica le opzioni correnti dei metadati dell'istanza nella finestra di dialogo Modifica delle opzioni dei metadati dell'istanza.

AWS CLI

Per interrogare le opzioni dei metadati dell'istanza per un'istanza esistente utilizzando il AWS CLI

Utilizzare il comando della CLI describe-instances.

```
aws ec2 describe-instances \
    --instance-id i-1234567898abcdef0 \
    --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Per interrogare le opzioni dei metadati dell'istanza per un'istanza esistente, utilizzare gli strumenti per PowerShell

Utilizzare il Get-EC2Instancecmdlet.

```
(Get-EC2Instance `
    -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Richiesta dell'uso di IMDSv2

Utilizza uno dei metodi seguenti per modificare le opzioni dei metadati dell'istanza su un'istanza esistente, in modo da utilizzare IMDSv2 quando si richiedono i metadati dell'istanza. Quando è richiesto IMDSv2, non è possibile utilizzare IMDSv1.

> **Note**
>
> Prima di richiedere l'utilizzo di IMDSv2, assicurati che l'istanza non stia effettuando chiamate IMDSv1. La metrica tiene traccia delle chiamate IMDSv1. `MetadataNoToken` CloudWatch Quando non `MetadataNoToken` registra un utilizzo di IMDSv1 per un'istanza, l'istanza è pronta a richiedere IMDSv2.

Console

Per richiedere l'uso di IMDSv2 su un'istanza esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Nella finestra di dialogo Modifica opzioni dei metadati dell'istanza, esegui una delle operazioni indicate di seguito:

a. In Servizio di metadati dell'istanza, seleziona Abilita.

b. Per IMDSv2, scegli Obbligatorio.

c. Selezionare Salva.

AWS CLI

Per richiedere l'uso di IMDSv2 su un'istanza esistente

Utilizzate il comando modify-instance-metadata-optionsCLI e impostate il `http-tokens` parametro su. `required` Quando si specifica un valore per `http-tokens`, è necessario impostare `http-endpoint` anche su `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

PowerShell

Per richiedere l'uso di IMDSv2 su un'istanza esistente

Utilizzare il Edit-EC2InstanceMetadataOptioncmdlet e impostare il `HttpTokens` parametro su. `required` Quando si specifica un valore per `HttpTokens`, è necessario impostare `HttpEndpoint` anche su `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens required `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Ripristino dell'uso di IMDSv1

Se IMDSv2 è obbligatorio, IMDSv1 non funziona quando si richiedono i metadati dell'istanza. Al contrario, quando IMDSv2 è facoltativo, funzioneranno sia IMDSv2 che IMDSv1. Per ripristinare IMDSv1, quindi, è necessario rendere IMDSv2 facoltativo utilizzando uno dei metodi descritti di seguito.

Console

Per ripristinare l'uso di IMDSv1 su un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Nella finestra di dialogo Modifica opzioni dei metadati dell'istanza, esegui una delle operazioni indicate di seguito:

   a. In Servizio di metadati dell'istanza, assicurati che l'opzione Abilita sia selezionata.

   b. Per IMDSv2, scegli Facoltativo.

   c. Selezionare Salva.

AWS CLI

Per ripristinare l'uso di IMDSv1 su un'istanza

È possibile utilizzare il comando modify-instance-metadata-optionsCLI con `http-tokens` set to per `optional` ripristinare l'uso di IMDSv1 quando si richiedono i metadati dell'istanza.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

PowerShell

Per ripristinare l'uso di IMDSv1 su un'istanza

È possibile utilizzare il Edit-EC2InstanceMetadataOptioncmdlet con `HttpTokens` set to per ripristinare l'uso di IMDSv1 quando si richiedono `optional` i metadati dell'istanza.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens optional `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Modifica del limite di hop di risposta PUT

Per istanze esistenti, puoi modificare le impostazioni del limite di hop della risposta PUT.

Attualmente solo gli AWS SDK AWS CLI and supportano la modifica del limite dell'hop di risposta PUT.

AWS CLI

Per modificare il limite di hop di risposta PUT

Utilizzate il comando modify-instance-metadata-optionsCLI e impostate il `http-put-response-hop-limit` parametro sul numero di hop richiesto. Nell'esempio seguente, il limite di hop è impostato su `3`. Tieni presente che quando si specifica un valore per `http-put-response-hop-limit`, è necessario anche impostare `http-endpoint` su `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

PowerShell

Per modificare il limite di hop di risposta PUT

Utilizzare il Edit-EC2InstanceMetadataOptioncmdlet e impostare il `HttpPutResponseHopLimit` parametro sul numero di hop richiesto. Nell'esempio seguente, il limite di hop è impostato su `3`. Tieni presente che quando si specifica un valore per `HttpPutResponseHopLimit`, è necessario anche impostare `HttpEndpoint` su `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpPutResponseHopLimit 3 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Abilita gli endpoint IMDS IPv4 e IPv6

L'IMDS ha due endpoint su un'istanza: IPv4 () e IPv6 (). `169.254.169.254` `[fd00:ec2::254]` Quando si abilita l'IMDS, l'endpoint IPv4 viene abilitato automaticamente. L'endpoint IPv6 rimane

disabilitato anche se si avvia un'istanza in una sottorete solo IPv6. Per abilitare l'endpoint IPv6, è necessario farlo in modo esplicito. Quando si abilita l'endpoint IPv6, l'endpoint IPv4 rimane abilitato.

È possibile abilitare l'endpoint IPv6 all'avvio dell'istanza o dopo.

Requisiti per l'abilitazione dell'endpoint IPv6

- Il tipo di istanza selezionato è basato sul sistema Nitro.AWS
- La sottorete selezionata supporta IPv6, dove la sottorete è dual stack o solo IPv6.

Attualmente solo gli AWS SDK AWS CLI and supportano l'abilitazione dell'endpoint IPv6 IMDS dopo il lancio dell'istanza.

AWS CLI

Per abilitare l'endpoint IMDS IPv6 per la tua istanza

Utilizzate il comando modify-instance-metadata-optionsCLI e impostate il `http-protocol-ipv6` parametro su. `enabled` Tieni presente che quando si specifica un valore per `http-protocol-ipv6`, è necessario anche impostare `http-endpoint` su `enabled`.

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567898abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

PowerShell

Per abilitare l'endpoint IMDS IPv6 per la tua istanza

Utilizzare il Edit-EC2InstanceMetadataOptioncmdlet e impostare il parametro su. `HttpProtocolIpv6` `enabled` Tieni presente che quando si specifica un valore per `HttpProtocolIpv6`, è necessario anche impostare `HttpEndpoint` su `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpProtocolIpv6 enabled `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Attivazione dell'accesso ai metadati dell'istanza

Puoi attivare l'accesso ai metadati dell'istanza abilitando l'endpoint HTTP del servizio di metadati dell'istanza (IMDS), indipendentemente dalla versione in uso. Puoi invertire questa modifica in qualsiasi momento disabilitando l'endpoint HTTP.

Per attivare l'accesso ai metadati dell'istanza, utilizza uno dei metodi seguenti.

Console

Per attivare l'accesso ai metadati dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Nella finestra di dialogo Modifica opzioni dei metadati dell'istanza, esegui una delle operazioni indicate di seguito:
   a. In Servizio di metadati dell'istanza, seleziona Abilita.
   b. Selezionare Salva.

AWS CLI

Per attivare l'accesso ai metadati dell'istanza

Utilizzate il comando modify-instance-metadata-optionsCLI e impostate il `http-endpoint` parametro su. `enabled`

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint enabled
```

PowerShell

Per attivare l'accesso ai metadati dell'istanza

Utilizzare il Edit-EC2InstanceMetadataOptioncmdlet e impostare il `HttpEndpoint` parametro su. `enabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Disattivazione dell'accesso ai metadati dell'istanza

Puoi disattivare l'accesso ai metadati dell'istanza disabilitando l'endpoint HTTP del servizio di metadati dell'istanza (IMDS), indipendentemente dalla versione in uso. Puoi invertire questa modifica in qualsiasi momento abilitando l'endpoint HTTP.

Per disattivare l'accesso ai metadati dell'istanza, utilizza uno dei metodi seguenti.

Console

Come disattivare l'accesso ai metadati dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Nella finestra di dialogo Modifica opzioni dei metadati dell'istanza, esegui una delle operazioni indicate di seguito:
   a. In Servizio di metadati dell'istanza, deseleziona Abilita.
   b. Selezionare Salva.

AWS CLI

Come disattivare l'accesso ai metadati dell'istanza

Utilizzate il comando modify-instance-metadata-optionsCLI e impostate il `http-endpoint` parametro su. `disabled`

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint disabled
```

PowerShell

Come disattivare l'accesso ai metadati dell'istanza

Utilizzare il Edit-EC2InstanceMetadataOptioncmdlet e impostare il `HttpEndpoint` parametro su. `disabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint disabled).InstanceMetadataOptions
```

Recupero dei metadati dell'istanza

Dal momento che i metadati dell'istanza sono disponibili dall'istanza in esecuzione, non devi utilizzare la console Amazon EC2 o AWS CLI. Ciò può risultare utile quando sta scrivendo script da eseguire dall'istanza. Ad esempio, puoi accedere all'indirizzo IP locale dell'istanza dai metadati dell'istanza per gestire una connessione a un'applicazione esterna.

I metadati dell'istanza sono suddivisi in categorie. Per una descrizione di ciascuna categoria di metadati dell'istanza, consulta Categorie di metadati dell'istanza.

Per visualizzare tutte le categorie di metadati di istanza dall'interno di un'istanza in esecuzione, recupera i dati dai seguenti URI IPv4 o IPv6. Questi indirizzi IP sono indirizzi locali del collegamento e sono validi solo per l'istanza. Per ulteriori informazioni, consulta Indirizzi link local.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Prezzi

Non verrà addebitato alcun costo per le richieste HTTP utilizzate per recuperare i metadati dell'istanza e i dati utente.

Considerazioni

Per evitare problemi con il recupero dei metadati dell'istanza, considerate quanto segue.

Formato del comando

Il formato del comando è diverso, a seconda che si utilizzi IMDSv1 o IMDSv2. Per impostazione predefinita, puoi utilizzare entrambe le versioni dell'IMDS. Per richiedere l'utilizzo di IMDSv2, consulta Usa IMDSv2.

(IMDSv2) Se IMDSv2 è richiesto, IMDSv1 non funziona

Per verificare se IMDSv2 è richiesto, seleziona l'istanza per visualizzarne i dettagli. Il valore per IMDSv2 è Obbligatorio (è necessario utilizzare IMDSv2) o Facoltativo (è possibile utilizzare IMDSv2 o IMDSv1).

(/latest/api/tokenIMDSv2) Utilizzare per recuperare il token

L'invio di PUT richieste a qualsiasi percorso specifico della versione, ad esempio, comporta la restituzione da parte del servizio di metadati degli `/2021-03-23/api/token` errori 403 Forbidden. Questo è il comportamento previsto.

Supporto IPv6

Per recuperare i metadati dell'istanza utilizzando l'indirizzo IPv6, assicurati di abilitare e utilizzare al posto dell'indirizzo IPv4. `[fd00:ec2::254]` L'istanza deve essere creata sul sistema AWS Nitro e avviata in una sottorete che supporti IPv6.

(Windows) Crea AMI personalizzate utilizzando Windows Sysprep

Per garantire che IMDS funzioni quando si avvia un'istanza da un'AMI Windows personalizzata, l'AMI deve essere un'immagine standardizzata creata con Windows Sysprep. In caso contrario, l'IMDS non funzionerà. Per ulteriori informazioni, vedere. Creare un'AMI con Windows Sysprep

In un ambiente contenitore, imposta il limite di hop su 2

Gli AWS SDK utilizzano le chiamate IMDSv2 per impostazione predefinita. Se la chiamata IMDSv2 non riceve alcuna risposta, l'SDK ritenta la chiamata e, se ancora non riesce, utilizza IMDSv1. Ciò può comportare un ritardo, soprattutto in un ambiente del container. In un ambiente container, se il limite di hop è 1, la risposta IMDSv2 non viene restituita perché andare al container è considerato un hop di rete aggiuntivo. Per evitare il processo di fallback di IMDSv1 e il ritardo risultante, in un ambiente container si consiglia di impostare il limite di hop su 2. Per ulteriori informazioni, consulta Configura le opzioni dei metadati dell'istanza.

Versione dei metadati

Per evitare di dover aggiornare il codice ogni volta che Amazon EC2 rilascia una nuova build di metadati dell'istanza, ti consigliamo di utilizzare `latest` nel percorso e non nel numero di versione.

Risposte e messaggi di errore

Tutti i metadati dell'istanza vengono restituiti come testo (tipo di contenuto HTTP `text/plain`).

Una richiesta relativa a una risorsa di metadati specifica restituisce il valore appropriato o un codice di errore HTTP `404 - Not Found` se la risorsa non è disponibile.

Una richiesta relativa a una risorsa di metadati generica (l'URI termina con /) restituisce l'elenco delle risorse disponibili o un codice di errore HTTP `404 - Not Found` se la risorsa specificata non è disponibile. Le voci dell'elenco si trovano su righe distinte che terminano con caratteri di avanzamento riga (ASCII 10).

Per richieste effettuate mediante Servizio di metadati dell'istanza Versione 2, possono essere restituiti i seguenti codici di errore HTTP:

- `400 - Missing or Invalid Parameters` – La richiesta PUT non è valida.
- `401 - Unauthorized` – La richiesta GET utilizza un token non valido. L'operazione consigliata è quella di generare un nuovo token.
- `403 - Forbidden`: la richiesta non è consentita o l'IMDS è disattivato.

Esempi per IMDSv2

Esegui i seguenti esempi sulla tua istanza Amazon EC2 per recuperare i metadati dell'istanza per IMDSv2.

Nelle istanze Windows, puoi usare Windows PowerShell oppure puoi installare cURL o wget. Se installate uno strumento di terze parti su un'istanza di Windows, assicuratevi di leggere attentamente la documentazione di accompagnamento, poiché le chiamate e l'output potrebbero essere diversi da quelli descritti qui.

Esempi

- Recupero delle versioni disponibili dei metadati dell'istanza

- Recupero degli elementi di metadati di primo livello
- Ottieni i valori per gli elementi di metadati
- Recupero dell'elenco di chiavi pubbliche disponibili
- Visualizzazione dei formati in cui è disponibile la chiave pubblica 0
- Recupero della chiave pubblica 0 (nel formato di chiave OpenSSH)
- Recupero dell'ID della sottorete per un'istanza
- Ottenere i tag dell'istanza per un'istanza

Recupero delle versioni disponibili dei metadati dell'istanza

Questo esempio recupera le versioni disponibili dei metadati dell'istanza. Ogni versione fa riferimento a una build dei metadati dell'istanza quando sono state rilasciate nuove categorie di metadati dell'istanza. Le versioni di build dei metadati dell'istanza non sono correlate alle versioni dell'API di Amazon EC2. Le versioni precedenti sono disponibili in presenza di script basati sulla struttura e sulle informazioni presenti in una versione precedente.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Recupero degli elementi di metadati di primo livello

Questo esempio recupera gli elementi di metadati di primo livello. Per ulteriori informazioni sugli elementi della risposta, vedereCategorie di metadati dell'istanza.

Tieni presente che i tag sono inclusi in questo output solo se hai consentito l'accesso. Per ulteriori informazioni, consulta the section called “Per consentire l'accesso ai tag nei metadati delle istanze”.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
ami-id
```

```
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
```

```
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Ottieni i valori per gli elementi di metadati

Questi esempi ottengono i valori di alcuni degli elementi di metadati di primo livello ottenuti nell'esempio precedente. Queste richieste utilizzano il token memorizzato creato utilizzando il comando nell'esempio precedente. Il token non deve essere scaduto.

cURL

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Recupero dell'elenco di chiavi pubbliche disponibili

Questo esempio recupera l'elenco delle chiavi pubbliche disponibili.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Visualizzazione dei formati in cui è disponibile la chiave pubblica 0

Questo esempio mostra i formati in cui è disponibile la chiave pubblica 0.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Recupero della chiave pubblica 0 (nel formato di chiave OpenSSH)

Questo esempio recupera la chiave pubblica 0 (nel formato di chiave OpenSSH).

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
```

```
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Recupero dell'ID della sottorete per un'istanza

In questo esempio viene recuperato l'ID della sottorete per un'istanza.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Ottenere i tag dell'istanza per un'istanza

Questi esempi accedono ai tag di un'istanza. È necessario consentire l'accesso ai tag prima di poter utilizzare questi esempi.

cURL

Questo esempio ottiene tutte le chiavi dei tag per un'istanza.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

In questo esempio viene ottenuto il valore della `Name` chiave ottenuta nell'esempio precedente. La richiesta IMDSv2 utilizza il token memorizzato creato utilizzando il comando dell'esempio precedente. Il token non deve essere scaduto.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

PowerShell

Questo esempio ottiene tutte le chiavi dei tag per un'istanza.

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

In questo esempio viene ottenuto il valore della `Name` chiave ottenuta nell'esempio precedente. La richiesta IMDSv2 utilizza il token memorizzato creato utilizzando il comando dell'esempio precedente. Il token non deve essere scaduto.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

Esempi per IMDSv1

Esegui i seguenti esempi sulla tua istanza Amazon EC2 per recuperare i metadati dell'istanza per IMDSv1.

Nelle istanze Windows, puoi usare Windows PowerShell oppure puoi installare cURL o wget. Se installate uno strumento di terze parti su un'istanza di Windows, assicuratevi di leggere attentamente la documentazione di accompagnamento, poiché le chiamate e l'output potrebbero essere diversi da quelli descritti qui.

Esempi

- Recupero delle versioni disponibili dei metadati dell'istanza
- Recupero degli elementi di metadati di primo livello
- Ottieni i valori per gli elementi di metadati
- Recupero dell'elenco di chiavi pubbliche disponibili
- Visualizzazione dei formati in cui è disponibile la chiave pubblica 0
- Recupero della chiave pubblica 0 (nel formato di chiave OpenSSH)
- Recupero dell'ID della sottorete per un'istanza
- Ottenere i tag dell'istanza per un'istanza

Recupero delle versioni disponibili dei metadati dell'istanza

Questo esempio recupera le versioni disponibili dei metadati dell'istanza. Ogni versione fa riferimento a una build dei metadati dell'istanza quando sono state rilasciate nuove categorie di metadati dell'istanza. Le versioni di build dei metadati dell'istanza non sono correlate alle versioni dell'API di Amazon EC2. Le versioni precedenti sono disponibili in presenza di script basati sulla struttura e sulle informazioni presenti in una versione precedente.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
```

```
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Recupero degli elementi di metadati di primo livello

Questo esempio recupera gli elementi di metadati di primo livello. Per ulteriori informazioni sugli elementi della risposta, vedereCategorie di metadati dell'istanza.

Tieni presente che i tag sono inclusi in questo output solo se hai consentito l'accesso. Per ulteriori informazioni, consulta the section called “Per consentire l'accesso ai tag nei metadati delle istanze”.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
```

```
services/
tags/
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Ottieni i valori per gli elementi di metadati

Questi esempi ottengono i valori di alcuni degli elementi di metadati di primo livello ottenuti nell'esempio precedente.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
```

```
r-0efghijk987654321
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Recupero dell'elenco di chiavi pubbliche disponibili

Questo esempio recupera l'elenco delle chiavi pubbliche disponibili.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/ 0=my-public-key
```

Visualizzazione dei formati in cui è disponibile la chiave pubblica 0

Questo esempio mostra i formati in cui è disponibile la chiave pubblica 0.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
openssh-key
```

Recupero della chiave pubblica 0 (nel formato di chiave OpenSSH)

Questo esempio recupera la chiave pubblica 0 (nel formato di chiave OpenSSH).

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
```

```
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Recupero dell'ID della sottorete per un'istanza

In questo esempio viene recuperato l'ID della sottorete per un'istanza.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/
interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Ottenere i tag dell'istanza per un'istanza

Questi esempi accedono ai tag di un'istanza. È necessario consentire l'accesso ai tag prima di poter utilizzare questi esempi.

cURL

Questo esempio ottiene tutte le chiavi dei tag per un'istanza.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance
Name
```

```
Environment
```

In questo esempio viene ottenuto il valore della `Name` chiave ottenuta nell'esempio precedente.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

PowerShell

Questo esempio ottiene tutte le chiavi dei tag per un'istanza.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

In questo esempio viene ottenuto il valore della `Name` chiave ottenuta nell'esempio precedente.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/
instance/Name
MyInstance
```

Throttling delle query

La limitazione (della larghezza di banda della rete) delle query viene applicata in base all'istanza, ovvero vengono applicate restrizioni al numero di connessioni simultanee da un'istanza all'IMDS.

Se utilizzi l'IMDS per recuperare le credenziali di AWS sicurezza, evita di richiedere le credenziali durante ogni transazione o contemporaneamente a un numero elevato di thread o processi, poiché ciò potrebbe comportare un rallentamento. Consigliamo invece di memorizzare le credenziali nella cache fino all'approssimarsi della relativa data di scadenza. Per ulteriori informazioni sul ruolo IAM e sulle credenziali di sicurezza associate al ruolo, consulta Recupero delle credenziali di sicurezza dai metadati delle istanze.

Se si verifica tale limitazione (della larghezza di banda della rete) durante l'accesso all'IMDS, riprova a eseguire la query con un approccio basato sul backoff esponenziale.

Limitazione dell'accesso al servizio di metadati dell'istanza (IMDS)

Puoi valutare se utilizzare regole firewall locali per disabilitare l'accesso all'IMDS da alcuni processi o da tutti.

Per le istanze basate sul sistema AWS Nitro, l'IMDS può essere raggiunto dalla propria rete quando un dispositivo di rete all'interno del VPC, ad esempio un router virtuale, inoltra i pacchetti all'indirizzo IMDS e il controllo di origine/destinazione predefinito sull'istanza è disabilitato. Per evitare che una fonte esterna al tuo VPC raggiunga l'IMDS, ti consigliamo di modificare la configurazione dell'appliance di rete in modo da eliminare pacchetti con l'indirizzo IPv4 di destinazione dell'IMDS `169.254.169.254` e, se hai abilitato l'endpoint IPv6, l'indirizzo IPv6 dell'IMDS. `[fd00:ec2::254]`

Istanze Linux

Utilizzo di iptables per limitare l'accesso

L'esempio seguente utilizza iptables Linux e il relativo modulo `owner` per impedire al server Web Apache (basato sul suo ID utente di installazione predefinito di `apache`) di accedere a 169.254.169.254. Utilizza una regola di rifiuto per rifiutare tutte le richieste dei metadati dell'istanza (IMDSv1 o IMDSv2) da qualsiasi processo in esecuzione come tale utente.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner
 --uid-owner apache --jump REJECT
```

Oppure, puoi valutare di consentire l'accesso solo a utenti o gruppi particolari, utilizzando regole che autorizzano. Le regole che autorizzano potrebbero essere più facili da gestire dal punto di vista della sicurezza, perché richiedono di prendere una decisione sul software che deve poter accedere ai metadati dell'istanza. Se utilizzi regole che autorizzano, è meno probabile che venga accidentalmente concesso al software l'accesso al servizio di metadati (a cui non intendevi accedere) se in seguito modifichi il software o la configurazione su un'istanza. Puoi anche combinare l'utilizzo dei gruppi con le regole che autorizzano, in modo da poter aggiungere e rimuovere utenti da un gruppo autorizzato senza la necessità di modificare la regola firewall.

L'esempio seguente impedisce a tutti i processi di accedere all'IMDS, tranne a quelli in esecuzione nell'account utente `trustworthy-user`.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match
 owner ! --uid-owner trustworthy-user --jump REJECT
```

> **Note**
>
> - Per utilizzare regole firewall locali, è necessario adattare i comandi dell'esempio precedente in base alle proprie esigenze.

- Per impostazione predefinita, le regole iptables non vengono mantenute tra riavvii del sistema. Possono essere rese persistenti utilizzando funzionalità del sistema operativo non descritte in questo argomento.
- Il modulo `owner` iptables corrisponde all'appartenenza al gruppo solo se il gruppo è quello primario di un determinato utente locale. Altri gruppi non corrispondono.

Utilizzo di PF o IPFW per limitare l'accesso

Se utilizzi FreeBSD o OpenBSD, puoi anche valutare l'utilizzo di PF o IPFW. Gli esempi seguenti limitano l'accesso all'IMDS al solo utente root.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

> **Note**
>
> L'ordine dei comandi PF e IPFW è importante. PF è preimpostato sull'ultima regola corrispondente e IPFW è preimpostato sulla prima regola corrispondente.

Istanze Windows

Utilizzo del firewall Windows per limitare l'accesso

L' PowerShell esempio seguente utilizza il firewall integrato di Windows per impedire al server Web di Internet Information Server (in base all'ID utente di installazione predefinito di`NT AUTHORITY\IUSR`) di accedere a 169.254.169.254. Utilizza una regola di rifiuto per rifiutare tutte le richieste dei metadati dell'istanza (IMDSv1 o IMDSv2) da qualsiasi processo in esecuzione come tale utente.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT
 AUTHORITY\IUSR")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action
 block -Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

Oppure, puoi valutare di consentire l'accesso solo a utenti o gruppi particolari, utilizzando regole che autorizzano. Le regole che autorizzano potrebbero essere più facili da gestire dal punto di vista della sicurezza, perché richiedono di prendere una decisione sul software che deve poter accedere ai metadati dell'istanza. Se utilizzi regole che autorizzano, è meno probabile che venga accidentalmente concesso al software l'accesso al servizio di metadati (a cui non intendevi accedere) se in seguito modifichi il software o la configurazione su un'istanza. Puoi anche combinare l'utilizzo dei gruppi con le regole che autorizzano, in modo da poter aggiungere e rimuovere utenti da un gruppo autorizzato senza la necessità di modificare la regola firewall.

L'esempio seguente impedisce l'accesso ai metadati dell'istanza da tutti i processi in esecuzione su un gruppo OS specificato nella variabile `blockPrincipal` (in questo esempio, il gruppo Windows `Everyone`), ad eccezione dei processi specificati in `exceptionPrincipal` (in questo esempio, un gruppo denominato `trustworthy-users`). È necessario specificare entrambi i principali di rifiuto e di autorizzazione perché Windows Firewall, a differenza della regola `! --uid-owner trustworthy-user` in iptables Linux, non fornisce un meccanismo di scelta rapida per consentire solo un principale particolare (utente o gruppo) rifiutando tutti gli altri.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("Everyone")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
 $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
 $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

> **Note**
>
> Per utilizzare regole firewall locali, è necessario adattare i comandi dell'esempio precedente in base alle proprie esigenze.

Utilizzo di regole netsh per limitare l'accesso

Puoi considerare di bloccare tutto il software utilizzando regole `netsh`, ma queste sono molto meno flessibili.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"
 dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

> **Note**
>
> - Per utilizzare regole firewall locali, è necessario adattare i comandi dell'esempio precedente in base alle proprie esigenze.
> - Le regole `netsh` devono essere impostate da un prompt dei comandi con privilegi elevati e non possono essere impostate per rifiutare o autorizzare principali particolari.

Utilizzo dei dati utente dell'istanza

È possibile utilizzare i dati utente dell'istanza per personalizzare le istanze. Quando avvii un'istanza, puoi memorizzare parametri o script come dati utente. Tutti gli script nei dati utente vengono eseguiti all'avvio dell'istanza. È possibile visualizzare i dati utente come attributo dell'istanza. Puoi anche visualizzare i dati utente dell'istanza tramite il servizio di metadati di istanza (IMDS).

Considerazioni

- I dati utente vengono trattati come dati opachi: ciò che specifichi è ciò che ottieni al momento del recupero. Spetta all'istanza interpretare e agire sui dati dell'utente.
- I dati utente devono essere codificati con base64. A seconda dello strumento o dell'SDK che stai utilizzando, la codifica base64 potrebbe essere eseguita automaticamente. Per esempio:
  - La console Amazon EC2 può eseguire automaticamente la codifica con base64 oppure accettare input codificati con base64.

  - AWS CLI la versione 2 esegue automaticamente la codifica in base64 dei parametri binari. AWS CLI la versione 1 esegue la codifica base64 del parametro per voi. `--user-data`
  - AWS SDK for Python (Boto3) Esegue la codifica base64 del parametro per voi. `UserData`
- I dati dell'utente sono limitati a 16 KB, in formato raw, prima della codifica base 64. La dimensione di una stringa di lunghezza n dopo la codifica base64 è ceil(n/3)*4.
- I dati utente devono essere decodificati con base64 quando li recuperi. Se recuperi i dati utilizzando i metadati dell'istanza o la console, vengono decodificati automaticamente.
- Se arresti un'istanza, ne modifichi i dati utente e quindi avvii l'istanza, i dati utente aggiornati non vengono eseguiti automaticamente quando si avvia l'istanza. Con le istanze Windows, è possibile configurare le impostazioni in modo che gli script di dati utente aggiornati vengano eseguiti una volta all'avvio dell'istanza o ogni volta che si riavvia o si avvia l'istanza.
- I dati utente sono un attributo dell'istanza. Se si crea un'AMI da un'istanza, i dati utente dell'istanza non vengono inclusi nell'AMI.

Specifica dei dati utente dell'istanza all'avvio

Puoi specificare i dati utente dell'istanza al momento dell'avvio di un'istanza. Per le indicazioni per la console, consulta Specifica dei dati utente dell'istanza all'avvio. Per un esempio di Linux che utilizza il AWS CLI, vedi. the section called “I dati dell'utente e il AWS CLI” Per un esempio di Windows che utilizza gli strumenti per Windows PowerShell, vederethe section called “Dati utente e strumenti per Windows PowerShell”.

Modifica dei dati utente dell'istanza

È possibile modificare i dati utente per le istanze con un volume root EBS. L'istanza deve essere nello stato stopped (arrestato). Per le indicazioni per la console, consulta Visualizzazione e aggiornamento dei dati utente dell'istanza. Per un esempio di Linux che utilizza il AWS CLI, vedi modify-instance-attribute. Per un esempio di Windows che utilizza gli strumenti per Windows PowerShell, vederethe section called “Dati utente e strumenti per Windows PowerShell”.

Recupero dei dati utente dell'istanza dall'istanza

Per recuperare i dati utente da un'istanza, utilizza uno dei seguenti URI. Per recuperare i dati utente utilizzando l'indirizzo IPv6, è necessario abilitarlo e l'istanza deve essere un'istanza creata sul sistema AWS Nitro in una sottorete che supporta IPv6.

IPv4

```
http://169.254.169.254/latest/user-data
```

IPv6

```
http://[fd00:ec2::254]/latest/user-data
```

Una richiesta di dati utente restituisce i dati nel formato originale (tipo di contenuto `application/octet-stream`). Se l'istanza non dispone di dati utente, la richiesta restituisce `404 - Not Found`.

Esempio: recupera testo separato da virgole

Questo esempio recupera i dati utente specificati come testo separato da virgole.

cURL

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

PowerShell

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod
 -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Esempio: recuperare uno script

Questo esempio recupera i dati utente che sono stati specificati come script.

cURL

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Powershell

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/user-data
```

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Recupero dei dati utente per un'istanza dal tuo computer

È possibile recuperare i dati utente per un'istanza dal tuo computer. Per le indicazioni per la console, consulta Visualizzazione e aggiornamento dei dati utente dell'istanza. Per un esempio che utilizza il AWS CLI, vedereI dati dell'utente e il AWS CLI. Per un esempio che utilizza gli strumenti per Windows PowerShell, vedereDati utente e strumenti per Windows PowerShell.

Esegui comandi sulla tua istanza Amazon EC2 al momento del lancio

Quando avvii un'istanza Amazon EC2, puoi passare i dati utente all'istanza utilizzata per eseguire attività di configurazione automatizzate o per eseguire script dopo l'avvio dell'istanza.

Se sei interessato a scenari di automazione più complessi, potresti prendere in considerazione o AWS CloudFormation . AWS OpsWorks Per ulteriori informazioni, consulta gli argomenti seguenti:

- Implementazione di applicazioni su Amazon EC2 con AWS CloudFormation nella Guida per l'utente di AWS CloudFormation .
- AWS OpsWorks Guida per l'utente.

Sulle istanze Linux, puoi passare due tipi di dati utente ad Amazon EC2: script di shell e direttive cloud-init. Puoi anche passare questi dati nella procedura guidata di avvio dell'istanza come testo semplice, come file (utile per avviare istanze con gli strumenti della riga di comando) o come testo con codifica base64 (per le chiamate API).

Nelle istanze Windows, gli agenti di avvio gestiscono gli script dei dati utente. Nelle sezioni seguenti vengono illustrate le differenze nel modo in cui i dati utente vengono gestiti su ciascun sistema operativo.

In che modo Amazon EC2 gestisce i dati utente per le istanze Linux

Negli esempi seguenti, i comandi del server Installa un LAMP su Amazon Linux 2 vengono convertiti in uno script di shell e in un set di direttive cloud-init che vengono eseguite all'avvio dell'istanza. In ogni esempio, le seguenti attività vengono eseguite in base ai dati utente:

- I pacchetti del software di distribuzione vengono aggiornati.
- Il server Web necessario, `php`, e i pacchetti `mariadb` vengono installati.
- Il servizio `httpd` viene avviato e abilitato tramite systemctl.
- Il `ec2-user` viene aggiunto al gruppo apache.
- Vengono configurati la proprietà e le autorizzazioni di file appropriati per la directory Web e i file in essa contenuti.
- Viene creata una semplice pagina Web per testare il server Web e il motore PHP.

Indice

Prerequisiti

Per gli esempi in questo argomento si presuppone quanto riportato di seguito:

- L'istanza dispone di un nome DNS pubblico raggiungibile da Internet.
- Il gruppo di sicurezza associato all'istanza è configurato per consentire il traffico SSH (porta 22) in modo da potersi connettere all'istanza per visualizzare i file di log di output.
- L'istanza viene avviata con un'AMI Amazon Linux 2. Queste istruzioni sono pensate per essere utilizzate con Amazon Linux 2. I comandi e le direttive potrebbero non funzionare per altre

distribuzioni Linux. Per ulteriori informazioni su altre distribuzioni, ad esempio sul relativo supporto delle direttive cloud-init, consulta la documentazione specifica.

Dati utente e script della shell

Se hai familiarità con lo scripting della shell, questo è il modo più semplice e completo per inviare le istruzioni a un'istanza all'avvio. L'aggiunta di queste attività in fase di avvio aumenta il tempo necessario per l'avvio dell'istanza. Ti consigliamo di prevedere alcuni minuti aggiuntivi per il completamento delle attività prima di procedere alla verifica del corretto completamento dello script utente.

> **Important**
>
> Per impostazione predefinita, gli script di dati utente e le direttive cloud-init vengono eseguiti solo durante il ciclo di avvio quando si avvia un'istanza per la prima volta. È possibile aggiornare la configurazione per garantire che gli script dei dati utente e le direttive cloud-init vengano eseguiti ogni volta che si riavvia l'istanza. Per ulteriori informazioni, consulta Come posso utilizzare i dati utente per eseguire automaticamente uno script a ogni riavvio della mia istanza Amazon EC2 Linux? nel AWS Knowledge Center.

Gli script della shell relativi ai dati utente devono iniziare con i caratteri `#!` e con il percorso dell'interprete che deve leggere lo script, in genere /bin/bash). Per un'introduzione allo shell scripting, consultate il manuale di riferimento di Bash sul sito web del sistema operativo GNU.

Gli script immessi come dati utente vengono eseguiti come utente root. Non utilizzare pertanto il comando sudo nello script. Ricorda che tutti i file creati saranno di proprietà dell'utente root. Se devi concedere l'accesso ai file a utenti non root, devi modificare di conseguenza le autorizzazioni nello script. Inoltre, dal momento che lo script non viene eseguito in modo interattivo, non puoi includere comandi che richiedono il feedback degli utenti, ad esempio il comando yum update senza il contrassegno `-y`.

Se utilizzi un' AWS API, inclusa la AWS CLI, in uno script di dati utente, devi utilizzare un profilo di istanza all'avvio dell'istanza. Un profilo di istanza fornisce le AWS credenziali appropriate richieste dallo script dei dati utente per emettere la chiamata API. Per ulteriori informazioni, consulta Utilizzo dei profili dell'istanza in Guida per l'utente di IAM. Le autorizzazioni assegnate al ruolo IAM dipendono dai servizi chiamati con l'API. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.

Il file di log dell'output della direttiva cloud-init acquisisce l'output della console in modo da semplificare il debug degli script dopo l'avvio se l'istanza ha un comportamento imprevisto. Per visualizzare il file di log, connettiti all'istanza e apri `/var/log/cloud-init-output.log`.

Quando uno script di dati utente viene elaborato, viene copiato ed eseguito da `/var/lib/cloud/instances/instance-id/`. Lo script non viene eliminato dopo l'esecuzione. Assicurati di eliminare gli script di dati utente da `/var/lib/cloud/instances/instance-id/` prima di creare un'AMI dall'istanza. In caso contrario, lo script esisterà in questa directory su qualsiasi istanza avviata dall'AMI.

Dati utente e console

Puoi specificare i dati utente dell'istanza al momento dell'avvio dell'istanza. Se il volume root dell'istanza è un volume EBS, puoi anche arrestare l'istanza e aggiornare i relativi dati utente.

Specifica dei dati utente dell'istanza all'avvio

Segui la procedura per l'avvio di un'istanza. Il campo User data (Dati utente) campo si trova nella sezione Dettagli avanzati della procedura guidata di avvio dell'istanza. Inserisci lo script della shell nel campo User data (Dati utente), quindi completa la procedura di avvio dell'istanza.

Questo script di esempio crea e configura il nostro server web.

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Prevedi tempo aggiuntivo per l'avvio dell'istanza e l'esecuzione dei comandi nello script e quindi verifica se lo script ha completato le attività come previsto.

Nel nostro esempio, in un browser Web immetti l'URL del file di test PHP creato dallo script. Questo URL è l'indirizzo DNS pubblico dell'istanza, seguito da una barra e dal nome di file.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Viene visualizzata la pagina delle informazioni PHP. Se non sei in grado di vedere questa pagina, controlla che il gruppo di sicurezza che stai utilizzando contenga una regola che consenta il traffico HTTP (porta 80). Per ulteriori informazioni, consulta Aggiunta di regole a un gruppo di sicurezza.

(Facoltativo) Se lo script non ha completato le attività previste oppure se vuoi semplicemente verificare che lo script sia stato completato senza errori, connettiti all'istanza, esamina il file di log dell'output della direttiva cloud-init (`/var/log/cloud-init-output.log`) e cerca eventuali messaggi di errore nell'output.

Per informazioni aggiuntive sul debug, puoi creare un archivio in formato Mime multipart contenente una sezione di dati cloud-init con la seguente direttiva:

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Questa direttiva invia l'output del comando dallo script a `/var/log/cloud-init-output.log`. Per ulteriori informazioni sui formati dei dati cloud-init e sulla creazione dell'archivio Mime in più parti, consulta la sezione relativa ai formati cloud-init.

Visualizzazione e aggiornamento dei dati utente dell'istanza

Per aggiornare i dati utente dell'istanza, è necessario prima arrestare l'istanza. Se l'istanza è in esecuzione, è possibile visualizzare i dati utente ma non modificarli.

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

Per modificare i dati utente dell'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona l'istanza e scegli Instance state (Stato istanza), Stop instance (Arresta istanza). Se questa opzione è disabilitata, l'istanza è già arrestata o il suo dispositivo root è un volume di instance store.

4. Quando viene richiesta la conferma, selezionare Stop (Arresta). Possono essere necessari alcuni minuti per arrestare l'istanza.
5. Con l'istanza ancora selezionata, selezionare Actions (Operazioni), Instance Settings (Impostazioni istanza), Edit user data (Modifica i dati utente).
6. Modificare i dati utente in base alle esigenze, quindi scegliere Save (Salva).
7. Avviare l'istanza. I nuovi dati utente sono visibili nell'istanza dopo averla avviata. Tuttavia, gli script dei dati utente non vengono eseguiti.

Dati utente e direttive cloud-init

Il pacchetto cloud-init configura aspetti specifici di una nuova istanza di Amazon Linux quando viene avviata. In particolare, configura il file `.ssh/authorized_keys` per ec2-user in modo da consentirti di eseguire il login utilizzando la tua chiave privata. Per ulteriori informazioni sulle attività di configurazione eseguite dal pacchetto cloud-init per le istanze Amazon Linux, consulta Using cloud-init on Amazon Linux 2 nella Amazon Linux 2 User Guide.

Le direttive utente cloud-init possono essere trasferite a un'istanza all'avvio con le stesse modalità di trasferimento di uno script, anche se la sintassi è diversa. Per ulteriori informazioni su cloud-init, visita la pagina http://cloudinit.readthedocs.org/en/latest/index.html.

> **Important**
>
> Per impostazione predefinita, gli script di dati utente e le direttive cloud-init vengono eseguiti solo durante il ciclo di avvio quando si avvia un'istanza per la prima volta. È possibile aggiornare la configurazione per garantire che gli script dei dati utente e le direttive cloud-init vengano eseguiti ogni volta che si riavvia l'istanza. Per ulteriori informazioni, consulta Come posso utilizzare i dati utente per eseguire automaticamente uno script a ogni riavvio della mia istanza Amazon EC2 Linux? nel AWS Knowledge Center.

L'aggiunta di queste attività in fase di avvio aumenta il tempo necessario per l'avvio di un'istanza. Ti consigliamo di prevedere alcuni minuti aggiuntivi per il completamento delle attività prima di procedere alla verifica del corretto completamento delle direttive relative ai dati utente.

Per trasferire le direttive cloud-init a un'istanza con i dati utente

1. Segui la procedura per l'avvio di un'istanza. Il campo User data (Dati utente) campo si trova nella sezione Dettagli avanzati della procedura guidata di avvio dell'istanza. Inserisci il testo

della direttiva cloud-init nel campo User data (Dati utente), quindi completa la procedura di avvio dell'istanza.

Nell'esempio riportato di seguito, le direttive creano e configurano un server Web su Amazon Linux 2. La riga `#cloud-config` all'inizio è obbligatoria per l'identificazione dei comandi come direttive cloud-init.

```
#cloud-config
repo_update: true
repo_upgrade: all

packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- sudo systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

2. Prevedi tempo aggiuntivo per l'avvio dell'istanza e l'esecuzione delle direttive nei dati utente e quindi verifica se le direttive hanno completato le attività come previsto.

   Nel nostro esempio, in un browser Web, inserisci l'URL del file di test PHP creato dalle direttive. Questo URL è l'indirizzo DNS pubblico dell'istanza, seguito da una barra e dal nome di file.

   ```
   http://my.public.dns.amazonaws.com/phpinfo.php
   ```

   Viene visualizzata la pagina delle informazioni PHP. Se non sei in grado di vedere questa pagina, controlla che il gruppo di sicurezza che stai utilizzando contenga una regola che consenta il traffico HTTP (porta 80). Per ulteriori informazioni, consulta Aggiunta di regole a un gruppo di sicurezza.

3. (Facoltativo) Se le direttive non hanno completato le attività previste oppure se desideri verificare che siano state completate senza errori, connettiti all'istanza, esamina il file di log dell'output (/

`var/log/cloud-init-output.log`) e cerca eventuali messaggi di errore nell'output. Per ulteriori informazioni sul debug, è possibile aggiungere la seguente riga alle direttive:

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Questa direttiva invia l'output del comando runcmd a `/var/log/cloud-init-output.log`.

I dati dell'utente e il AWS CLI

È possibile utilizzare i AWS CLI per specificare, modificare e visualizzare i dati utente per l'istanza. Per informazioni sulla visualizzazione dei dati utente dall'istanza tramite metadati dell'istanza, consulta Recupero dei dati utente dell'istanza dall'istanza.

In Windows, è possibile utilizzare il AWS Tools for Windows PowerShell anziché utilizzare AWS CLI. Per ulteriori informazioni, consulta Dati utente e strumenti per Windows PowerShell.

Esempio: specifica dei dati utente all'avvio

Per specificare i dati utente all'avvio di un'istanza, utilizza il comando run-instances con il parametro `--user-data`. Conrun-instances, AWS CLI esegue la codifica in base64 dei dati utente per te.

L'esempio seguente illustra come specificare uno script come stringa nella riga di comando:

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data echo user data
```

L'esempio seguente illustra come specificare uno script utilizzando un file di testo. Assicurati di utilizzare il prefisso `file://` per specificare il file.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data file://my_script.txt
```

Di seguito è riportato un esempio di file di testo con uno script della shell.

```
#!/bin/bash
yum update -y
service httpd start
```

```
chkconfig httpd on
```

Esempio: modifica dei dati utente di un'istanza arrestata

È possibile modificare i dati utente di un'istanza interrotta utilizzando il comando. modify-instance-attribute Conmodify-instance-attribute, AWS CLI non esegue la codifica in base64 dei dati utente per voi.

- Su un computer Linux utilizzare il comando con codifica Base64 per codificare i dati utente.

  ```
  base64 my_script.txt >my_script_base64.txt
  ```

- Su un computer Windows, utilizza il comando certutil per codificare i dati utente. Prima di poter utilizzare questo file con AWS CLI, è necessario rimuovere la prima riga (BEGIN CERTIFICATE) e l'ultima (END CERTIFICATE).

  ```
  certutil -encode my_script.txt my_script_base64.txt
  notepad my_script_base64.txt
  ```

Utilizza i parametri `--attribute` e `--value` per utilizzare il file di testo codificato per specificare i dati utente. Assicurati di utilizzare il prefisso `file://` per specificare il file.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --value file://my_script_base64.txt
```

Esempio: cancellazione dei dati utente di un'istanza arrestata

Per eliminare i dati utente esistenti, utilizzate il modify-instance-attributecomando come segue:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Esempio: visualizzazione dei dati utente

Per recuperare i dati utente per un'istanza, utilizzate il describe-instance-attributecomando. Condescribe-instance-attribute, AWS CLI non esegue la decodifica in base64 dei dati utente per voi.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData
```

L'esempio seguente è l'output contenente i dati utente con codifica base64.

```
{
    "UserData": {
        "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
    },
    "InstanceId": "i-1234567890abcdef0"
}
```

- Su un computer Linux, utilizza l'opzione `--query` per recuperare i dati utente codificati e il comando con codifica Base64 per decodificarli.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" | base64 --decode
```

- Su un computer Windows, utilizza l'opzione `--query` per recuperare i dati utente codificati e il comando certutil per decodificarli. Si noti che l'output codificato viene memorizzato in un file, mentre l'output decodificato viene memorizzato in un file diverso.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" >my_output.txt
certutil -decode my_output.txt my_output_decoded.txt
type my_output_decoded.txt
```

Di seguito è riportato un output di esempio.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Combinazione di script di shell e direttive cloud-init

Per impostazione predefinita, nei dati utente puoi includere solo un tipo di contenuto alla volta. Tuttavia, puoi utilizzare tipi di contenuto `text/cloud-config` e `text/x-shellscript` in un file multipart MIME per includere nei dati utente sia uno script di shell che direttive cloud-init.

Di seguito è illustrato il formato multipart MIME.

```
Content-Type: multipart/mixed; boundary="//"
```

```
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
cloud-init directives

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
shell script commands
--//--
```

Ad esempio, i seguenti dati utente includono direttive cloud-init e uno script di shell bash. Le direttive cloud-init creano un file (`/test-cloudinit/cloud-init.txt`) e scrivono `Created by cloud-init` in tale file. Lo script della shell bash crea un file (`/test-userscript/userscript.txt`) e scrive `Created by bash shell script` in quel file.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
runcmd:
- [ mkdir, /test-cloudinit ]
write_files:
- path: /test-cloudinit/cloud-init.txt
content: Created by cloud-init

--//
```

```
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
mkdir test-userscript
touch /test-userscript/userscript.txt
echo "Created by bash shell script" >> /test-userscript/userscript.txt
--//--
```

In che modo Amazon EC2 gestisce i dati utente per le istanze Windows

Nelle istanze Windows, gli agenti di avvio predefiniti per la versione del sistema operativo in uso gestiscono i dati degli utenti nel modo seguente.

- EC2Launch v2esegue script di dati utente su Windows Server 2022
- EC2Launchesegue script di dati utente su Windows Server 2016 e 2019
- EC2Config serviceesegue script di dati utente su versioni di Windows Server precedenti a Windows Server 2016

Per esempi di assemblaggio di una `UserData` proprietà in un AWS CloudFormation modello, vedere Base64 Encoded Property e Base64 Encoded UserData Property with and. UserData AccessKey SecretKey

Per un esempio di esecuzione di comandi su un'istanza all'interno di un gruppo Auto Scaling che funziona con i lifecycle hook, consulta Tutorial: Configura i dati utente per recuperare lo stato del ciclo di vita di destinazione tramite i metadati dell'istanza nella Amazon EC2 Auto Scaling User Guide.

Indice

Script di dati utente

Per `EC2Config` o per `EC2Launch` eseguire gli script, è necessario racchiudere lo script in un tag speciale quando lo si aggiunge ai dati utente. Il tag utilizzato dipende dal fatto che i comandi vengano eseguiti in una finestra del prompt dei comandi (comandi batch) o utilizzino Windows. PowerShell

Se si specificano sia uno script batch che uno PowerShell script di Windows, lo script batch viene eseguito per primo e lo PowerShell script di Windows viene eseguito successivamente, indipendentemente dall'ordine in cui vengono visualizzati nei dati utente dell'istanza.

Se si utilizza un' AWS API, inclusa la AWS CLI, in uno script di dati utente, è necessario utilizzare un profilo di istanza all'avvio dell'istanza. Un profilo di istanza fornisce le AWS credenziali appropriate richieste dallo script dei dati utente per effettuare la chiamata API. Per ulteriori informazioni, consulta Profili delle istanze. Le autorizzazioni assegnate al ruolo IAM dipendono dai servizi chiamati con l'API. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.

Tipo di script

- Sintassi di script batch
- Sintassi per gli script di Windows PowerShell
- Sintassi per gli script di configurazione YAML
- Codifica Base64

Sintassi di script batch

Specificare uno script batch tramite il tag `script`. Separa i comandi utilizzando le interruzioni di riga, come illustrato nell'esempio seguente.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

Per impostazione predefinita, gli script di dati utente vengono eseguiti una volta all'avvio dell'istanza. Per eseguire gli script di dati utente ogni volta che si riavvia o avvia l'istanza, aggiungere `<persist>true</persist>` ai dati utente.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

```
</script>
<persist>true</persist>
```

Agente EC2Launch v2

Per eseguire uno script di dati utente XML come processo separato con l'executeScriptattività EC2Launch v2 nello `UserData` stage, aggiungilo `<detach>true</detach>` ai dati utente.

> **Note**
>
> Il detach tag non è supportato dai precedenti agenti di lancio.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<detach>true</detach>
```

Sintassi per gli script di Windows PowerShell

Le AMI AWS Windows includono AWS Tools for Windows PowerShell, quindi è possibile specificare questi cmdlet nei dati utente. Se associ un ruolo IAM alla tua istanza, non è necessario specificare le credenziali per i cmdlet, poiché le applicazioni eseguite sull'istanza utilizzano le credenziali del ruolo per accedere alle AWS risorse (ad esempio, i bucket Amazon S3).

Specificate uno script di Windows utilizzando il tag. PowerShell `<powershell>` Separare i comandi tramite interruzioni di riga. Il tag `<powershell>` rileva la distinzione tra maiuscole e minuscole.

Per esempio:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

Per impostazione predefinita, gli script dei dati utente vengono eseguiti una sola volta all'avvio dell'istanza. Per eseguire gli script di dati utente ogni volta che si riavvia o avvia l'istanza, aggiungere `<persist>true</persist>` ai dati utente.

```
<powershell>
```

```
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

È possibile specificare uno o più PowerShell argomenti con il `<powershellArguments>` tag. Se non viene passato alcun argomento, EC2Launch e EC2Launch v2 aggiungono il seguente argomento per impostazione predefinita:. `-ExecutionPolicy Unrestricted`

Esempio:

```
<powershell>
    $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Agente EC2Launch v2

Per eseguire uno script di dati utente XML come processo separato con il executeScript task EC2Launch v2 nello stage, aggiungilo ai dati utente. `UserData <detach>true</detach>`

> **Note**
>
> Il detach tag non è supportato dai precedenti agenti di lancio.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

Sintassi per gli script di configurazione YAML

Se si utilizza EC2Launch v2 per eseguire script, è possibile utilizzare il formato YAML. Per visualizzare le attività di configurazione, i dettagli e gli esempi per EC2Launch v2, consulta Configurazione dell'attività di EC2Launch v2.

Specificare uno script YAML con l'attività `executeScript`.

Esempio di sintassi YAML per eseguire uno script PowerShell

```
version: 1.0
    tasks:
    - task: executeScript
      inputs:
      - frequency: always
        type: powershell
        runAs: localSystem
        content: |-
          $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
          New-Item $file -ItemType file
```

Esempio di sintassi YAML per eseguire uno script batch

```
version: 1.1
    tasks:
    - task: executeScript
      inputs:
      - frequency: always
        type: batch
        runAs: localSystem
        content: |-
          echo Current date and time >> %SystemRoot%\Temp\test.log
          echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Codifica Base64

Se utilizzi l'API Amazon EC2 o uno strumento che non esegue la codifica base64 dei dati utente, codificare direttamente i dati utente. In caso contrario, verrà registrato un errore sull'impossibilità di individuare i tag `script` o `powershell` da eseguire. Di seguito è riportato un esempio di codifica tramite Windows. PowerShell

```
$UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Di seguito è riportato un esempio che decodifica utilizzando. PowerShell

```
$Script =
 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Per ulteriori informazioni sulla codifica base64, vedere https://www.ietf.org/rfc/rfc4648.txt.

Esecuzione dei dati utente

Per impostazione predefinita, tutte le AMI AWS Windows hanno l'esecuzione dei dati utente abilitata all'avvio iniziale. Puoi specificare che gli script di dati utente vengano eseguiti la prossima volta che l'istanza è riavviata. In alternativa, puoi specificare che gli script di dati utente vengano eseguiti ogni volta che l'istanza è riavviata.

> **Note**
>
> Per impostazione predefinita, l'esecuzione dei dati utente non è abilitata dopo l'avvio iniziale. Per abilitare l'esecuzione dei dati utente al riavvio o all'avvio dell'istanza, consulta Avvii o riavvii successivi.

Gli script di dati utente vengono eseguiti dall'account amministratore locale quando viene generata una password casuale. In caso contrario, gli script di dati utente vengono eseguiti dall'account del sistema.

Avvio dell'istanza

Gli script nei dati utente dell'istanza vengono eseguiti durante l'avvio iniziale dell'istanza. Se individui il tag `persist`, l'esecuzione dei dati utente è abilitata per i riavvii successivi. I file di log per EC2Launch v2, EC2Launch ed EC2Config contengono i risultati dell'output standard e i flussi di errore standard.

EC2Launch v2

Il file di log per EC2Launch v2 è `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> La cartella `C:\ProgramData` potrebbe essere nascosta. Per visualizzare la cartella, è necessario mostrare i file e le cartelle nascosti.

Le informazioni seguenti vengono registrate durante l'esecuzione dei dati utente:

- `Info: Converting user-data to yaml format` - Se i dati utente sono stati forniti in formato XML

- `Info: Initialize user-data state` - L'inizio dell'esecuzione dei dati utente
- `Info: Frequency is: always` - Se l'attività dei dati utente è in esecuzione a ogni avvio
- `Info: Frequency is: once` - Se l'attività dei dati utente è in esecuzione una sola volta
- `Stage: postReadyUserData execution completed` - La fine dell'esecuzione dei dati dell'utente

EC2Launch

Il file di log per EC2Launch è `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

La cartella `C:\ProgramData` potrebbe essere nascosta. Per visualizzare la cartella, è necessario mostrare i file e le cartelle nascosti.

Le informazioni seguenti vengono registrate durante l'esecuzione dei dati utente:

- `Userdata execution begins` - L'inizio dell'esecuzione dei dati utente
- `<persist> tag was provided: true` - Se viene individuato il tag persist
- `Running userdata on every boot` - Se viene individuato il tag persist
- `<powershell> tag was provided.. running powershell content` - Se viene individuato il tag powershell
- `<script> tag was provided.. running script content` - Se viene individuato il tag script
- `Message: The output from user scripts` - Se vengono eseguiti script di dati utente, il loro output viene registrato

EC2Config

Il file di log per EC2config è `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log`. Le informazioni seguenti vengono registrate durante l'esecuzione dei dati utente:

- `Ec2HandleUserData: Message: Start running user scripts` - L'inizio dell'esecuzione dei dati utente
- `Ec2HandleUserData: Message: Re-enabled userdata execution` - Se viene individuato il tag persist

- `Ec2HandleUserData: Message: Could not find <persist> and </persist>` - Se non viene individuato il tag persist
- `Ec2HandleUserData: Message: The output from user scripts` - Se vengono eseguiti script di dati utente, il loro output viene registrato

Avvii o riavvii successivi

Quando aggiorni i dati utente dell'istanza, gli script dei dati utente non vengono eseguiti in modo automatico al riavvio dell'istanza. Tuttavia, puoi abilitare l'esecuzione dei dati utente in modo che gli script dei dati utente vengano eseguiti una volta al riavvio dell'istanza o ogni volta che riavvii l'istanza.

Selezionando l'opzione Shutdown with Sysprep (Arresta con Sysprep), gli script dei dati utente vengono eseguiti al successivo avvio o riavvio dell'istanza, anche se non hai abilitato l'esecuzione dei dati utente per i riavvii o avvii successivi. Gli script dei dati utente non verranno eseguiti ai riavvii o agli avvii successivi.

Per abilitare l'esecuzione dei dati utente con EC2Launch v2 (Anteprima AMI)

- Per eseguire un'attività nei dati utente al primo avvio, impostare `frequency` su `once`.
- Per eseguire un'attività nei dati utente ad ogni avvio, impostare `frequency` su `always`.

Abilitazione dell'esecuzione dei dati utente con EC2Launch (Windows Server 2016 o versioni successive)

1. Connettersi all'istanza Windows.
2. Aprire una finestra di PowerShell comando ed eseguire il comando seguente:

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
   ```

3. Disconnettersi dall'istanza Windows. Per eseguire gli script aggiornati al prossimo avvio dell'istanza, arresta l'istanza e aggiorna i dati utente.

Per abilitare l'esecuzione dei dati utente con EC2Config (Windows Server 2012 R2 e versioni precedenti)

1. Connettersi all'istanza Windows.
2. Aprire `C:\Program Files\Amazon\Ec2ConfigService \Ec2ConfigServiceSetting.exe`.

3. Per Dati utente, seleziona Abilita UserData l'esecuzione per il prossimo avvio del servizio.
4. Disconnettersi dall'istanza Windows. Per eseguire gli script aggiornati al prossimo avvio dell'istanza, arresta l'istanza e aggiorna i dati utente.

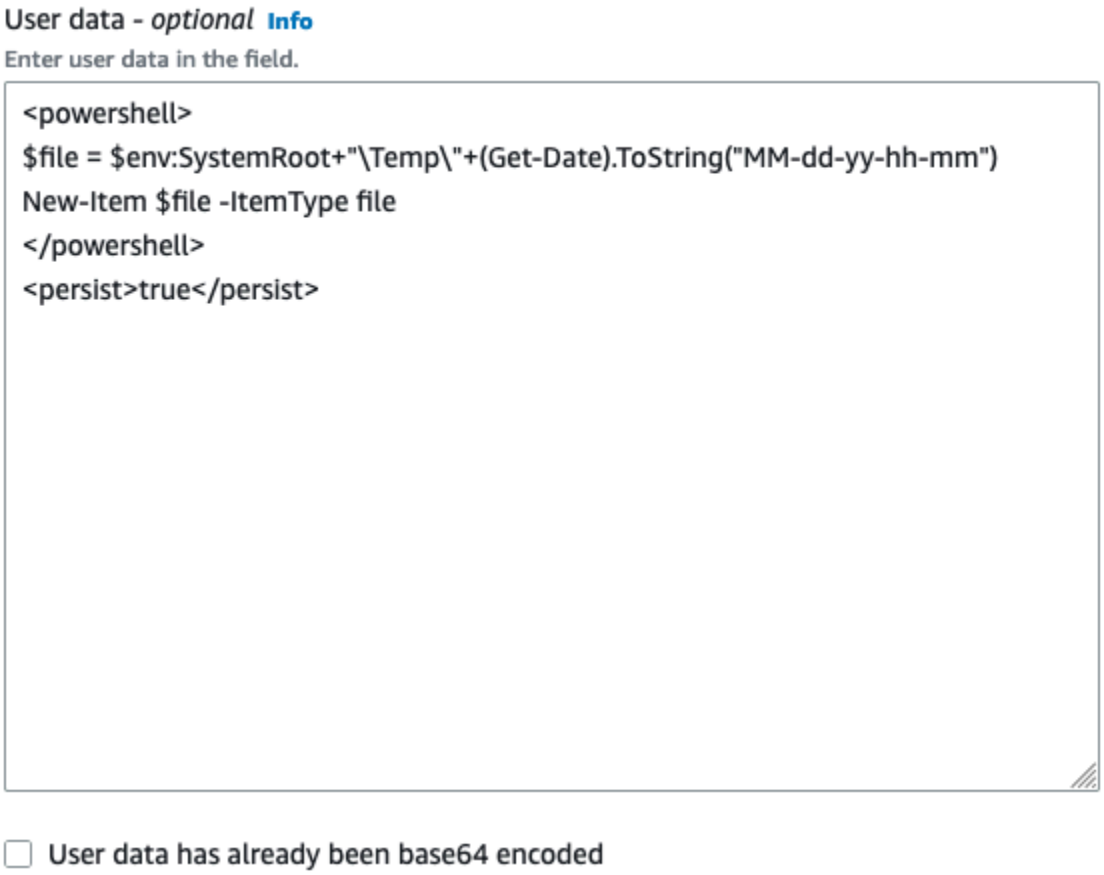
Dati utente e console

Puoi specificare i dati utente dell'istanza al momento dell'avvio dell'istanza. Se il volume root dell'istanza è un volume EBS, puoi anche arrestare l'istanza e aggiornare i relativi dati utente.

Specifica dei dati utente dell'istanza all'avvio

Segui la procedura per l'avvio di un'istanza. Il campo User data (Dati utente) campo si trova nella sezione Dettagli avanzati della procedura guidata di avvio dell'istanza. Inserisci PowerShell lo script nel campo Dati utente, quindi completa la procedura di avvio dell'istanza.

Nel seguente screenshot del campo Dati utente, lo script di esempio crea un file nella cartella temporanea di Windows, utilizzando la data e l'orario correnti nel nome del file. Quando includi `<persist>true</persist>`, lo script viene eseguito ogni volta che riavvii o avvii l'istanza. Se lasci vuota la casella di controllo I dati utente sono già stati codificati in base64, la console Amazon EC2 esegue la codifica in base64 per te.



Visualizzazione e aggiornamento dei dati utente dell'istanza

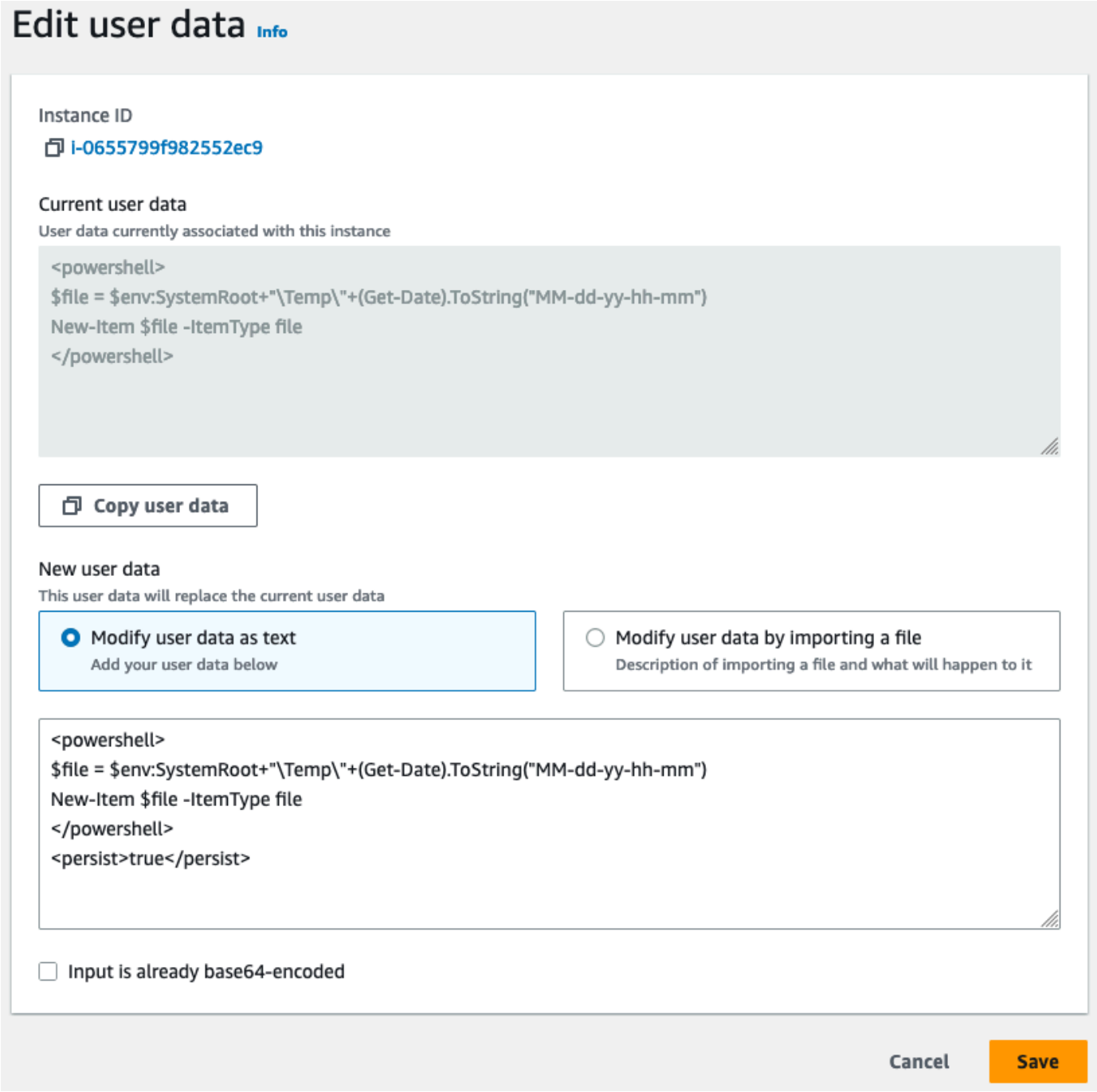
Puoi visualizzare i dati utente dell'istanza per qualsiasi istanza, oltre a poter aggiornare i dati utente dell'istanza per un'istanza arrestata.

Aggiornamento dei dati utente di un'istanza tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza e scegliere Actions (Operazioni), Instance state (Stato istanza), Stop (Arresta).

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

4. Quando viene richiesta la conferma, selezionare Stop (Arresta). Possono essere necessari alcuni minuti per arrestare l'istanza.
5. Con l'istanza ancora selezionata, selezionare Actions (Operazioni), Instance Settings (Impostazioni istanza), Edit user data (Modifica i dati utente). Non puoi modificare i dati utente se l'istanza è in esecuzione, ma puoi visualizzarli.
6. Nella finestra di dialogo Edit user data (Modifica i dati utente), aggiorna i dati utente, quindi scegli Save (Salva). Per eseguire gli script dei dati utente ogni volta che riavvii o avvii l'istanza, aggiungi `<persist>true</persist>`, come illustrato nell'esempio seguente:



7. Avviare l'istanza. Se hai abilitato l'esecuzione dei dati utente per i riavvii o gli avvii successivi, gli script dei dati utente aggiornati vengono eseguiti come parte del processo di avvio dell'istanza.

Dati utente e strumenti per Windows PowerShell

È possibile utilizzare gli strumenti per Windows PowerShell per specificare, modificare e visualizzare i dati utente per l'istanza. Per informazioni sulla visualizzazione dei dati utente dall'istanza tramite

metadati dell'istanza, consulta Recupero dei dati utente dell'istanza dall'istanza. Per informazioni sui dati utente e su AWS CLI, vederel dati dell'utente e il AWS CLI.

Esempio: Specificare i dati utente dell'istanza all'avvio

Creare un file di testo con i dati utente dell'istanza. Per eseguire gli script dei dati utente ogni volta che si riavvia o avvia l'istanza, aggiungere `<persist>true</persist>`, come illustrato nell'esempio seguente:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Per specificare i dati utente dell'istanza all'avvio dell'istanza, utilizza il New-EC2Instancecomando. Questo comando non esegue la codifica base64 al tuo posto dei dati utente. Utilizza i seguenti comandi per codificare i dati utente in un file di testo denominato `script.txt`.

```
PS C:\> $Script = Get-Content -Raw script.txt
PS C:\> $UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Utilizzare il parametro `-UserData` per trasferire i dati utente al comando New-EC2Instance.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
    -KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
    -UserData $UserData
```

Esempio: Aggiornamento dei dati utente dell'istanza di un'istanza arrestata

È possibile modificare i dati utente di un'istanza interrotta utilizzando il Edit-EC2InstanceAttributecomando.

Creare un file di testo con il nuovo script. Utilizza i seguenti comandi per codificare i dati utente nel file di testo denominato `new-script.txt`.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
```

```
PS C:\> $NewUserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Utilizzare i parametri `-UserData` e `-Value` per specificare i dati utente.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Esempio: Visualizzazione dei dati utente dell'istanza

Per recuperare i dati utente per un'istanza, utilizzate il Get-EC2InstanceAttributecomando.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
 userData).UserData
```

Di seguito è riportato un output di esempio. Tieni presente che i dati utente sono codificati.

```
PHBvd2Vyc2hlbGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Utilizzare i comandi seguenti per archiviare i dati utente codificati in una variabile e poi decodificarli.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded)
```

Di seguito è riportato un output di esempio.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Esempio: rinominare l'istanza per corrispondere al valore di tag

È possibile utilizzare il Get-EC2Tagcomando per leggere il valore del tag, rinominare l'istanza al primo avvio in modo che corrisponda al valore del tag e riavviare. Per eseguire efficacemente questo

comando, è necessario disporre di un ruolo con autorizzazioni `ec2:DescribeTags` collegate all'istanza, perché le informazioni sul tag sono recuperate da una chiamata all'API. Per ulteriori informazioni sulle autorizzazioni delle impostazioni utilizzando i ruoli IAM, consulta. Collegamento di un ruolo IAM all'istanza

```
<powershell>
 $instanceId = (invoke-webrequest http://169.254.169.254/latest/meta-data/instance-id -
UseBasicParsing).content
 $nameValue = (get-ec2tag -filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

È inoltre possibile rinominare l'istanza utilizzando i tag nei metadati delle istanze, se l'istanza è configurata su access tags from the instance metadata (accedi ai tag dai metadati dell'istanza). Per ulteriori informazioni, consulta Utilizzo dei tag dell'istanza nei metadati dell'istanza.

```
<powershell>
 $nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Recupera dati dinamici dalla tua istanza

Per recuperare dati dinamici da un'istanza in esecuzione, utilizza uno dei seguenti URI. Per recuperare i dati utente utilizzando l'indirizzo IPv6, è necessario abilitarlo e l'istanza deve essere un'istanza creata sul sistema AWS Nitro in una sottorete che supporta IPv6.

IPv4

```
http://169.254.169.254/latest/dynamic/
```

IPv6

```
http://[fd00:ec2::254]/latest/dynamic/
```

Questo esempio recupera le categorie di identità delle istanze di alto livello.

cURL

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

PowerShell

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

Per ulteriori informazioni sui dati dinamici e per esempi di come recuperarli, consulta Documenti di identità dell'istanza.

Categorie di metadati dell'istanza

I metadati dell'istanza sono suddivisi in categorie. Per recuperare i metadati dell'istanza, specifica la categoria nella richiesta e i metadati verranno restituiti nella risposta.

Quando vengono rilasciate nuove categorie, viene creata una nuova build di metadati di istanza con un nuovo numero di versione. Nella tabella che segue, la colonna Version when category was released (Versione in cui è stata rilasciata la categoria) specifica la versione di build quando è stata rilasciata una categoria di metadati dell'istanza. Per evitare di dover aggiornare il codice ogni volta che Amazon EC2 rilascia una nuova build di metadati dell'istanza, utilizza `latest` invece del numero di versione nelle richieste di metadati. Per ulteriori informazioni, consulta Recupero delle versioni disponibili dei metadati dell'istanza.

Quando Amazon EC2 rilascia una nuova categoria di metadati dell'istanza, i metadati dell'istanza per la nuova categoria potrebbero non essere disponibili per le istanze esistenti. Con istanze costruite sul Sistema Nitro, è possibile recuperare i metadati dell'istanza solo per le categorie disponibili al

momento dell'avvio. Per le istanze con l'hypervisor Xen, è possibile arrestare e avviare l'istanza per aggiornare le categorie disponibili.

Nella tabella seguente sono elencate le categorie di metadati dell'istanza. Alcuni dei nomi delle categorie includono segnaposti per i dati univoci dell'istanza. Ad esempio, *mac* rappresenta l'indirizzo MAC per l'interfaccia di rete. Quando richiami i metadati dell'istanza, devi sostituire i segnaposti con i valori effettivi.

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
ami-id	ID dell'AMI utilizzata per avviare l'istanza.	1
ami-launch-index	Se si avviano più istanze utilizzando la stessa RunInstances chiamata, questo valore indica l'ordine di avvio per ciascuna istanza. Il valore della prima istanza avviata è 0. Se avvii istanze utilizzando Auto Scaling o la flotta EC2, questo valore è sempre 0.	1
ami-manifest-path	Percorso del file manifest dell'AMI in Amazon S3. Se hai utilizzato un'AMI supportata da Amazon EBS per avviare l'istanza, il valore restituito è unknown.	1
ancestor-ami-ids	ID dell'AMI di qualsiasi istanza raggruppata per creare l'AMI corrente. Questo valore esiste solo se il file manifest dell'AMI contiene una chiave ancestor-amis .	10-10-2007
autoscaling/target-lifecycle-state	Valore che mostra lo stato del ciclo di vita di Auto Scaling di destinazi	2021-07-15

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
	one a cui sta passando un'istanza di Auto Scaling. Presente quando l'istanza passa a uno degli stati del ciclo di vita di destinazione dopo il 10 marzo 2022. Valori possibili: `Detached` | `InService` | `Standby` | `Terminated` | `Warmed:Hibernated` | `Warmed:Running` | `Warmed:Stopped` | `Warmed:Terminated`. Consulta la sezione Recupero dello stato del ciclo di vita tramite i metadati dell'istanza nella Guida per l'utente di Amazon EC2 Auto Scaling.	
`block-device-mapping/ami`	Dispositivo virtuale contenente il file system radice/di avvio.	15-12-2007
`block-device-mapping/ebs` N	Dispositivi virtuali associati a qualsiasi volume Amazon EBS. I volumi Amazon EBS sono disponibili solo nei metadati se erano presenti al momento dell'avvio o quando l'istanza è stata avviata per l'ultima volta. N indica il valore di indice del volume Amazon EBS (ad esempio `ebs1` o `ebs2`).	15-12-2007

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`block-device-mapping/ephemeral` N	I dispositivi virtuali per qualsiasi volume instance store non NVMe. La N indica l'indice di ogni volume. Il numero di volumi instance store nella mappatura del dispositivo a blocchi potrebbero non corrispondere al numero effettivo dei volumi instance store per l'istanza. Il tipo di istanza determina il numero di volumi instance store disponibili per un'istanza. Se il numero di volumi instance store in una mappatura dei dispositivi a blocchi supera il numero disponibile per un'istanza, i volumi instance store aggiuntivi vengono ignorati.	15-12-2007
`block-device-mapping/root`	Dispositivi o partizioni virtuali associati ai dispositivi o alle partizioni radice sul dispositivo virtuale, dove il file system radice (/ o C:) è associato all'istanza specificata.	15-12-2007
`block-device-mapping/swap`	Dispositivi virtuali associati a `swap`. Non sempre presenti.	15-12-2007
`elastic-gpus/associations/` *`elastic-gpu-id`*	Se è presente una GPU elastica collegata all'istanza, include una stringa JSON con le informazioni relative alla GPU elastica, compresi il relativo ID e le informazioni di connessione.	30-11-2016

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`elastic-inference/associations/` *`eia-id`*	Se è presente un acceleratore Elastic Inference collegato all'istanza, contiene una stringa JSON con informazioni sull'acceleratore Elastic Inference, inclusi l'ID e il tipo.	2018-11-29
`events/maintenance/history`	Se sono presenti eventi di manutenzione completati o cancellati per l'istanza, contiene una stringa JSON con informazioni sugli eventi.	17-08-2018
`events/maintenance/scheduled`	Se sono presenti eventi di manutenzione attivi per l'istanza, contiene una stringa JSON con informazioni sugli eventi. Per ulteriori informazioni, consulta Visualizzazione degli eventi pianificati.	17-08-2018
`events/recommendations/rebalance`	Ora approssimativa, in UTC, in cui viene emessa la notifica della raccomandazione di ribilanciamento dell'istanza EC2 per l'istanza. Di seguito è riportato un esempio dei metadati per questa categoria: `{"noticeTime": "2020-11-05T08:22:00Z"}` . Questa categoria è disponibile solo dopo che la notifica è stata emessa. Per ulteriori informazioni, consulta Raccomandazioni per il ribilanciamento delle istanze EC2.	2020-10-27

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`hostname`	Se l'istanza EC2 utilizza la denominazione basata su IP (IPBN), questo è il nome host DNS IPv4 privato dell'istanza. Se l'istanza EC2 utilizza la denominazione basata su risorse (RBN), questo è l'RBN. Se sono presenti più interfacce di rete, fa riferimento al dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0). Per ulteriori informazioni su IPBN e RBN, consultare Tipi di nomi host delle istanze Amazon EC2.	1
`iam/info`	Se all'istanza è associato un ruolo IAM, contiene informazioni sull'ultima volta in cui il profilo dell'istanza è stato aggiornato, inclusa la LastUpdated data dell'istanza, e. InstanceProfileArn InstanceProfileId In caso contrario, non presente.	12-01-2012
`iam/security-credentials/role-name`	Se è presente un ruolo IAM associato all'istanza, *`role-name`* rappresenta il nome del ruolo e *`role-name`* contiene le credenziali di sicurezza temporane e associate al ruolo (per ulteriori informazioni, consulta Recupero delle credenziali di sicurezza dai metadati delle istanze). In caso contrario, non presente.	12-01-2012

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`identity-credentials/ec2/info`	Informazioni sulle credenziali in `identity-credentials/ec2/security-credentials/ec2-instance` .	23/05/2018
`identity-credentials/ec2/security-credentials/ec2-instance`	Credenziali per il ruolo di identità dell'istanza che consente al software sull'istanza di AWS identificarsi per supportare funzionalità come EC2 Instance Connect e AWS Systems Manager Default Host Management Configuration. Queste credenziali non hanno policy associate, quindi non dispongono di autorizzazioni AWS API aggiuntive oltre all'identificazione dell'istanza e della funzionalità. AWS Per ulteriori informazioni, consulta Ruoli di identità dell'istanza.	23/05/2018
`instance-action`	Comunica all'istanza la necessità di un riavvio in preparazione del processo di raggruppamento. Valori validi: `none` | `shutdown` | `bundle-pending` .	01-09-2008
`instance-id`	ID dell'istanza corrente.	1
`instance-life-cycle`	L'opzione di acquisto di questa istanza. Per ulteriori informazioni, consulta Opzioni di acquisto delle istanze.	01-10-2019

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`instance-type`	Tipo di istanza. Per ulteriori informazioni, consulta Tipi di istanza Amazon EC2.	29-08-2007
`ipv6`	L'indirizzo IPv6 dell'istanza. Se sono presenti più interfacce di rete, fa riferimento all'interfaccia di rete del dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0) e al primo indirizzo IPv6 assegnato. Se non esiste un indirizzo IPv6 sull'interfaccia di rete [0], questo elemento non viene impostato e viene restituita una risposta HTTP 404.	2021-01-03
`kernel-id`	ID del kernel avviato con questa istanza, se applicabile.	01-02-2008
`local-hostname`	Se sono presenti più interfacce di rete, fa riferimento al dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0). Se l'istanza EC2 utilizza la denominazione basata su IP (IPBN), questo è il nome host DNS IPv4 privato dell'istanza. Se l'istanza EC2 utilizza la denominazione basata su risorse (RBN), questo è l'RBN. Per ulteriori informazioni sulla denominazione delle istanze IPBN, RBN ed EC2, consultare Tipi di nomi host delle istanze Amazon EC2.	19-01-2007

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`local-ipv4`	Indirizzo IPv4 privato dell'istanza. Se sono presenti più interfacce di rete, fa riferimento al dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0). Se si tratta di un'istanza solo IPv6, questo elemento non è impostato e restituisce una risposta HTTP 404.	1
`mac`	Indirizzo MAC (Media Access Control) dell'istanza. Se sono presenti più interfacce di rete, fa riferimento al dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0).	01-01-2011
`metrics/vhostmd`	Non più disponibile.	2011-05-01
`network/interfaces/macs/mac/device-number`	Numero di dispositivo univoco associato all'interfaccia specificata. Il numero di dispositivo corrisponde al nome del dispositivo, ad esempio `device-number` pari a 2 indica il dispositivo eth2. Questa categoria corrisponde ai campi `DeviceIndex` e `device-index` utilizzati dall'API Amazon EC2 e ai comandi EC2 per AWS CLI.	01-01-2011
`network/interfaces/macs/mac/interface-id`	L'ID dell'interfaccia di rete.	01-01-2011

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`network/interfaces/macs/mac/ipv4-associations/public-ip`	Indirizzi IPv4 privati associati a ogni indirizzo IP pubblico e assegnati all'interfaccia specificata.	01-01-2011
`network/interfaces/macs/mac/ipv6s`	Gli indirizzi IPv6 assegnati all'interfaccia.	30-06-2016
`network/interfaces/macs/mac/ipv6-prefix`	Il prefisso IPv6 assegnato all'interfaccia di rete.	
`network/interfaces/macs/mac/local-hostname`	Nome host DNS IPv4 privato dell'istanza. Se sono presenti più interfacce di rete, fa riferimento al dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0). Se si tratta di un'istanza solo IPv6, questo è il nome basato sulle risorse. Per ulteriori informazioni su IPBN e RBN, consultare Tipi di nomi host delle istanze Amazon EC2.	19-01-2007
`network/interfaces/macs/mac/local-ipv4s`	Indirizzi IPv4 privati associati all'interfaccia. Se questa è un'interfaccia di rete solo IPv6, questo elemento non è impostato e restituisce una risposta HTTP 404.	01-01-2011
`network/interfaces/macs/mac/mac`	Indirizzo MAC dell'istanza.	01-01-2011
`network/interfaces/macs/`*`mac`*`/network-card`	L'indice della scheda di rete. Alcuni tipi di istanza supportano più schede di rete.	2020-11-01

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`network/interfaces/macs/mac/owner-id`	ID del proprietario dell'interfaccia di rete. In ambienti con più interfacce, un'interfaccia può essere collegata mediante una terza parte, ad esempio Elastic Load Balancing . Il traffico di un'interfaccia viene sempre addebitato al proprietario dell'interfaccia.	01-01-2011
`network/interfaces/macs/mac/public-hostname`	DNS pubblico (IPv4) dell'interfaccia. Questa categoria viene restituita solo se l'attributo `enableDnsHostnames` è impostato su `true`. Per ulteriori informazioni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC. Se l'istanza ha solo un indirizzo IPv6 pubblico e nessun indirizzo IPv4 pubblico, questo elemento non è impostato e restituisce una risposta HTTP 404.	01-01-2011
`network/interfaces/macs/mac/public-ipv4s`	L'indirizzo IP pubblico o gli indirizzi IP elastici associati all'interfaccia. In un'istanza possono essere presenti più indirizzi IPv4.	01-01-2011
`network/interfaces/macs/mac/security-groups`	Gruppi di sicurezza a cui appartiene l'interfaccia di rete.	01-01-2011

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`network/interfaces/macs/mac/security-group-ids`	ID dei gruppi di sicurezza a cui appartiene l'interfaccia di rete.	01-01-2011
`network/interfaces/macs/mac/subnet-id`	ID della sottorete in cui si trova l'interfaccia di rete.	01-01-2011
`network/interfaces/macs/mac/subnet-ipv4-cidr-block`	Blocco CIDR IPv4 della sottorete in cui si trova l'interfaccia di rete.	01-01-2011
`network/interfaces/macs/mac/subnet-ipv6-cidr-blocks`	Blocco CIDR IPv6 della sottorete in cui si trova l'interfaccia di rete.	30-06-2016
`network/interfaces/macs/mac/vpc-id`	ID del VPC in cui si trova l'interfaccia di rete.	01-01-2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-block`	Blocco CIDR IPv4 primario del VPC.	01-01-2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-blocks`	Blocchi CIDR IPv4 del VPC.	30-06-2016
`network/interfaces/macs/mac/vpc-ipv6-cidr-blocks`	Blocco CIDR IPv6 del VPC in cui si trova l'interfaccia di rete.	30-06-2016
`placement/availability-zone`	zona di disponibilità in cui l'istanza è stata avviata.	01-02-2008

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`placement/availability-zone-id`	ID dell'area di disponibilità statica in cui viene avviata l'istanza. L'ID dell'area di disponibilità è coerente tra gli account. Tuttavia, potrebbe essere diverso dall'area di disponibilità, che può variare in base all'account.	01-10-2019
`placement/group-name`	Nome del gruppo di posiziona mento in cui viene avviata l'istanza.	2020-08-24
`placement/host-id`	ID dell'host su cui viene avviata l'istanza. Applicabile solo a Host dedicati.	2020-08-24
`placement/partition-number`	Il numero della partizione in cui viene avviata l'istanza.	2020-08-24
`placement/region`	La AWS regione in cui viene avviata l'istanza.	2020-08-24
`product-codes`	Marketplace AWS eventuali codici di prodotto associati all'istanza.	01-03-2007

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`public-hostname`	Il DNS pubblico dell'istanza (IPv4). Questa categoria viene restituit a solo se l'attributo `enableDns Hostnames` è impostato su `true`. Per ulteriori informazi oni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC. Se l'istanza ha solo un indirizzo IPv6 pubblico e nessun indirizzo IPv4 pubblico, questo elemento non è impostato e restituisce una risposta HTTP 404.	19-01-2007
`public-ipv4`	Indirizzo IPv4 pubblico. Se un indirizzo IP elastico è associato all'istanza, il valore restituito è l'indirizzo IP elastico.	19-01-2007
`public-keys/0/openssh-key`	Chiave pubblica. Disponibile solo se viene specificato in fase di avvio dell'istanza.	1
`ramdisk-id`	ID del disco RAM specificato in fase di avvio, se applicabile.	10-10-2007
`reservation-id`	ID della prenotazione.	1
`security-groups`	Nomi dei gruppi di sicurezza applicati all'istanza. Dopo l'avvio puoi modificare i gruppi di sicurezza delle istanze. Tali modifiche verranno implement ate qui e in network/interfaces/ macs/*mac*/security-groups.	1

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`services/domain`	Il dominio per AWS le risorse per la regione.	25-2-2014
`services/partition`	Partizione in cui si trova la risorsa. Per AWS le regioni standard, la partizione è`aws`. Se sono presenti risorse in altre partizioni, la partizione è `aws-`*`partition name`* . Ad esempio, la partizione per le risorse nella regione Cina (Pechino) è `aws-cn`.	20-10-2015
`spot/instance-action`	Operazione (ibernazione, arresto o terminazione) e orario indicativo, in UTC, in cui si verificherà l'operazione. Questo elemento è presente solo se l'istanza spot è stata contrassegnata per essere ibernata, arrestata o terminata. Per ulteriori informazioni, consulta instance-action.	15-11-2016

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`spot/termination-time`	Ora approssimativa, in formato UTC, in cui il sistema operativo dell'istanza spot riceverà il segnale di arresto. Questo elemento è presente e contiene un valore orario, ad esempio 2015-01-05T18:02:00Z, solo se l'istanza spot è stata contrassegnata per essere interrotta da Amazon EC2. L'elemento "termination-time" non è impostato su un'ora se termini manualmente l'istanza spot. Per ulteriori informazioni, consulta termination-time.	05-11-2014
`tags/instance`	I tag istanza associati all'istanza. Disponibile solo se permetti esplicitamente l'accesso ai tag nei metadati dell'istanza. Per ulteriori informazioni, consulta Per consentire l'accesso ai tag nei metadati delle istanze.	2021-03-23

Categorie dei dati dinamici

Nella tabella seguente sono elencate le categorie dei dati dinamici.

Categoria	Descrizione	Versione in cui è stata rilasciata la categoria
`fws/instance-monitoring`	Valore che indica se il cliente ha abilitato il monitoraggio dettagliato in un minuto. CloudWatch Valori validi: `enabled | disabled`	04-04-2009
`instance-identity/document`	JSON contenente gli attributi dell'istanza, ad esempio ID istanza, indirizzo IP privato e così via Per informazioni, consulta Documenti di identità dell'istanza.	04-04-2009
`instance-identity/pkcs7`	Utilizzato per verificare l'autenticità e i contenuti del documento in base alla firma. Per informazioni, consulta Documenti di identità dell'istanza.	04-04-2009
`instance-identity/signature`	Dati che possono essere utilizzati da altre parti per verificare la relativa origine e autenticità. Per informazioni, consulta Documenti di identità dell'istanza.	04-04-2009

Esempio Linux: valore dell'indice di lancio AMI

Questo esempio dimostra come è possibile utilizzare sia i dati utente che i metadati delle istanze per configurare le istanze Linux.

> **Note**
>
> Negli esempi riportati in questa sezione viene utilizzato l'indirizzo IPv4 del servizio di metadati dell'istanza (IMDS): `169.254.169.254`. Se si recuperano i metadati per le istanze EC2 tramite l'indirizzo IPv6, accertarsi invece di abilitare e utilizzare l'indirizzo IPv6: `[fd00:ec2::254]`. L'indirizzo IPv6 del servizio di metadati dell'istanza (IMDS) è compatibile con i comandi IMDSv2. L'indirizzo IPv6 è accessibile solo sulle istanze create sul sistema AWS Nitro e in una sottorete supportata da IPv6 (dual stack o solo IPv6).

Alice vuole avviare quattro istanze dell'AMI del suo database preferito, dove la prima istanza funge da istanza originale e le altre tre fungono da repliche. Al momento dell'avvio vuole aggiungere i dati utente relativi alla strategia di replica per ciascuna replica. Consapevole del fatto che questi dati saranno disponibili per tutte e quattro le istanze, deve strutturare i dati utente in modo da consentire a ciascuna istanza di riconoscere le parti valide. A tale scopo, utilizza il valore `ami-launch-index` dei metadati dell'istanza, che sarà univoco per ogni istanza. Se hai avviato più di un'istanza contemporaneamente, il `ami-launch-index`indica l'ordine in base al quale sono state avviate le istanze. Il valore della prima istanza avviata è `0`.

Di seguito sono descritti i dati utente strutturati da Alice.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

I dati `replicate-every=1min` definiscono la configurazione della prima replica, `replicate-every=5min` definisce la configurazione della seconda replica e così via. Alice decide di specificare questi dati come stringa ASCII con una barra verticale (`|`) per delimitare i dati per le singole istanze.

Alice avvia le quattro istanze utilizzando il comando run-instances e specificando i dati utente.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Dopo l'avvio, le istanze includono una copia dei dati utente e i metadati comuni riportati di seguito:

- ID AMI: ami-0abcdef1234567890
- ID prenotazione: r-1234567890abcabc0
- Chiavi pubbliche: nessuna
- Nome del gruppo di sicurezza: nome di default
- Tipo di istanza: t2.micro

Tuttavia, ogni istanza ha metadati unici, come illustrato nelle tabelle seguenti.

Metadati	Valore
instance-id	i-1234567890abcdef0

Metadati	Valore
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

Metadati	Valore
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

Metadati	Valore
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal

Metadati	Valore
local-ipv4	10.251.50.37

Metadati	Valore
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice può utilizzare il valore `ami-launch-index` per determinare la parte di dati utente validi per un'istanza specifica.

1. Collega una delle istanze e recupera il valore `ami-launch-index` per tale istanza per assicurarsi che sia una delle repliche:

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

   Per le fasi seguenti, le richieste IMDSv2 utilizzano il token memorizzato dal comando IMDSv2 precedente, presupponendo che non sia scaduto.

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

2. Salva il valore `ami-launch-index` come una variabile.

   IMDSv2

   ```
   [ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/meta-data/ami-launch-index`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-
   launch-index`
   ```

3. Salva i dati utente come una variabile.

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/user-data`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
   ```

4. Alice utilizza infine il comando cut per estrarre la parte di dati utente valida per l'istanza specifica.

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

   IMDSv1

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

Documenti di identità dell'istanza

Ogni istanza avviata dispone di un Documenti di identità dell'istanza che fornisce informazioni sull'istanza stessa. Puoi utilizzare il Documenti di identità dell'istanza per convalidare gli attributi dell'istanza.

Il documento di identità dell'istanza viene generato quando l'istanza viene arrestata e avviata, riavviata o avviata. Il documento di identità dell'istanza viene esposto (in formato JSON di testo normale) tramite il servizio di metadati dell'istanza (IMDS). L'indirizzo IPv4 `169.254.169.254` è un indirizzo link-local ed è valido solo dall'istanza. Per ulteriori informazioni, consultare Indirizzo link-local su Wikipedia. L'indirizzo IPv6 `[fd00:ec2::254]` è un indirizzo locale univoco ed è valido solo dall'istanza. Per ulteriori informazioni, consulta Indirizzo locale univoco su Wikipedia.

> **Note**
>
> Negli esempi riportati in questa sezione viene utilizzato l'indirizzo IPv4 del servizio di metadati dell'istanza (IMDS): `169.254.169.254`. Se si recuperano i metadati per le istanze EC2 tramite l'indirizzo IPv6, accertarsi invece di abilitare e utilizzare l'indirizzo IPv6: `[fd00:ec2::254]`. L'indirizzo IPv6 del servizio di metadati dell'istanza (IMDS) è compatibile con i comandi IMDSv2. L'indirizzo IPv6 è accessibile solo sulle istanze create sul sistema AWS Nitro e in una sottorete supportata da IPv6 (dual stack o solo IPv6).

Puoi recuperare il Documenti di identità dell'istanza da un'istanza in esecuzione in qualsiasi momento. Il Documenti di identità dell'istanza include le seguenti informazioni:

Dati	Descrizione
`accountId`	L' AWS ID dell'account che ha avviato l'istanza.
`architecture`	L'architettura dell'AMI utilizzata per avviare l'istanza (i386 | x86_64 | arm64).
`availabilityZone`	Zona di disponibilità in cui viene eseguita l'istanza.
`billingProducts`	I prodotti di fatturazione dell'istanza.
`devpayProductCodes`	Obsoleta.
`imageId`	L'ID dell'AMI utilizzato per avviare l'istanza.
`instanceId`	ID dell'istanza.

Dati	Descrizione
`instanceType`	Il tipo di istanza dell'istanza.
`kernelId`	L'ID del kernel associato all'istanza, se applicabile.
`marketplaceProductCodes`	Il codice Marketplace AWS prodotto dell'AMI utilizzato per avviare l'istanza.
`pendingTime`	La data e l'ora in cui l'istanza è stata avviata.
`privateIp`	Indirizzo IPv4 privato dell'istanza.
`ramdiskId`	L'ID del disco RAM associato a questa istanza, se applicabile.
`region`	La regione in cui viene eseguita l'istanza.
`version`	Versione del formato del Documenti di identità dell'istanza.

Recuperare l'Documenti di identità dell'istanza di testo normale

Per recuperare il Documenti di identità dell'istanza di testo normale

Connettersi all'istanza ed eseguire il comando riportato di seguito.

Linux

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/document
```

IMDSv1

```
$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token}
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

IMDSv1

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/
document).Content
```

Di seguito è riportato un output di esempio.

```
{
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
    "ramdiskId" : null,
    "region" : "us-west-2"
}
```

Verificare l'Documenti di identità dell'istanza

Se si intende utilizzare i contenuti del Documenti di identità dell'istanza per uno scopo importante, occorre verificarne il contenuto e l'autenticità prima di utilizzarlo.

Il Documenti di identità dell'istanza di testo normale è accompagnato da tre firme con hash e crittografate. Puoi utilizzare queste firme per verificare l'origine e l'autenticità del Documenti di identità dell'istanza e delle informazioni incluse. Vengono fornite le seguenti firme:

- Firma con codifica base64: si tratta di un hash SHA256 con codifica base64 del Documenti di identità dell'istanza che è stato crittografato utilizzando una coppia di chiavi RSA.
- Firma PKCS7: si tratta di un hash SHA1 del Documenti di identità dell'istanza che è crittografato utilizzando una coppia di chiavi DSA.
- Firma RSA-2048: si tratta di un hash SHA256 del Documenti di identità dell'istanza crittografato utilizzando una coppia di chiavi RSA-2048.

Ogni firma è disponibile in un endpoint diverso nei metadati dell'istanza. Puoi utilizzare una di queste firme qualsiasi a seconda dei requisiti di hashing e di crittografia. Per verificare le firme, è necessario utilizzare il certificato AWS pubblico corrispondente.

Negli argomenti seguenti vengono illustrate le fasi dettagliate di convalida dell'indirizzo Documenti di identità dell'istanza utilizzando ogni firma.

- Utilizzo della firma PKCS7 per verificare il Documenti di identità dell'istanza
- Utilizzo della firma con codifica base64 per verificare l'Documenti di identità dell'istanza
- Utilizzo della firma RSA-2048 per verificare l'Documenti di identità dell'istanza

Utilizzo della firma PKCS7 per verificare il Documenti di identità dell'istanza

Questo argomento spiega come verificare il documento di identità dell'istanza utilizzando la firma PKCS7 e il certificato pubblico AWS DSA.

Istanze Linux

Per verificare il documento di identità dell'istanza utilizzando la firma PKCS7 e il certificato pubblico DSA AWS

1. Collegati all'istanza.
2. Recuperare la firma PKCS7 dai metadati dell'istanza e aggiungerla a un file denominato `pkcs7` insieme all'intestazione e al piè di pagina richiesti. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

IMDSv2

```
$ echo "-----BEGIN PKCS7-----" >> pkcs7 \
&& TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/pkcs7 >> pkcs7 \
&& echo "" >> pkcs7 \
&& echo "-----END PKCS7-----" >> pkcs7
```

IMDSv1

```
$ echo "-----BEGIN PKCS7-----" >> pkcs7 \
&& curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
 >> pkcs7 \
&& echo "" >> pkcs7 \
&& echo "-----END PKCS7-----" >> pkcs7
```

3. Trovare il certificato pubblico DSA per la propria regione in AWS certificati pubblici e aggiungere i contenuti in un nuovo file denominato `certificate`.
4. Utilizzare il comando OpenSSL smime per verificare la firma. Includere l'opzione `-verify` per indicare che la firma deve essere verificata e l'opzione `-noverify` per indicare che il certificato non deve essere verificato.

```
$ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
 document
```

Se la firma è valida, viene visualizzato il messaggio `Verification successful`.

Il comando, inoltre, scrive i contenuti del documento di identità dell'istanza in un nuovo file denominato `document`. Puoi confrontare i contenuti del documento di identità dell'istanza dai metadati dell'istanza con i contenuti di questo file utilizzando i comandi seguenti.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Se non è possibile verificare la firma, contattare AWS Support.

Istanze Windows

Prerequisiti

Questa procedura richiede la classe `System.Security` Microsoft .NET Core. Per aggiungere la classe alla PowerShell sessione, esegui il comando seguente.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Il comando aggiunge la classe solo alla PowerShell sessione corrente. Se avvii una nuova sessione, devi eseguire nuovamente il comando.

Per verificare il documento di identità dell'istanza utilizzando la firma PKCS7 e il certificato pubblico AWS DSA

1. Collegati all'istanza.
2. Recuperare la firma PKCS7 dai metadati dell'istanza, convertirla in un array di byte e aggiungerla a una variabile denominata `$Signature`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/pkcs7).Content)
   ```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```

3. Recuperare il documento di identità dell'istanza in testo normale dai metadati dell'istanza, convertirlo in un array di byte e aggiungerlo a una variabile denominata `$Document`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Trovare il certificato pubblico DSA per la propria regione in AWS certificati pubblici e aggiungere i contenuti in un nuovo file denominato `certificate.pem`.

5. Estrarre il certificato dal file del certificato e archiviarlo in una variabile denominata `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Verifica la firma.

   ```
   PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
   ```

   ```
   PS C:\> $SignatureDocument.Decode($Signature)
   ```

   ```
   PS C:\> $SignatureDocument.CheckSignature($Store, $true)
   ```

   Se la firma è valida, il comando non restituisce alcun output. Se non è possibile verificare la firma, il comando restituisce `Exception calling "CheckSignature" with "2"`

`argument(s): "Cannot find the original signer`. Se non è possibile verificare la firma, contattare AWS Support.

7. Convalidare il contenuto del documento di identità dell'istanza.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Se il contenuto del documento di identità dell'istanza è valido, il comando restituisce `True`. Se il documento di identità dell'istanza non può essere convalidato, contattare AWS Support.

Utilizzo della firma con codifica base64 per verificare l'Documenti di identità dell'istanza

Questo argomento spiega come verificare il documento di identità dell'istanza utilizzando la firma con codifica base64 e il certificato pubblico RSA. AWS

Istanze Linux

Per convalidare il documento di identità dell'istanza utilizzando la firma con codifica base64 e il certificato pubblico RSA AWS

1. Collegati all'istanza.
2. Recuperare la firma con codifica base64 dai metadati dell'istanza, convertirla in un formato binario e aggiungerla a un file denominato `signature`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/signature | base64 -d >> signature
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature |
    base64 -d >> signature
   ```

3. Recuperare il Documenti di identità dell'istanza in testo normale dai metadati dell'istanza e aggiungerlo a un file denominato `document`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document >> document
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
    >> document
   ```

4. Trovare il certificato pubblico RSA per la propria regione in AWS certificati pubblici e aggiungere i contenuti in un nuovo file denominato `certificate`.

5. Estrai la chiave pubblica dal certificato pubblico AWS RSA e salvala in un file denominato. `key`

   ```
   $ openssl x509 -pubkey -noout -in certificate >> key
   ```

6. Utilizzare il comando OpenSSL dgst per verificare il Documenti di identità dell'istanza.

   ```
   $ openssl dgst -sha256 -verify key -signature signature document
   ```

   Se la firma è valida, viene visualizzato il messaggio `Verification successful`.

   Il comando, inoltre, scrive i contenuti del documento di identità dell'istanza in un nuovo file denominato `document`. Puoi confrontare i contenuti del documento di identità dell'istanza dai metadati dell'istanza con i contenuti di questo file utilizzando i comandi seguenti.

   ```
   $ openssl dgst -sha256 < document
   ```

   ```
   $ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document | openssl dgst -sha256
   ```

   Se non è possibile verificare la firma, contattare AWS Support.

Istanze Windows

Per convalidare il documento di identità dell'istanza utilizzando la firma con codifica base64 e il certificato pubblico RSA AWS

1. Collegati all'istanza.
2. Recuperare la firma con codifica base64 dai metadati dell'istanza, convertirla in un array di byte e aggiungerla alla variabile denominata `$Signature`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/signature).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
   ```

3. Recuperare il documento di identità dell'istanza in testo normale dai metadati dell'istanza, convertirlo in un array di byte e aggiungerlo a una variabile denominata `$Document`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Trovare il certificato pubblico RSA per la propria regione in AWS certificati pubblici e aggiungere i contenuti in un nuovo file denominato `certificate.pem`.
5. Verificare il documento di identità dell'istanza.

```
PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-
Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
```

Se la firma è valida, il comando restituisce `True`. Se non è possibile verificare la firma, contattare AWS Support.

Utilizzo della firma RSA-2048 per verificare l'Documenti di identità dell'istanza

Questo argomento spiega come verificare il documento di identità dell'istanza utilizzando la firma RSA-2048 e il certificato pubblico RSA-2048. AWS

Istanze Linux

Per verificare il documento di identità dell'istanza utilizzando la firma RSA-2048 e il certificato pubblico RSA-2048 AWS

1. Collegati all'istanza.
2. Recuperare la firma RSA-2048 dai metadati dell'istanza e aggiungerla a un file denominato `rsa2048`, insieme all'intestazione e al piè di pagina richiesti. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
   && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/rsa2048 >> rsa2048 \
   && echo "" >> rsa2048 \
   && echo "-----END PKCS7-----" >> rsa2048
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
   ```

```
&& curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048
 >> rsa2048 \
&& echo "" >> rsa2048 \
&& echo "-----END PKCS7-----" >> rsa2048
```

3. Trovare il certificato pubblico RSA-2048 per la propria regione in AWS certificati pubblici e aggiungere i contenuti in un nuovo file denominato `certificate`.
4. Utilizzare il comando OpenSSL smime per verificare la firma. Includere l'opzione `-verify` per indicare che la firma deve essere verificata e l'opzione `-noverify` per indicare che il certificato non deve essere verificato.

   ```
   $ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |
    tee document
   ```

   Se la firma è valida, viene visualizzato il messaggio `Verification successful`. Se non è possibile verificare la firma, contattare AWS Support.

Istanze Windows

Prerequisiti

Questa procedura richiede la classe `System.Security` Microsoft .NET Core. Per aggiungere la classe alla PowerShell sessione, esegui il comando seguente.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Il comando aggiunge la classe solo alla PowerShell sessione corrente. Se avvii una nuova sessione, devi eseguire nuovamente il comando.

Per verificare il documento di identità dell'istanza utilizzando la firma RSA-2048 e il certificato pubblico RSA-2048 AWS

1. Collegati all'istanza.
2. Recuperare la firma RSA-2048 dai metadati dell'istanza, convertirla in un array di byte e aggiungerla a una variabile denominata `$Signature`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/rsa2048).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
```

3. Recuperare il documento di identità dell'istanza in testo normale dai metadati dell'istanza, convertirlo in un array di byte e aggiungerlo a una variabile denominata `$Document`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Trovare il certificato pubblico RSA-2048 per la propria regione in AWS certificati pubblici e aggiungere i contenuti in un nuovo file denominato `certificate.pem`.

5. Estrarre il certificato dal file del certificato e archiviarlo in una variabile denominata `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Verifica la firma.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

Se la firma è valida, il comando non restituisce alcun output. Se non è possibile verificare la firma, il comando restituisce `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Se non è possibile verificare la firma, contattare AWS Support.

7. Convalidare il contenuto del documento di identità dell'istanza.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Se il contenuto del documento di identità dell'istanza è valido, il comando restituisce `True`. Se il documento di identità dell'istanza non può essere convalidato, contattare AWS Support.

AWS certificati pubblici

I seguenti certificati AWS pubblici possono essere utilizzati per verificare il contenuto del documento di identità dell'istanza di un'istanza, come descritto nei seguenti argomenti:

- Verificare utilizzando la firma PKCS7
- Verificare l'utilizzo della firma con codifica base64
- Verificare utilizzando la firma RSA-2048

Assicurarsi di utilizzare il certificato corretto per la propria regione e per la procedura di verifica utilizzata. Se si verifica la firma PKCS7, utilizzare il certificato DSA. Se si verifica la firma con codifica base6, utilizzare il certificato RSA. Se si verifica la firma RSA-2048, utilizzare il certificato RSA-2048.

Espandere ciascuna delle seguenti regioni per visualizzare i certificati specifici per la regione.

Stati Uniti orientali (Ohio) - us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUVJTc+hOU+8Gk3JlqsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MTE0OVoXDTI5MDQyODE3MTE0OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUVJTc+hOU
+8Gk3JlqsX438Dk5c58wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAywJQaVNWJqW0R0T0xVOSoN1GLk9x9kKEuN67RN9CLin4dA97qa7Mr5W4P
FZ6vnh5CjOhQBRXV9xJUeYSdqVItNAUFK/fEzDdjf1nUfPlQ3OJ49u6CV01NoJ9m
usvY9kWcV46dqn2bk2MyfTTgvmeqP8fiMRPxxnVRkSzlldP5Fg==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----
```

Stati Uniti orientali (Virginia) - us-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUE1y2NIKCU+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MzQwMVoXDTI5MDQyODE3MzQwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUE1y2NIKC
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSWb5jT8pYjQb8ZoZkXXRGb09mvYeU
NeqOBr27rvRAnaQ/9LUQf72+SahDFuS4CMI8nwowytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCfOJTpu0temHcFA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
```

```
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

Stati Uniti occidentali (California settentrionale) - us-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUK2zmY9PUSTR7rc1k2OwPYu4+g7wwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MDI0M1oXDTI5MDQyODE3MDI0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUK2zmY9PU
STR7rc1k2OwPYu4+g7wwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQA1Ng4QmN4n7iPh5CnadSOc0ZfM7by0dBePwZJyGvOHdaw6P6E/vEk76KsC
Q8p+akuzVzVPkU4kBK/TRqLp19wEWoVwhhTaxHjQ1tTRHqXIVlrkw4JrtFbeNM21
GlkSLonuzmNZdivn9WuQYeGe7nUD4w3q9GgiF3CPorJe+UxtbA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7Jffupz7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
```

```
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

Stati Uniti occidentali (Oregon) - us-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFx8PxCkbHwpD31bOyCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MjM1OVoXDTI5MDQyODE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFx8PxCkb
```

```
HwpD31bOyCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzOl+9Xy1+UsbUBI95HO9mbbdnuX+aMJXgG9uFZNjgNEbMcvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM4O5+r7vUa1O
dWU+hP/T7DUrPAIVMOE7mpYa+WPWJrN6BlRwQkKQ7twm9kDalA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----
```

Africa (Città del Capo) - af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
```

```
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
```

```
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----
```

Asia Pacifico (Hong Kong) - ap-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
```

```
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----
```

Asia Pacifico (Hyderabad) - ap-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXjrQ4+XMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
```

```
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAJCKGBBoxIUxqBk94JHhwZZbgvbP0DAOoHENQWxp/98lI7/
YOfYJOVMJS22aCnHDurofmo5rvNIkgXi7Rztbhu
+lko9rK6DgpmpUwBU0WZtf34aZ2IWNBwHaVhHvWAQf9/46u18dMa2YucK1Wi+Vc+M
+KldrvgXmhym6ErNlzhJyMAkGByqGSM44BAMDLwAwLAIUaaPKxaOHoYvwz709xXpsQueIq+UCFFa/
GpzoDOSokl1057NU/2hnsiW4
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLj9CMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+sFcobrjvcAYm0PNRD8f4R1jAzvoLt2+qGeOTAyO1Httj6cmsYN3AP1hN5iYuppFiYsl2eNPa/
CD0Vg0BAfDFlV5rzjpA0j7TJabVh4kj7JvtD+xYMi6wEQA4x6SPONY4OeZ2+8o/
HS8nucpWDVdPRO6ciWUlMhjmDmwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAAy6sgTdRkTqELHBeWj69q60xHyUmsWqHAQ
TGGbYP0yP2qfMl0cCImzRI5W0gn8gogdervfeT7nH5ih0TWEy/QDWfkQ601L4erm4yh4YQq8vcqAPSkf04N
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAIVWfPw/X82fMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MDQx
NDMwMjhaGA8yMjAxMTIwODE0MzAyOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAg29QEFriG+qFEjYW/v62nN70lMJY/Hevx5TtmU/VIYBPQa3HUGTBAbbI
2Tmy8UMpa8kZeaYeI3RAfiQWt0Ws7wUrBuO2Pdp518WDPaJUH7RWEuu1BDDkyZRW
NAMNPCn3ph7Od243IFcLGku7HVekel5poqRpSfojrMasjlf+CvixUeAJbmFoxUHK
kh5unzG2sZyO4wHXcJPQkRf5a8zSTPe9YZP1kXPPEv4p/jTSggaYPxXyS6QVaTlV
zLeLFZ0fesLPMeil3KYQtV7IKLQiEA2F6dxWnxNWQlyMHtdq6PucfEmVx17i/Xza
yNBRo0azY8WUNVkEXrRhp/pU8Nh3GQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU9AO1aZk9RLXk2ZvRVoUxYvQy9uwwgY4GA1UdIwSBhjCBg4AU9AO1
aZk9RLXk2ZvRVoUxYvQy9uyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAIVWfPw/X82fMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADexluMRQRftqViahCnauEWGdMvLCBr8A+Yr
6hJq0guoxEk/lahxR137DnfMPuSbi1Rx5QKo7oBrWfG/zsgQUnF2IwHTzwD+i/2m
XCane6FiS5RpK3lGdILq8ZmlhQk+6iI8yoZLr0LCfTh+CLgIKHOknfR5lFzgzAiF
SI8/Q9mm+uvYtSTZECI6Zh57QZPoETAG/yl+9jiOy2lAelqa/k1i+Qo8gMfOc+Pm
```

```
dwY7o6fV+oucgRlsdey6VM45LeyILQqv0RXtVzjuowanzmCCFMjgqiO9oZAWu4Oh
+F3unijELo01vZJs8s2N3KGlo3/jtUFTX6RTKShZlAPLwBi5GMI=
-----END CERTIFICATE-----
```

Asia Pacifico (Giacarta) - ap-southeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3JQ6cVwntJie67D8OuNo4jGRn
+crEtL7YO0jSVB9zGE1ga
+UgRPIaYETL293S8rTJTVgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM
+/52g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIRtwK+9qnaTOBhvO/
njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXbVDG2yMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sDP+ZrS0LO1ZJfKhXf1R9S3AUwLnsc7b
+IuVXdY5LK9RKqu64nyXP5dx170zoL8loEyCSuRR2fs+04i2QsWBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV
+OkP9ab5wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAI4WUy6+DKh0JDSzQEZNyBgNlSoSuC2owtMxCwGB6nBfzzfcekWvs
+87w/g9lNwUnUt0ZHYyh2tuBG6hVJuUEwDJ/z3wDd6wQviLOTF3MITawt9P8siR1hXqLJNxpjRQFZrgHqi
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyyc Gt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
-----END CERTIFICATE-----
```

Asia Pacifico (Melbourne) - ap-southeast-4

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXKlrgBgEVCprLHdK/bbrMas0XMu1EhOD
+q
+0PcTr8+iwbtoXlY5MCeatWIp1GrXQjVqsF8vQqxlEuRuYKbR3nq4mWwaeGlx9AG5EjQHRa3GQ44wWHOdof0M3NRI1MP
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSh40SMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+qWTGAbGsPeMX4hBMjAJUKys2NIRcRZaLM/BCew2FIPVjNtlaj6Gwn9ipU4Mlz3zIwAMWi1AvGMSreppt
+wV6MRtfOjh0Dvj/veJe88aEZJMozNgkJFRS
```

```
+WFWsckQeL56tf6kY6QTlNo8V/0CsQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAF7vpPghH0FRo5gu49EArRNPrIvW1egM
wcgkqIwwuXYj+1rhlL+/
iMpQWjdVGEqIZSeXn5fLmdx50eegFCwND837r9e8XYTiQS143Sxt9+Yi6BZ7U7YD8kK9NBWoJxFqUeHdpRCs0O7COjT3
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAN4GTQ64zVs8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTMx
MzMzMDBaGA8yMjAxMTIxNzEzMzMwMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2BYgeCr+Rk/jIAEDOHS7wJql62vc83QEwjuzk0qOFEReIZzlN1fBRNXK
g0T178Kd3gLYcE59wEFbTe/X5yOA1Lo95x1anSAo7R+Cisf9C2HQuJp+gVb+zx71
lniPF7gHziGpm0M8DdAU/IW+wkZwGbP4z7Hq9+bJ0P2ltvPJ5yxSgkFuDsI9VBHa
CLoprHsCHh2VdP8KcMgQQMmHe1NmBpyTk0ul/aLmQkCQEX6ZIRGOeq228fwlh/t+
Ho+jv87duihVKic6MrL32SlD+maX0LSDUydWdaOLLTGkh7oV7+bFuH6msrXUu+Ur
ZEP1r/MidCWMhfgrFzeTBzOHA97qxQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUcHMd1cHqzmsQ5hpUK3EMLhHdsi4wgY4GA1UdIwSBhjCBg4AUcHMd
1cHqzmsQ5hpUK3EMLhHdsi6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIEExMQ4IJAN4GTQ64zVs8MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAI4PFyVN+7EGSObioiPnv0LL0f70SSzUZJ8p
XO90d4rWea7jIbgZ2AKb+ErynkU9xVg7XQQ5k6KDWgp/4jYFL2dqnt/YAY4PS0un
RSrYElawxLT0BcLn4rcSDC79vQe1xGC5//wDdV6b399COAHRAK6axWYy5w32u9PL
uw0cIp3Ch8JoNwcgTHKRRGzePmBeR4PNqhHTArG4/dJk6/aUO4OpX0WzI6L67CGY
6Nex3dau+gkLCK93dTEkrXtyXHu4wB0J9zd1w+iQ0SEa9eKc78/NjEsF/FZdGrWC
t57lIMOOXJhQ1kRgSwNeZdQWV1dRakvO6sfcvVYkfj1wAvZvvAw=
-----END CERTIFICATE-----
```

Asia Pacifico (Mumbai) - ap-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
```

```
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUDLA+x6tTAP3LRTr0z6nOxfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MTMwMVoXDTI5MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUDLA+x6tT
AP3LRTr0z6nOxfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAZ7rYKoAwwiiH1M5GJbrT/BEk3OO2VrEPw8ZxgpqQ/EKlzMlOs/0Cyrmp7
UYyUgYFQe5nq37Z94rOUSeMgv/WRxaMwrLlLqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIHOpQocJUSlm/dLeMuE0+0A3HNR6JVktGsUdv9ulmKw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
```

```
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

Asia Pacifico (Osaka-Locale) - ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZFOGvTFKxHoy9+f5Hl8wDQYJKoZIhvcNAQEL
```

```
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NTQwN1oXDTI5MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUHTRhxHhB
ZFOGvTFKxHoy9+f5Hl8wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUZx7DcYbhWNTD4BNGhr5beruT2OUoGHH9J73UKxwdqeb9bH1LIWhIZO0X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBRy8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXENlkC04v5yxdKxZxyg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
-----END CERTIFICATE-----
```

Asia Pacifico (Seoul) - ap-northeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbBSn2UIO6vYk4iNWV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEzMzg0NloXDTI5MDQyODEzMzg0NlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbBSn2UIO
6vYk4iNWV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAmjTjalG8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlfRtc2OwPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUhO2+xVRXDXVxM/VObFgPERbJpyA==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----
```

Asia Pacifico (Singapore) - ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
```

```
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXngrWf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MzAxNFoXDTI5MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUSqP6ih++
+5KF07NXngrWf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAw13BxW11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750MOcP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNCk+5GZG4Xec5DoapBZHXmfMo93sjxBFP
4x9rWn0GuwAVO9ukjYPevq2Rerilrq5VvppHtbATVNY2qecXDA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
```

```
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

Asia Pacifico (Sydney) - ap-southeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFxWyAdk4oiXIOC9PxcgjYYh71mwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MjE0M1oXDTI5MDQyODE1MjE0M1owXDELMAkGA1UEBhMCVVMx
```

```
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFxWyAdk4
oiXIOC9PxcgjYYh71mwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQByjeQe6lr7fiIhoGdjBXYzDfkX0lGGvMIhRh57G1bbceQfaYdZd7Ptc0jl
bpycKGaTvhUdkpMOiV2Hi9dOOYawkdhyJDstmDNKu6P9+b6Kak8He5z3NU1tUR2Y
uTwcz7Ye8Nldx//ws3raErfTI7D6s9m63OX8cAJ/f8bNgikwpw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
-----END CERTIFICATE-----
```

Asia Pacifico (Tokyo) - ap-northeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEyMjMxMFoXDTI5MDQyODEyMjMxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEExMQ4IULgwDh7Ti
DrPPBJwscqDwiBHkEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBtjAglBde1t4F9EHCZOj4qnY6Gigy07Ou54i+lR77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro1OVY1lHmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0BjOC
gepj1lUoiN7OA6PtA+ycNlsP0oJvdBjhvayLiuM3tUfLTrgHbw==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
KeznOtxzqQ5Wo5NLE9bA61sziUAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
-----END CERTIFICATE-----
```

Canada (Centrale) - ca-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MzU0M1oXDTI5MDQyODE1MzU0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUIrLgixJJ
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBHiQJmzyFAaSYs8SpiRijIDZW2RIo7qBKb/pI3rqK6yOWDlPuMr6yNI81D
IrKGGftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwddhKYy4BhteFQl/Wex3xTlX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iyOWrz/jVxwq7TOkCw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
```

```
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----
```

Canada occidentale (Calgary) - ca-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRSlFQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZIzjgEAwMvADAsAhRJc4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvuPrmGPupPlGiHe0veZiO8=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAYPou9weMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
v4XBVH13ZCMgqlRHMqV8AWI5iO6gFn2A9sN3AZXTMqwtZeiDdebq3k6Wt7ieYvpXTg0qvgsjQIovRZWaBDBJy9x8C2hW
+w9lMQjFHkJ7Jy/
PHCJ69EzebQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAGe9Snkz1A6rHBH6/5kDtYvtPYwhx2sXNxztbhkXErFk40Nw5l4
gvDVtWG7qyb6fAqgoisyAbk8K9LzxSim2S1nmT9vD84B/t/VvwQBylc
+ej8kRxMH7fquZLp7IXfmtBzyUqu6Dpbne+chG2
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALyTn5IHrIZjMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMzEyMDcx
NTM3MDFaGA8yMjAzMDUxMzE1MzcwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1GP5os424BJmGPCKOSgOclP7lzUiB85du03M4hfjzSOszsBpmBGFDLz1
owYHtIxlq3+Vi1Lt5Qlx3id/ov1QyaBPFWXVeklHVXy9vieCcI3TdjGjTl1W/8MM
m3X26QPcsnHM/Kk2wJ7s186MrqmdSsp3SCPpxv4vEG2Q9yR2bXY41hpc2rWlW8qU
D0JGXluvmmAdFnto20l1XWZ6xFen1h60DRugek/ufCbN+ljKy0xLqPoavH0Ybjsb
UpsAsBs7phaoN+X/5hIERfbp5LfVnqq54pNG5KNu4KynfW9+kA/WS4cJ6FTTN5t+
y0P1HvcL+BL2RuDy6T2bB21xw5WqtQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQURTvu/Dd4zDnmS5G5CfVLnmUBNOswgY4GA1UdIwSBhjCBg4AURTvu
/Dd4zDnmS5G5CfVLnmUBNOuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALyTn5IHrIZjMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFt523A3Aug6/F8xxyITgA8gkU0btFhlXNSP
U4U2OQ9n0tWI9WqnKNWH3KBxwY5EPitU6b3LM4xc9lDWpz7h2Pto+WhxP9LVKe6f
r8r7teTLCVZ7cfYZHzHg+flZjVpAgzE5BVfrRlj3QKpv0hYT3J1wMtI++Vorq5Nf
aPjzedehJLhmZVALwnfqfLrgv6/gmraP9Vmoa8U4D6AljNiQGYaLwyoPoRm3bUs2
v1Mh9GkEQ1b9+1pFXcqgzJJTGRuiPCyPbECI79FAnx5JM/CkGJV8HlOmjIW1qkK1
Y2qT7wzErrKLJyB53Pw15BdIM1onbDAQreZb0yZQLdoEl/tx7Uk=
-----END CERTIFICATE-----
```

Europa (Francoforte) - eu-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
```

```
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1NTUyOVoXDTI5MDQyODE1NTUyOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFD5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBBh0WaXlBsW56Hqk588MmJxsOrvcKfDjF57RgEDgnGnQaJcStCVWDO9UYO
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
O/LYOVHCknuPL123VmVRNs51qQA9hkPjvw21UzpDLxaUxt9Z/w==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
```

```
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

Europa (Irlanda) - eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
```

```
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MTgxMFoXDTI5MDQyODE2MTgxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQADIkn/MqaLGPuK5+prZZ5Ox4bBZLPtreO2C7r0pqU2kPM2lVPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYVir5r/yDmWzx+BVH5S/g==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

Europa (Londra) - eu-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUCgCV/DPxYNND/swDgEKGiC5I+EwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MjkxNFoXDTI5MDQyODE2MjkxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCgCV/DPx
YNND/swDgEKGiC5I+EwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQATPu/sOE2esNa4+XPEGKlEJSgqzyBSQLQc+VWo6FAJhGG9fp7D97jhHeLC
5vwfmtTAfnGBxadfAOT3ASkxnOZhXtnRna460LtnNHm7ArCVgXKJo7uBn6ViXtFh
uEEw4y6p9YaLQna+VC8Xtgw6WKq2JXuKzuhuNKSFaGGw9vRcHg==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----
```

Europa (Milano) - eu-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
```

```
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
```

```
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

Europa (Parigi) - eu-west-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUaC9fX57UDr6u1vBvsCsECKBZQyIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MzczOFoXDTI5MDQyODE2MzczOFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUaC9fX57U
```

```
Dr6u1vBvsCsECKBZQyIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCARv1bQEDaMEzYI0nPlu8GHcMXgmgA94HyrXhMMcaIlQwocGBs6VILGVhM
TXP2r3JFaPEpmXSQNQHvGA13clKwAZbni8wtzv6qXb4L4muF34iQRHF0nYrEDoK7
mMPR8+oXKKuPO/mv/XKo6XAV5DDERdSYHX5kkA2R9wtvyZjPnQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
-----END CERTIFICATE-----
```

Europa (Spagna) - eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAGG2m8EKmaf5qQqj3Z
```

```
+rzSaTaXE3B/R/4A2VuGqRYR7MljPtwdmU6/3CPjCACcZmTIcOAKbFiDHqadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8qOU7oZ0UWK4lbiAQs1MihoUwCQYHKoZIzjg
WmbaU7YM5GwCFCvIJOesO5hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLkiaMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIbSDbWFhA3fi5ippjKkh3sl8VyCvCOUXKdOaNrYBrPRkrdH
+3m/
rxIUZ2IK1fDlC6sWAjddf6sBrV2w2a78H0H8EwuwiSgttURBjwJ7KPPJCqaqrQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
+FzqQDzun/
iMMzcFucmLMl5BxEblrFXOz7IIuOeiGkndmrqUeDCykztLku45s7hxdNy4ltTuVAaE5aNBdw5J8U1mRvsKvHLy2ThH6h
+hBgiphYp84DUbWVYeP8YqLEJSqscKscWC
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALWSmO6DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuAAhuSpsHC00/fD2zNlBDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZCOsbpPZ+i74NOEQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNVlxYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9O12xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph0lbaqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
ilo8kr+tbIF+JmcgYLBvO8Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALWSmO6DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFWeNhAmtrwyE/i6FDSIphDrMHBkvw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtClOZL5WJiJwel8eDSg+sqJUxE0l
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHEOVP7Zk9C2ehrBXzCMLSDt3GV
fEuMea2RxMhozwz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILpOZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----
```

Europa (Stoccolma) - eu-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUN1c9U6U/xiVDFgJcYKZB4NkH1QEwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MDYwM1oXDTI5MDQyODE2MDYwM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUN1c9U6U/
xiVDFgJcYKZB4NkH1QEwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBTIQdoFSDRHkpqNPUbZ9WXR2O5v/9bpmHojMYZb3Hw46wsaRso7STiGGX/
tRqjIkPUIXsdhZ3+7S/RmhFznmZc8e0bjU4n5vi9CJtQSt+1u4E17+V2bF+D3h/7
wcfE0l3414Q8JaTDtfEf/aF3F0uyBvr4MDMd7mFvAMmDmBPSlA==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
-----END CERTIFICATE-----
```

Europa (Zurigo) - eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAYNjaCNg/
cfgQOOl1BUj5ClUulqwZ9Q+SfDzPZh9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjwvta2Ch//
b+sZ86E5h0XWWr+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDtlL8X/
Rpfalu2Z2OJgjFJWGf7hRwxe456n
+lowCQYHKoZIzjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
```

```
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSGFGiMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
opKZAUusJx2hpgU3pUHhlp9ATh/VeVD582jTd9IY
+8t5MDa6Z3fGliByEiXz0LEHdi8MBacLREu1TwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAILlpoE3k9o7KdALAxsFJNit
+g3RMzdbiFM+7MA63Nv5fsf+0xgcjSNBElvPCDKFvTJl4QQhToy056llO5GvdS9RK
+H8xrP2mrqngApoKTApv93vHBixgFSn5KrczRO0YSm3OjkqbydU7DFlmkXXR7GYE+5jbHvQHYiT1J5sMu
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
NTEyMDdaGA8yMjAxMTIyMjE1MTIwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyn+Lsnq1ykrfYlZkk6aAAYNReNd9Iw8AUwCBkgOr2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpghIoamcYhrPXyIxlWiRQlaqSg
OFiE9bsqL3rCF5Vz+tOiTe5W/7ojfOFls6++g7ZpobwJlpMbuJepqyeHMPyjvO5A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9kl3IOQrsLshBB5fFUjl09NiFipCGBwi+8ZMeSn1
5qwBI01BWXPfG7WX6Owyjhmh6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGlHYDtcHpfBvdHx9HeQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtrOd9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMVlSQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978Wy9ccXwVSeYG/YAr5rJpS6ZH7eRQvUY0IzwFNeaOPgOTEVpcjWlV6+MQEvsEx
W85q+s6AVr49eppEx8SLJsl0C23yB+L+t32tAveQImRWtJMpzZ5cxh/sYgDVeoC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHGOAmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----
```

Israele (Tel Aviv) - il-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYX
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgjOoUwWdl6fjlzWca
pq+l1ezuK2DFOzNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jkpXsvrS
+xTo2M9h2s2uLAhEQIUOZ2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAX0QQGVLMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+S8vOy5hpLoRe4RkOrY0cM3bN07GdEMlin5mU0y1t8y3ct4YewvmkgT42kTyMM
+t1K4S0xsqjXxxS716uGYh7eWtkxrCihj8AbXN/6pa095h
+7TZyl2n83keiNUzM2KoqQVMwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADwA6VVEIIZD2YL00F12po40xDLzIc9XvqFPS
FmU7H8s62/jD6cOR1A1cClIyZUe1yT1ZbPySCs43J+Thr8i8FSRxzDBSZZi5foW
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOVp1h2I9wW7MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTUx
MjQ0MTJaGA8yMjAxMTIxOTEyNDQxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13PkyWvl61iV/SYfO1UFO76UpDfPm2SF/Rz/o33cm699X++EYPxTnoEc
vmWeS0I7eDXc4OCUiToG0sEx0klE0CX1Z1tK6qJ+zgWQLZ9SZEC9H0NsSA6LhrHu
Nq0dzeK3LjhdfcX46/4GqdiptpdTuM4m/hOQ5yx4JMQ/n1sdpv4M5VLRWwWW9Lem
ufb79Id7O9SispxgRsz1KXIjp7N9S4BY7itSXz97uSyzTqEjWZ6mDUhTu3t21GKC
6flALGTTrG2yghEhz53rkvLsvwzjPSSlT6LIf0mrRPzHaf+EdaKoasElE1SHh+ZH
9mI81HywpE+HZ+W+5hBCvjYp90Y1fwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
```

```
BgNVHQ4EFgQU58tN2JO+yEGq5JbIXxGi4vRVPyIwgY4GA1UdIwSBhjCBg4AU58tN
2JO+yEGq5JbIXxGi4vRVPyKhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOVp1h2I9wW7MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANBN0e1EqNy4+IU2yQzMJ+Wy5ZIOtTP6GSBR
7muVY1bDeAwtNTEOpwgrZVlC7/xq5Q0LC1y0Z70hHXEf8au7qStaAoUtxzvhTAZI
NC0lwoFU56UFw4N0vZII17iqEfoqRC4PpI3OxqEJHFy0VLlvAzJoKB4QLLqDAYVA
LXCiOLoVT+y9tRYsxw5MyO0Bi6fxQIIADl2bE9xkunTN1Jkkwqo3LxNy/ryz4QWR
8K7jHUItifv4h/hxBKpHEquN8CkdvM9oeGl7I8PFrSFEpGr1euDXY0euZzzYiDBV
m6GpTJgzpVsEuIX52dPcPemwQncoIfZyhWDW85MJUnby2WTEcFo=
-----END CERTIFICATE-----
```

Medio Oriente (Bahrein) - me-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1QliO0B
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
```

```
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

Regione Medio Oriente (EAU) - me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf8moOhqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z
+XGmzKmgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C3qzE4rIenmahvUplu9ZmLwL1idWXMRX2R
+d2SeoKOKQWoc2UOFZMHYxDue7zkyk1CIRaBukTeY13/
RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHuBTvJE2+WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
```

```
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----
```

Sud America (San Paolo) - sa-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
```

```
MB4XDTI0MDQyOTE2NDYwOVoXDTI5MDQyODE2NDYwOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBoNarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaKO09Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

Cina (Pechino) - cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
```

```
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

Cina (Ningxia) - cn-nordovest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
```

```
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
```

```
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

AWS GovCloud (Stati Uniti orientali) — -1 us-gov-east

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qelPCiShB1KCCj4wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE1MjIzNloXDTI5MDUwNjE1MjIzNlowXDELMAkGA1UEBhMCVVMx
```

```
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULVyrqjjw
Z461qelPCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBfAL/YZv0y3zmVbXjyxQCsDloeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
puIAf05x6GQiEqfBMk+YMxJfcTmJB4Ebaj4egFlslJPSHyC2xuydHlr3B04INOH5
Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgq8zErQVQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----
```

AWS GovCloud (Stati Uniti occidentali) — -1 us-gov-west

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb7lUHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE3MzAzMloXDTI5MDUwNjE3MzAzMlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUe5wGF3jf
b7lUHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCbTdpx1Iob9SwUReY4exMnlwQlmkTLyA8tYGWzchCJOJJEPfsW0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d8OWtOJQcI+ZnFfG4
KyM4rUsBrljpG2aOCm12iACEyrvgJJrS8VZwUDZS6mZEnn/lhA==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----
```

Ruoli di identità dell'istanza

Ogni istanza avviata dispone di un ruolo di identità dell'istanza che ne rappresenta l'identità. Un ruolo di identità di istanza è un tipo di ruolo IAM. AWS i servizi e le funzionalità che sono integrati per utilizzare il ruolo di identità dell'istanza possono utilizzarlo per identificare l'istanza nel servizio.

Le credenziali del ruolo di identità dell'istanza sono accessibili dal servizio di metadati dell'istanza (IMDS) in `/identity-credentials/ec2/security-credentials/ec2-instance`. Le credenziali sono costituite da una coppia di chiavi di accesso AWS temporanea e da un token di sessione. Vengono utilizzate per firmare le richieste AWS Sigv4 ai AWS servizi che utilizzano il ruolo di identità dell'istanza. Le credenziali sono presenti nei metadati dell'istanza indipendentemente dal fatto che sull'istanza sia abilitato un servizio o una funzione che fa uso dei ruoli di identità dell'istanza.

I ruoli di identità dell'istanza vengono creati automaticamente all'avvio di un'istanza, non dispongono di alcun documento relativo alla policy di affidabilità ruolo e non sono soggetti a policy di identità o risorse.

Servizi supportati

I seguenti AWS servizi utilizzano il ruolo di identità dell'istanza:

- Amazon EC2 — EC2 Instance Connect utilizza il ruolo di identità dell'istanza per aggiornare le chiavi host per un'istanza Linux.
- Amazon GuardDuty — Runtime Monitoring utilizza il ruolo di identità dell'istanza per consentire all'agente runtime di inviare telemetria di sicurezza all'endpoint GuardDuty VPC.
- AWS Security Token Service (AWS STS) — Le credenziali del ruolo di identità dell'istanza possono essere utilizzate con l'azione. AWS STS `GetCallerIdentity`
- AWS Systems Manager— Quando si utilizza la configurazione predefinita di gestione dell'host, AWS Systems Manager utilizza l'identità fornita dal ruolo di identità dell'istanza per registrare le istanze EC2. Dopo aver identificato l'istanza, Systems Manager può passare il ruolo IAM `AWSSystemsManagerDefaultEC2InstanceManagementRole` all'istanza.

I ruoli di identità delle istanze non possono essere utilizzati con altri AWS servizi o funzionalità perché non hanno un'integrazione con i ruoli di identità delle istanze.

ARN del ruolo di identità dell'istanza

L'ARN del ruolo di identità dell'istanza presenta il formato seguente:

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Per esempio:

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-0123456789example
```

Per maggiori informazioni sugli ARN, consulta Nomi della risorsa Amazon (ARN) nella Guida per l'utente di IAM.

Connect alla tua istanza EC2

Questa sezione della Guida per l'utente di Amazon EC2 fornisce informazioni per aiutarti a connetterti alla tua istanza Amazon EC2 dopo averla avviata. Fornisce inoltre informazioni per aiutarti a connettere l'istanza a un'altra AWS risorsa.

Argomenti

Connessione all'istanza di Linux

Ci sono diversi modi per connetterti alla tua istanza Linux. Alcuni variano a seconda del sistema operativo del computer locale da cui ti connetti. Altri, come EC2 Instance Connect, Gestore di sessione di AWS Systems Manager , non variano. In questa sezione imparerai come connetterti alla tua istanza Linux e come trasferire file tra il tuo computer locale e l'istanza.

Prima di connetterti a un'istanza Linux, è necessario soddisfare i prerequisiti seguenti:

- Ottenimento di informazioni sull'istanza
- Individuazione della chiave privata e impostazione delle autorizzazioni
- (Opzionale) Ottenimento dell'impronta dell'istanza

Quindi, scegli una delle seguenti opzioni per connetterti alla tua istanza Linux.

Opzioni di connessione in base al sistema operativo locale

- Connessione da un computer locale Linux o macOS tramite SSH
- Connessione da un computer locale Windows

Opzioni per la connessione da qualsiasi sistema operativo locale

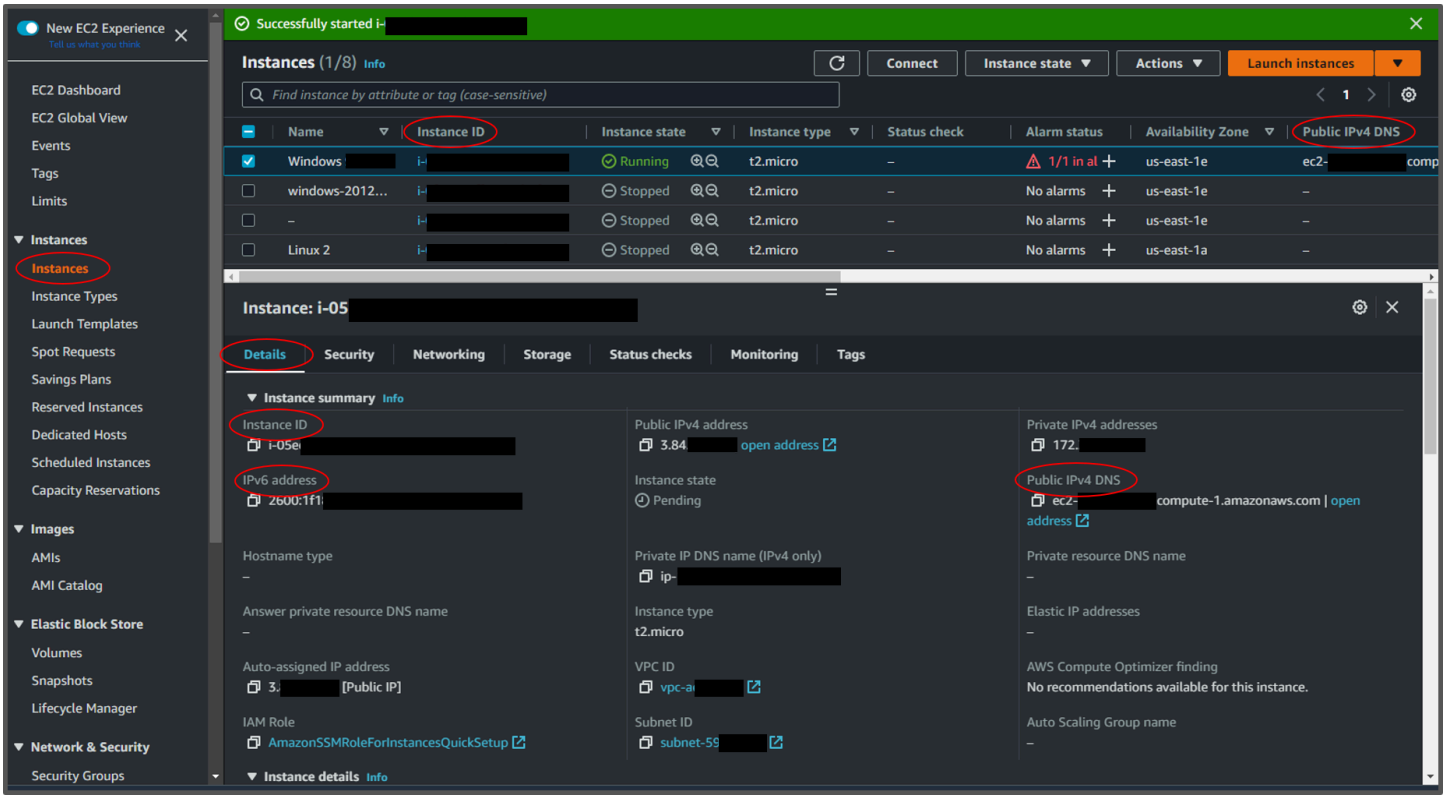
- Connessione tramite Session Manager

- Connessione a un'istanza Linux tramite EC2 Instance Connect.

> **Note**
>
> Per suggerimenti per la risoluzione dei problemi di connessione, consulta Risolvi i problemi di connessione alla tua istanza Linux.
> Per risolvere i problemi di avvio, configurazione di rete e altri problemi per le istanze basate su AWS Nitro System, puoi utilizzare Console seriale EC2 per istanze Amazon EC2.

Ottenimento di informazioni sull'istanza

Per prepararti a connetterti a un'istanza, ottieni le seguenti informazioni dalla console Amazon EC2 o utilizzando la AWS CLI.



- Ottieni il nome DNS pubblico dell'istanza.

  Puoi ottenere il DNS pubblico dell'istanza dalla console Amazon EC2. Controlla la colonna DNS IPv4 pubblico del riquadro Istanze. Se questa colonna è nascosta, scegli l'icona delle impostazioni (⚙)

nell'angolo superiore destro della schermata e seleziona DNS pubblico IPv4. Puoi anche trovare il DNS pubblico nella sezione delle informazioni sull'istanza del riquadro Istanze. Quando selezioni l'istanza nel riquadro Istanze della console Amazon EC2, le informazioni su quell'istanza verranno visualizzate nella metà inferiore della pagina. Nella scheda Dettagli, cerca DNS IPv4 pubblico.

Se preferisci, puoi usare i comandi describe-instances (AWS CLI) o Get-EC2Instance().AWS Tools for Windows PowerShell

Se non viene visualizzato alcun DNS IPv4 pubblico, verifica che lo Stato dell'istanza sia In esecuzione e che non sia stata avviata l'istanza in una sottorete privata. Se hai avviato l'istanza utilizzando la Procedura guidata di avvio dell'istanza, potresti aver modificato il campo Assegna automaticamente IP pubblico in Impostazioni di rete e modificato il valore in Disabilita. Se disabiliti l'opzione Assegna automaticamente IP pubblico, all'istanza non viene assegnato un indirizzo IP pubblico quando viene avviata.

- (Solo IPv6) Ottieni l'indirizzo IPv6 dell'istanza.

  Se hai assegnato un indirizzo IPv6 all'istanza, puoi facoltativamente connetterti all'istanza utilizzando il relativo indirizzo IPv6 anziché un indirizzo IPv4 pubblico o un nome host DNS IPv4 pubblico. Il tuo computer locale deve avere un indirizzo IPv6 ed essere configurato per utilizzare IPv6. Puoi ottenere l'indirizzo IPv6 dell'istanza dalla console Amazon EC2. Controlla la colonna IP IPv6 del riquadro Istanze. In alternativa, puoi trovare l'indirizzo IPv6 nella sezione delle informazioni sull'istanza. Quando selezioni l'istanza nel riquadro Istanze della console Amazon EC2, le informazioni su quell'istanza verranno visualizzate nella metà inferiore della pagina. Nella scheda Dettagli, cerca l'indirizzo IPv6.

  Se preferisci, puoi usare i comandi describe-instances () o ().AWS CLIGet-EC2InstanceAWS Tools for Windows PowerShell Per ulteriori informazioni su IPv6, consulta Indirizzi IPv6.

- Ottieni il nome utente per l'istanza.

  È possibile connettersi all'istanza utilizzando il nome utente dell'account utente o il nome utente predefinito per l'AMI utilizzato per avviare l'istanza.

  - Ottenere il nome utente per il proprio account utente.

    Per ulteriori informazioni su come creare un account utente, consulta Gestisci gli utenti di sistema sulla tua istanza Linux.

  - Ottieni il nome utente predefinito per l'AMI che hai utilizzato per avviare l'istanza:

AMI utilizzata per avviare l'istanza	Nome utente predefinito
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Altro	Verifica con il provider dell'AMI

Individuazione della chiave privata e impostazione delle autorizzazioni

Per connetterti all'istanza, devi conoscere la posizione del file della chiave privata. Per le connessioni SSH, devi impostare le autorizzazioni in modo che tu sia l'unico a poter leggere il file.

Per informazioni su come funzionano le coppie di chiavi quando si utilizza Amazon EC2, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.

- Individuazione della la chiave privata

Ottieni il percorso pienamente qualificato alla posizione nel tuo computer del file `.pem` per una coppia di chiavi che hai specificato quando hai avviato l'istanza. Per ulteriori informazioni, consulta the section called “Identificazione della chiave pubblica specificata al momento dell'avvio”.

Se non riesci a trovare il file della tua chiave privata, vedi

Se si perde la chiave privata per un'istanza supportata da EBS, è possibile riottenere l'accesso all'istanza. Arrestare l'istanza, distaccarne il volume root e collegarlo a un'altra istanza come volume dati, modificare il file `authorized_keys` con una nuova chiave pubblica, riportare il volume all'istanza originale e riavviare l'istanza. Per ulteriori informazioni sull'avvio, la connessione e l'arresto delle istanze, consulta Ciclo di vita dell'istanza.

Questa procedura è supportata solo per le istanze con volumi root EBS. Se il dispositivo principale è un volume dell'instance store, non è possibile utilizzare questa procedura per riconquistare l'accesso all'istanza; è necessario disporre della chiave privata per connettersi all'istanza. Per determinare il tipo di dispositivo root dell'istanza, apri la console Amazon EC2, scegli Istanze, seleziona l'istanza, scegli la scheda Archiviazione e nella sezione Dettagli del dispositivo root controlla il valore Tipo di dispositivo root.

Il valore è `EBS` o `INSTANCE-STORE`.

In aggiunta ai passaggi seguenti, esistono altri modi per connettersi all'istanza Linux in caso di perdita della chiave privata. Per ulteriori informazioni, consulta Come posso connettermi alla mia istanza Amazon EC2 se ho perso la mia coppia di chiavi SSH dopo il suo avvio iniziale?

Per connettersi a un'istanza supportata da EBS con una coppia di chiavi diversa

- Fase 1: creazione di una nuova coppia di chiavi
- Fase 2: Ottenere informazioni sull'istanza originale e il relativo volume radice
- Fase 3: Arrestare l'istanza originale
- Fase 4: Avviare un'istanza temporanea
- Fase 5: scollegare il volume radice dall'istanza originale e collegarlo all'istanza temporanea
- Fase 6: aggiungere la nuova chiave pubblica a authorized_keys sul volume originale montato sull'istanza temporanea
- Fase 7: smontare e scollegare il volume originale dall'istanza temporanea e ricollegarlo all'istanza originale
- Fase 8: connettersi all'istanza originale utilizzando la nuova coppia di chiavi

- Fase 9: pulizia

Fase 1: creazione di una nuova coppia di chiavi

Creare una nuova coppia di chiavi tramite la console Amazon EC2 o uno strumento di terza parte. Se si vuole assegnare alla nuova coppia di chiavi lo stesso nome della chiave privata persa, bisogna prima eliminare la coppia di chiavi esistente. Per informazioni su come creare una coppia di chiavi, consulta Creazione di una coppia di chiavi utilizzando Amazon EC2 o Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2.

Fase 2: Ottenere informazioni sull'istanza originale e il relativo volume radice

Prendere nota delle seguenti informazioni perché sono necessarie per completare questa procedura.

Per ottenere informazioni sull'istanza originale

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza a cui ci si vuole connettere. (Ci si riferirà a questa come istanza originale).
3. Nella scheda Details (Dettagli), prendere nota dell'ID istanza e dell'ID AMI.
4. Nella scheda Networking (Reti), prendere nota della zona di disponibilità.
5. Nella scheda Storage (Archiviazione), sotto Root device name (Nome dispositivo root) annotare il nome del dispositivo per il volume root (ad esempio `/dev/xvda`). Quindi, trova il nome di questo dispositivo in Block devices (Dispositivi a blocchi) e annota l'ID volume (ad esempio, vol-0a1234b5678c910de).

Fase 3: Arrestare l'istanza originale

Scegli Instance state (Stato istanza), Stop instance (Arresta istanza). Se questa opzione è disabilitata, l'istanza è già arrestata o il suo dispositivo root è un volume di instance store.

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

Fase 4: Avviare un'istanza temporanea

New console

Per avviare un'istanza temporanea

1. Nel riquadro di navigazione, selezionare Instances (Istanze), quindi selezionare Launch Instance (Avvia istanza).
2. Nella sezione Name and tags (Nome e tag), per Name (Nome) inserisci Temporary.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona la stessa AMI utilizzata per avviare l'istanza originale. Se questa AMI non è disponibile, è possibile creare un'AMI che può essere utilizzata dall'istanza arrestata. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.
4. Nella sezione Instance type (Tipo di istanza), mantieni il tipo di istanza di default.
5. Nella sezione Key pair (Coppia di chiavi), per Key pair name (Nome della coppia di chiavi) seleziona una coppia di chiavi esistente o creane una nuova.
6. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica), quindi per Subnet (Sottorete) seleziona una sottorete nella stessa zona di disponibilità dell'istanza originale.
7. Nel pannello Summary (Riepilogo), scegli Launch (Avvia).

Old console

Scegliere Launch instances (Avvia istanze), quindi utilizzare la procedura guidata di avvio per avviare un'istanza temporanea con le seguenti opzioni:

- Nella pagina Choose an AMI (Scegli un'AMI), selezionare la stessa AMI utilizzata per avviare l'istanza originale. Se questa AMI non è disponibile, è possibile creare un'AMI che

può essere utilizzata dall'istanza arrestata. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.

- Nella pagina Choose an Instance Type (Scegli un tipo di istanza), lasciare il tipo di istanza predefinita selezionata dalla procedura guidata.
- Nella pagina Configure Instance Details (Configura dettagli istanza) specificare la stessa zona di disponibilità dell'istanza originale. Se si sta avviando un'istanza in un VPC, selezionare una sottorete in questa zona di disponibilità.
- Nella pagina Add Tags (Aggiungi tag), aggiungere il tag `Name=Temporary` all'istanza per indicare che si tratta di un'istanza temporanea.
- Nella pagina Revisione, selezionare Launch (Avvia). Seleziona la coppia di chiavi che hai creato nella Fase 1, quindi seleziona Launch Instances (Avvia istanze).

Fase 5: scollegare il volume radice dall'istanza originale e collegarlo all'istanza temporanea

1. Nel riquadro di navigazione, selezionare Volumes (Volumi), quindi selezionare il volume dispositivo root per l'istanza originale (l'ID del volume è stato annotato in una fase precedente). Scegli Actions (Operazioni), Detach volume (Scollega volume), quindi scegli Detach (Scollega). Attendere che lo stato del volume diventi `available`. (Potrebbe essere necessario scegliere l'icona Refresh (Aggiorna)).
2. Con il volume ancora selezionato, scegli Actions (Operazioni), quindi scegli Attach volume (Collega volume). Seleziona l'ID istanza dell'istanza temporanea, prendi nota del nome del dispositivo specificato sotto Device name (Nome del dispositivo), ad esempio `/dev/sdf`, quindi scegli Attach volume (Collega volume).

   > **Note**
   >
   > Se hai avviato l'istanza originale da un' Marketplace AWS AMI e il volume contiene Marketplace AWS codici, devi prima interrompere l'istanza temporanea prima di poter collegare il volume.

Fase 6: aggiungere la nuova chiave pubblica a **authorized_keys** sul volume originale montato sull'istanza temporanea

1. Connettersi all'istanza temporanea.
2. Dall'istanza temporanea, montare il volume collegato all'istanza in modo da poter accedere al file system. Ad esempio, se il nome del dispositivo è `/dev/sdf`, utilizzare i seguenti comandi per montare il volume come `/mnt/tempvol`.

   > **Note**
   >
   > Il nome del dispositivo potrebbe apparire in modo diverso nell'istanza. Ad esempio, i dispositivi montati come `/dev/sdf` potrebbero essere visualizzati come `/dev/xvdf` nell'istanza. Alcune versioni di Red Hat (o le relative varianti, come CentOS), potrebbero anche aggiungere alla lettera finale 4 caratteri, in modo che `/dev/sdf` diventi `/dev/xvdk`.

   a. Utilizzare il comando lsblk per determinare se il volume è partizionato.

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   ##xvda1 202:1    0    8G  0 part /
   xvdf    202:80   0  101G  0 disk
   ##xvdf1 202:81   0  101G  0 part
   xvdg    202:96   0   30G  0 disk
   ```

   Nell'esempio precedente, `/dev/xvda` e `/dev/xvdf` sono volumi partizionati, mentre `/dev/xvdg` non lo è. Se il volume è partizionato, montare la partizione (`/dev/xvdf1`) invece del dispositivo raw (`/dev/xvdf`) nelle fasi successive.

   b. Creare una directory temporanea per montare il volume.

   ```
   [ec2-user ~]$ sudo mkdir /mnt/tempvol
   ```

   c. Montare il volume (o la partizione) nel punto di montaggio temporaneo, utilizzando il nome del volume o del dispositivo identificato in precedenza. Il comando necessario dipende dal file system del sistema operativo. Nota: il nome del dispositivo potrebbe

apparire in modo diverso nell'istanza. Per ulteriori informazioni, consulta la sezione note nel passaggio 6.

- Amazon Linux, Ubuntu e Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 e RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Se si riceve un errore che indica che il file system è corrotto, eseguire il seguente comando per utilizzare l'utilità fsck per controllare il file system e risolvere qualsiasi guasto:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Dall'istanza temporanea, utilizzare il seguente comando per aggiornare `authorized_keys` nel volume montato con la nuova chiave pubblica da `authorized_keys` per l'istanza temporanea.

> **Important**
>
> Gli esempi seguenti utilizzano il nome utente di Amazon Linux `ec2-user`. Potrebbe essere necessario sostituire un nome utente diverso, ad esempio `ubuntu` per le istanze di Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Se la copia ha avuto successo, è possibile passare alla fase successiva.

(Facoltativo) Altrimenti, se non si ha il permesso di modificare i file in `/mnt/tempvol`, sarà necessario aggiornare il file utilizzando sudo, quindi occorrerà controllare le autorizzazioni

sul file per verificare di poter accedere all'istanza originale. Utilizzare il comando seguente per verificare le autorizzazioni per il file:

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

In questo esempio di output, *222* è l'ID utente e *500* è l'ID di gruppo. Quindi, utilizzare sudo per eseguire nuovamente il comando di copia non riuscito.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Eseguire nuovamente il comando seguente per stabilire se le autorizzazioni sono state modificate.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Se l'ID utente e l'ID gruppo sono stati modificati, utilizzare il seguente comando per ripristinarli.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Fase 7: smontare e scollegare il volume originale dall'istanza temporanea e ricollegarlo all'istanza originale

1. Dall'istanza temporanea, smontare il volume collegato all'istanza in modo da ricollegarlo all'istanza originale. Ad esempio, utilizzare il seguente comando per smontare il volume in `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Scollega il volume dall'istanza temporanea (è stato smontato nel passaggio precedente): dalla console Amazon EC2, scegli Volumes (Volumi) nel riquadro di navigazione, seleziona il volume del dispositivo root per l'istanza originale (l'ID del volume è stato annotato in un passaggio precedente), scegli Actions (Operazioni), Detach volume (Scollega volume),

quindi scegli Detach (Scollega). Attendere che lo stato del volume diventi `available`. (Potrebbe essere necessario scegliere l'icona Refresh (Aggiorna)).

3. Ricollega il volume all'istanza originale: con il volume ancora selezionato, scegli Actions (Operazioni), Attach volume (Collega volume). Seleziona l'ID dell'istanza originale, specifica il nome del dispositivo annotato in precedenza nel Passaggio 2 per il collegamento del dispositivo root originale (`/dev/sda1` o `/dev/xvda`), quindi scegli Attach volume (Collega volume).

   Important

   Se non si specifica lo stesso nome del dispositivo dell'allegato originale, non è possibile avviare l'istanza originale. Amazon EC2 prevede il volume del dispositivo di root su `sda1` o `/dev/xvda`.

Fase 8: connettersi all'istanza originale utilizzando la nuova coppia di chiavi

Seleziona l'istanza originale, scegli Instance state (Stato istanza), Start instance (Avvia istanza). Dopo che l'istanza acquisisce lo stato `running`, è possibile connettersi a essa tramite il file della chiave privata per la nuova coppia di chiavi.

Note

Se il nome della nuova coppia di chiavi e del corrispondente file di chiave privata è diverso dal nome della coppia di chiavi originale, assicurarsi di specificare il nome del nuovo file della chiave privata quando ci si connette all'istanza.

Fase 9: pulizia

(Facoltativo) È possibile terminare l'istanza temporanea se non la si utilizza più. Selezionare l'istanza temporanea e scegliere Instance state (Stato istanza), Terminate instance (Termina istanza).

Se ti stai connettendo alla tua istanza usando Putty e devi convertire il file `.pem` in `.ppk`, consulta Convertire la chiave privata tramite PuTTYgen nell'argomento Connessione all'istanza Linux da Windows tramite PuTTY di questa sezione.

- Imposta le autorizzazioni della tua chiave privata in modo che solo tu possa leggerla
  - Connessione da macOS o Linux

    (Istanze Linux) Se prevedi di utilizzare un client SSH su un computer macOS o Linux per connetterti alla tua istanza Linux, usa il comando seguente per impostare le autorizzazioni del tuo file di chiave privata in modo che solo tu possa leggerlo.

    ```
    chmod 400 key-pair-name.pem
    ```

    Se non imposti queste autorizzazioni, allora non puoi connetterti alle tue istanze usando questa coppia di chiavi. Per ulteriori informazioni, consulta Errore: Unprotected Private Key File (File della chiave privata non protetto).
  - Connessione da Windows

    Apri Esplora file e fai clic con il pulsante destro del mouse sul file `.pem`. Seleziona la scheda Proprietà > Sicurezza e scegli Avanzate. Scegli Disabilita l'ereditarietà. Rimuovi l'accesso a tutti gli utenti tranne l'utente corrente.

(Opzionale) Ottenimento dell'impronta dell'istanza

Per proteggerti dagli man-in-the-middle attacchi, puoi verificare l'autenticità dell'istanza a cui stai per connetterti verificando l'impronta digitale visualizzata. La verifica dell'impronta digitale è utile se hai avviato l'istanza da un'AMI pubblica fornita da una terza parte.

Panoramica delle attività

Innanzitutto, recupera l'impronta digitale dell'istanza dall'istanza. Quindi, quando ti connetti all'istanza e ti viene richiesto di verificare l'impronta digitale, confronta l'impronta digitale ottenuta con questa procedura con l'impronta digitale visualizzata. Se le impronte digitali non corrispondono, è possibile che qualcuno stia tentando un attacco. man-in-the-middle Se tali impronte corrispondono, puoi collegarti in modo sicuro alla tua istanza.

Prerequisiti per ottenere l'impronta dell'istanza

- L'istanza non deve essere nello stato `pending`. L'impronta è disponibile solo al termine del primo avvio dell'istanza.
- Per ottenere l'output della console, devi essere il proprietario dell'istanza.

- Esistono vari modi per ottenere l'impronta digitale dell'istanza. Se si desidera utilizzare AWS CLI, è necessario installarlo sul computer locale. Per informazioni sull'installazione di AWS CLI, vedere Installazione di AWS Command Line Interface nella Guida AWS Command Line Interface per l'utente.

Per ottenere l'impronta dell'istanza

Nel passaggio 1, viene visualizzato l'output della console, che include l'impronta digitale dell'istanza. Nel passaggio 2, trovi l'impronta digitale dell'istanza nell'output della console.

1. Ottieni l'output della console utilizzando uno dei seguenti metodi.

   Console

   1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   2. Dal navigatore sinistro, scegli Istanze.
   3. Seleziona l'istanza, quindi scegli Azioni, Monitoraggio e risoluzione dei problemi, Ottieni registro di sistema.

   AWS CLI

   Sul computer locale (non sull'istanza a cui ti stai connettendo), usa il comando get-console-output(AWS CLI). Se l'output è grande, puoi reindirizzarlo a un file di testo per agevolarne la lettura. Tieni presente che devi specificare un Regione AWS quando usi la AWS CLI, in modo esplicito o impostando una Regione predefinita. Per informazioni su come impostare o specificare una regione, consulta Nozioni di base sulla configurazione nella Guida per l'utente di AWS Command Line Interface .

   ```
   aws ec2 get-console-output --instance-id instance_id --query Output --output
    text > temp.txt
   ```

2. Nell'output della console, trova l'impronta digitale dell'istanza (host), che si trova sotto. `BEGIN SSH HOST KEY FINGERPRINTS` Potrebbero esserci diverse impronte digitali dell'istanza. Quando ti connetti all'istanza, verrà visualizzata solo una delle impronte digitali.

   L'output esatto può variare in base al sistema operativo, alla versione AMI e al fatto che AWS crei o meno la coppia di chiavi. Di seguito è riportato un output di esempio.

```
ec2:#############################################################
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)
ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc no comment (RSA)
ec2: -----END SSH HOST KEY FINGERPRINTS-----
ec2: #############################################################
```

> **Note**
>
> Farai riferimento a questa impronta digitale quando ti connetti all'istanza.

Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH.

Puoi usare Secure Shell (SSH) per connetterti alla tua istanza Linux da un computer locale che esegue un sistema operativo Linux o macOS, oppure puoi usare uno strumento di connessione indipendente dalla piattaforma, come EC2 Instance AWS Systems Manager Connect o Session Manager. Per ulteriori informazioni sugli strumenti indipendenti dalla piattaforma, consulta Connessione all'istanza di Linux.

Questa pagina spiega come connettersi alla tua istanza con un client SSH. Per la connessione alla tua istanza Linux da Windows, consulta Connessione da Windows.

> **Note**
>
> Se compare un errore mentre tenti di connetterti alla tua istanza, assicurati che l'istanza soddisfi tutti i Prerequisiti per la connessione SSH. Se soddisfa tutti i prerequisiti e non riesci ancora a connetterti alla tua istanza Linux, consulta Risolvi i problemi di connessione alla tua istanza Linux.

Indice

Prerequisiti per la connessione SSH

Prima di connetterti a un'istanza Linux, è necessario soddisfare i prerequisiti seguenti:

Controllare lo stato dell'istanza

Dopo aver avviato un'istanza, possono essere necessari alcuni minuti affinché sia pronta e sia possibile connettervisi. Verifica che l'istanza abbia superato i controlli dello stato. Puoi vedere queste informazioni nella colonna Status checks (Verifiche di stato) della pagina Instances (Istanze).

Ottenere il nome DNS pubblico e il nome utente per connettersi all'istanza

Per trovare il nome DNS pubblico o l'indirizzo IP dell'istanza e il nome utente da utilizzare per connettersi all'istanza, consulta Ottenimento di informazioni sull'istanza.

Individuare la chiave privata e impostare le autorizzazioni

Per individuare la chiave privata necessaria per connettersi all'istanza e per impostare le autorizzazioni della chiave, consulta Individuazione della chiave privata e impostazione delle autorizzazioni.

Installare un client SSH sul computer locale in base alle esigenze

Il computer locale potrebbe avere un client SSH installato per impostazione predefinita. Puoi verificarlo digitando ssh sulla riga di comando. Se il computer non riconosce il comando, è possibile installare un client SSH.

- Versioni recenti di Windows Server 2019 e Windows 10: OpenSSH è incluso come componente installabile. Per informazioni, consulta OpenSSH in Windows.
- Versioni precedenti di Windows: scarica e installa OpenSSH. Per ulteriori informazioni, consulta Win32-OpenSSH.
- Linux e macOS X: scarica e installa OpenSSH. Per ulteriori informazioni, consulta https://www.openssh.com.

Connessione all'istanza Linux tramite un client SSH

Utilizza la seguente procedura per stabilire una connessione a un'istanza Linux tramite un client SSH. Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risolvi i problemi di connessione alla tua istanza Linux.

Connettersi all'istanza tramite SSH

1. Nella finestra del terminale, utilizzare il comando ssh per connettersi all'istanza. Specificare il percorso e il nome del file della chiave privata (`.pem`), il nome utente per l'istanza e il nome DNS pubblico o l'indirizzo IPv6 per l'istanza. Per ulteriori informazioni su come trovare la chiave privata, il nome utente per l'istanza e il nome DNS o l'indirizzo IPv6 per un'istanza, consulta Individuazione della chiave privata e impostazione delle autorizzazioni e Ottenimento di informazioni sull'istanza. Per connettersi all'istanza, utilizzare uno dei seguenti comandi.
   - (DNS pubblico) Per connettersi utilizzando il nome DNS pubblico dell'istanza, immettere il comando seguente.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
     ```
   - (IPv6) In alternativa, se l'istanza ha un indirizzo IPv6, per connettersi utilizzando l'indirizzo IPv6 dell'istanza, immettere il comando seguente.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
     ```

   La risposta visualizzata sarà simile alla seguente:

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
    can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```
2. (Opzionale) Verificare che l'impronta riportata nell'avviso di sicurezza corrisponda all'impronta ottenuta precedentemente in (Opzionale) Ottenimento dell'impronta dell'istanza. Se queste impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco. man-in-the-middle Se invece corrispondono, passare alla fase successiva.
3. Specificare (sì **`yes`**.

   La risposta visualizzata sarà simile alla seguente:

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
    the list of known hosts.
   ```

Trasferimento di file in istanze Linux utilizzando un client SCP

Un modo per trasferire file tra il computer locale e un'istanza Linux è utilizzare il protocollo secure copy (SCP). Questa sezione descrive come trasferire file utilizzando la funzionalità SCP. La procedura è simile a quella valida per la connessione a un'istanza tramite SSH.

Prerequisiti

- Verificare i prerequisiti generali per il trasferimento di file all'istanza.

  Prima di trasferire file tra il computer locale e l'istanza, esegui le seguenti azioni per assicurarti di disporre di tutte le informazioni necessarie.

  - Ottenimento di informazioni sull'istanza
  - Individuazione della chiave privata e impostazione delle autorizzazioni
  - (Opzionale) Ottenimento dell'impronta dell'istanza
- Installare un client SCP

  La maggior parte dei computer Linux, Unix e Apple includono un client SCP per impostazione di default. Se il computer in uso non dispone di questo client, il progetto OpenSSH fornisce un'implementazione gratuita della suite completa di strumenti SSH, incluso un client SCP. Per ulteriori informazioni, consulta https://www.openssh.com.

La seguente procedura in fasi consente di utilizzare SCP per trasferire un file mediante il nome DNS pubblico dell'istanza o l'indirizzo IPv6, se l'istanza ne ha uno.

Per utilizzare SCP per trasferire file tra il computer e l'istanza

1. Determina la posizione del file di origine nel computer e il percorso di destinazione nell'istanza. Negli esempi seguenti, il nome del file della chiave privata è `key-pair-name.pem`, il file da trasferire è `my-file.txt`, il nome utente per l'istanza è ec2-user, il nome DNS pubblico dell'istanza è `instance-public-dns-name` e l'indirizzo IPv6 dell'istanza è `instance-IPv6-address`.
   - (DNS pubblico) Per trasferire un file nella destinazione sull'istanza, immetti il seguente comando dal computer.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
     ```

- (IPv6) Per trasferire un file nella destinazione sull'istanza se l'istanza dispone di un indirizzo IPv6, immetti il seguente comando dal computer. L'indirizzo IPv6 deve essere racchiuso tra parentesi quadrate (`[ ]`), che devono essere inserite dopo un carattere di escape (\).

```
scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@\[instance-IPv6-address\]:path/
```

2. Se non hai già effettuato la connessione all'istanza utilizzando SSH, viene visualizzata una risposta simile alla seguente:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

(Facoltativo) È possibile verificare se l'impronta nell'avviso di sicurezza corrisponde all'impronta dell'istanza. Per ulteriori informazioni, consulta (Opzionale) Ottenimento dell'impronta dell'istanza.

Specificare **`yes`**.

3. Se il trasferimento ha esito positivo, la risposta è simile alla seguente:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                                   100%   480     24.4KB/s   00:00
```

4. Per trasferire un file nell'altra direzione, ovvero dall'istanza Amazon EC2 al computer, inverti l'ordine dei parametri host. Ad esempio, puoi trasferire `my-file.txt` dall'istanza EC2 a una destinazione nel computer locale come `my-file2.txt`, come illustrato negli esempi seguenti.

- (DNS pubblico) Per trasferire un file a una destinazione del computer, immetti il seguente comando dal computer.

```
scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-file.txt path/my-file2.txt
```

- (IPv6) Per trasferire un file a una destinazione del computer se l'istanza ha un indirizzo IPv6, immetti il seguente comando dal computer. L'indirizzo IPv6 deve essere racchiuso tra parentesi quadrate (`[ ]`), che devono essere inserite dopo un carattere di escape (\).

```
scp -i /path/key-pair-name.pem ec2-user@\[instance-IPv6-address\]:path/my-file.txt path/my-file2.txt
```

Connessione all'istanza Linux da Windows

Per connetterti alla tua istanza Linux da un computer locale con sistema operativo Windows hai a disposizione i metodi seguenti..

Connessione all'istanza Linux da Windows tramite OpenSSH

Le seguenti procedure mostrano come connettersi all'istanza Linux da Windows utilizzando OpenSSH, uno strumento di connettività open source per l'accesso remoto con il protocollo SSH. OpenSSH è supportato su Windows Server 2019 e sistemi operativi successivi.

Indice

Prerequisiti

Per connetterti a un'istanza Linux da Windows tramite OpenSSH, devi soddisfare i prerequisiti seguenti.

Verificare che l'istanza sia pronta

> Dopo aver avviato un'istanza, possono essere necessari alcuni minuti affinché sia pronta e sia possibile connettervisi. Verifica che l'istanza abbia superato i controlli dello stato. Puoi vedere queste informazioni nella colonna Status checks (Verifiche di stato) della pagina Instances (Istanze).

Verificare i prerequisiti generali per la connessione all'istanza

> Per trovare il nome DNS pubblico o l'indirizzo IP dell'istanza e il nome utente da utilizzare per connettersi all'istanza, consulta Ottenimento di informazioni sull'istanza.

Verifica della versione Windows

Per connetterti all'istanza Linux da Windows tramite OpenSSH, la versione Windows deve essere Windows Server 2019 e successive.

Verifica i PowerShell prerequisiti

Per installare OpenSSH sul tuo sistema operativo Windows PowerShell utilizzando, devi PowerShell eseguire la versione 5.1 o successiva e il tuo account deve essere membro del gruppo Administrators integrato. Esegui `$PSVersionTable.PSVersion` da PowerShell per verificare la tua versione. PowerShell

Per verificare se sei un membro del gruppo Administrators integrato, esegui il PowerShell comando seguente:

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Se sei un membro del gruppo Amministratori integrato, l'output è `True`.

Installa OpenSSH per Windows usando PowerShell

Per installare OpenSSH per Windows PowerShell utilizzando, esegui il seguente comando: PowerShell

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Output previsto:

```
Path          :
Online        : True
RestartNeeded : False
```

Connessione all'istanza Linux da Windows tramite OpenSSH

Dopo aver installato OpenSSH, utilizza la seguente procedura per connetterti all'istanza Linux da Windows tramite OpenSSH. Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risolvi i problemi di connessione alla tua istanza Linux.

Per connetterti all'istanza tramite OpenSSH

1. In PowerShell o nel prompt dei comandi, usa il ssh comando per connetterti all'istanza. Specifica il percorso e il nome del file della chiave privata (`.pem`), il nome utente per l'istanza e il nome DNS pubblico o l'indirizzo IPv6 per l'istanza. Per ulteriori informazioni su come trovare la chiave privata, il nome utente per l'istanza e il nome DNS o l'indirizzo IPv6 per un'istanza, consulta Individuazione della chiave privata e impostazione delle autorizzazioni e Ottenimento di informazioni sull'istanza. Per connettersi all'istanza, utilizzare uno dei seguenti comandi.
   - (DNS pubblico) Per connettersi utilizzando il nome DNS pubblico dell'istanza, immettere il comando seguente.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
     ```
   - (IPv6) In alternativa, se l'istanza ha un indirizzo IPv6, per connettersi utilizzando l'indirizzo IPv6 dell'istanza, immettere il comando seguente.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
     ```

   La risposta visualizzata sarà simile alla seguente:

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
    can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no/[fingerprint])?
   ```
2. (Opzionale) Verificare che l'impronta riportata nell'avviso di sicurezza corrisponda all'impronta ottenuta precedentemente in (Opzionale) Ottenimento dell'impronta dell'istanza. Se queste impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco. man-in-the-middle Se invece corrispondono, passare alla fase successiva.
3. Specificare (sì **`yes`**.

   La risposta visualizzata sarà simile alla seguente:

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
    the list of known hosts.
   ```

Disinstalla OpenSSH da Windows usando PowerShell

Per disinstallare OpenSSH da Windows PowerShell utilizzando, esegui il seguente comando: PowerShell

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Output previsto:

```
Path          :
Online        : True
RestartNeeded : True
```

Connessione all'istanza Linux da Windows tramite PuTTY

Se utilizzi Windows Server 2019 o versione successiva, ti consigliamo di utilizzare OpenSSH, che è uno strumento di connettività open source per l'accesso remoto con il protocollo SSH. Per i passaggi per connetterti a un'istanza Linux da Windows tramite OpenSSH, consulta Connessione all'istanza Linux da Windows tramite OpenSSH.

Le seguenti istruzioni illustrano come stabilire una connessione a un'istanza tramite PuTTY, un client SSH gratuito per Windows. Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risolvi i problemi di connessione alla tua istanza Linux.

Indice

Prerequisiti

Prima di connetterti a un'istanza Linux tramite PuTTY, è necessario soddisfare i prerequisiti seguenti.

Verificare che l'istanza sia pronta

Dopo aver avviato un'istanza, possono essere necessari alcuni minuti affinché sia pronta e sia possibile connettervisi. Verifica che l'istanza abbia superato i controlli dello stato. Puoi vedere

queste informazioni nella colonna Status checks (Verifiche di stato) della pagina Instances (Istanze).

Verificare i prerequisiti generali per la connessione all'istanza

Per trovare il nome DNS pubblico o l'indirizzo IP dell'istanza e il nome utente da utilizzare per connettersi all'istanza, consulta Ottenimento di informazioni sull'istanza.

Installare PuTTY sul computer locale

Scaricare e installare PuTTY dalla pagina di download di PuTTY. Se è già installata una versione precedente di PuTTY, ti consigliamo di scaricare la versione più aggiornata. Assicurarsi di installare l'intera suite.

Conversione della chiave privata .pem in .ppk tramite PuTTYgen

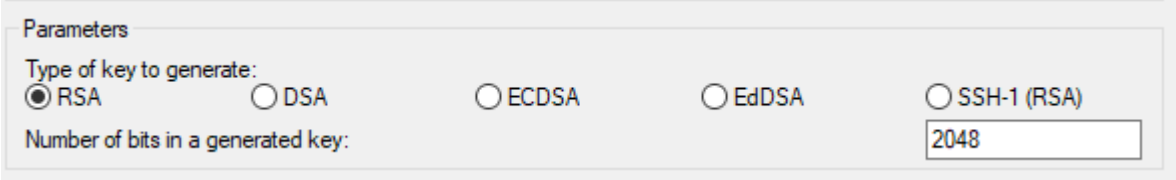
Per la coppia di chiavi specificata all'avvio dell'istanza, se si sceglie di creare la chiave privata nel formato .pem, è necessario convertirla in un file .ppk per utilizzarla con PuTTY. Individuare il file privato con estensione .pem, quindi seguire i passaggi nella sezione successiva.

Convertire la chiave privata tramite PuTTYgen

PuTTY non supporta a livello nativo il formato PEM per le chiavi SSH. PuTTY fornisce uno strumento denominato PuTTYgen, che converte le chiavi PEM nel formato PPK richiesto per PuTTY. È necessario convertire la chiave privata (file .pem) in questo formato (file .ppk) prima di tentare una connessione all'istanza tramite PuTTY.

Conversione della chiave privata .pem in .ppk.

1. Dal menu Start, scegliere All Programs (Tutti i programmi), PuTTY, PuTTYgen.
2. In Type of key to generate (Tipo di chiave da generare) scegliere RSA. Se la versione di PuTTYgen non include questa opzione scegli SSH-2 RSA.



3. Scegliere Load (Carica). Di default, PuTTYgen visualizza solo i file con estensione `.ppk`. Per individuare il file `.pem`, scegli l'opzione per visualizzare tutti i tipi di file.

4. Selezionare il file `.pem` per la coppia di chiavi specificata all'avvio dell'istanza, quindi scegliere Open (Apri). PuTTYgen visualizza un avviso che il file `.pem` è stato importato correttamente. Seleziona OK.
5. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegliere Save private key (Salva chiave privata). PuTTYgen visualizza un avviso relativo al salvataggio della chiave senza passphrase. Scegliere Yes (Sì).

> **Note**
>
> Le chiavi private con passphrase dispongono di un ulteriore livello di sicurezza. Anche se la chiave privata dovesse venire scoperta, non sarebbe possibile utilizzarla senza la passphrase. L'unico inconveniente dell'utilizzo di una passphrase è che complica l'automazione, in quanto è necessario l'intervento dell'utente per eseguire l'accesso all'istanza o per copiare i file in un'istanza.

6. Specificare per la chiave lo stesso nome usato per la coppia di chiavi (ad esempio, `key-pair-name`) e selezionare Save (Salva). PuTTY aggiunge automaticamente l'estensione di file `.ppk`.

La chiave privata ora ha il formato corretto per l'utilizzo con PuTTY. A questo punto è possibile connettersi all'istanza utilizzando il client SSH di PuTTY.

Connessione all'istanza di Linux

Utilizza la seguente procedura per stabilire una connessione a un'istanza Linux tramite PuTTY. Devi disporre del file `.ppk` creato per la chiave privata. Per maggiori informazioni, consulta Convertire la chiave privata tramite PuTTYgen nella sezione precedente. Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risolvi i problemi di connessione alla tua istanza Linux.

Ultima versione testata di PuTTY: .78

Per connettersi all'istanza tramite PuTTY

1. Avvia PuTTY (dal menu Start, cerca PuTTY e scegli Apri).
2. Nel riquadro Category (Categoria), scegliere Session (Sessione) e completare i seguenti campi:

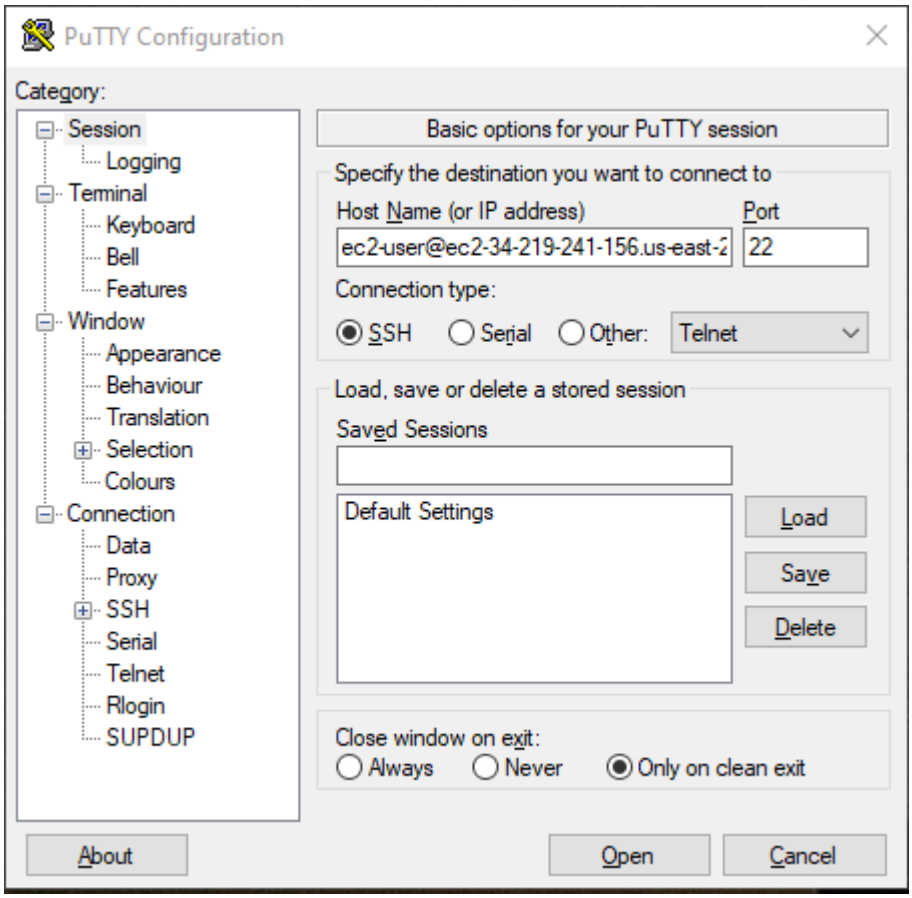
a. Nella casella Host Name (Nome host) eseguire una delle operazioni seguenti:

   - (DNS pubblico) Per connetterti utilizzando il nome DNS pubblico dell'istanza, inserisci @. *instance-user-nameinstance-public-dns-name*
   - *(IPv6) In alternativa, se l'istanza ha un indirizzo IPv6, per connetterti utilizzando l'indirizzo IPv6 dell'istanza, inserisci @ Instance-IPv6-address. instance-user-name*

   Per ulteriori informazioni su come ottenere il nome utente per l'istanza e il nome DNS pubblico o l'indirizzo IPv6 dell'istanza, consulta Ottenimento di informazioni sull'istanza.

b. Assicurarsi che il valore specificato per la Porta sia 22.

c. In Connection type (Tipo di connessione), selezionare SSH.



3. (Opzionale) È possibile configurare PuTTY in modo che invii automaticamente dati 'keepalive' a intervalli regolari per mantenere attiva la sessione. Ciò risulta utile per evitare la disconnessione dall'istanza a causa dell'inattività della sessione. Nel riquadro Categoria, scegli Connessione, quindi immettere l'intervallo richiesto nel campo Secondi tra dati keepalive. Ad esempio, se la

sessione si disconnette dopo 10 minuti di inattività, immettere 180 per configurare PuTTY per l'invio di dati keepalive ogni 3 minuti.

4. Nel riquadro Categoria, espandere Connessione, SSH e Autenticazione. Scegli Credenziali.
5. Accanto a File della chiave privata per l'autenticazione, scegli Sfoglia. Nella finestra di dialogo Seleziona file chiave privata, seleziona il file `.ppk` che hai generato per la tua coppia di chiavi. Puoi fare doppio clic sul file o scegliere Apri nella finestra di dialogo Seleziona file chiave privata.
6. (Opzionale) Se si prevede di connetterti di nuovo dopo questa sessione, puoi salvare le informazioni sulla sessione per uso futuro. Nel riquadro Categoria, scegli Sessione. Immetti un nome per la sessione in Sessioni salvate e quindi scegli Salva.
7. Per connetterti all'istanza, scegli Apri.
8. Se è la prima volta che si stabilisce una connessione a questa istanza, PuTTY visualizza una finestra di dialogo contenente un avviso di sicurezza che richiede di confermare l'affidabilità dell'host a cui ci si sta connettendo.

    a. (Opzionale) Verificare che l'impronta riportata nella finestra di dialogo dell'avviso di sicurezza corrisponda all'impronta precedentemente ottenuta in (Opzionale) Ottenimento dell'impronta dell'istanza. Se queste impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco "». man-in-the-middle Se invece corrispondono, passare alla fase successiva.

    b. Scegliere Accept (Accetta). Viene visualizzata una finestra e a questo punto si è connessi all'istanza.

> **Note**
>
> Se hai specificato una passphrase quando hai convertito la chiave privata nel formato PuTTY, devi specificare tale passphrase quando accedi all'istanza.

Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risolvi i problemi di connessione alla tua istanza Linux.

Trasferimento di file nell'istanza Linux tramite il client PuTTY Secure Copy

PuTTY Secure Copy client (PSCP) è uno strumento a riga di comando che puoi utilizzare per trasferire file tra il computer Windows in uso e un'istanza Linux. Se preferisci utilizzare un'interfaccia utente grafica (GUI), puoi utilizzare uno strumento GUI open source denominato WinSCP. Per ulteriori informazioni, consulta Trasferimento di file all'istanza Linux tramite WinSCP.

Per utilizzare PSCP, devi disporre della chiave privata generata in Convertire la chiave privata tramite PuTTYgen. È inoltre necessario il nome DNS pubblico dell'istanza Linux o l'indirizzo IPv6 se l'istanza ne ha uno.

Nell'esempio seguente, il file `Sample_file.txt` viene trasferito dall'unità C:\ su un computer Windows alla home directory `instance-user-name` su un'istanza Amazon Linux. Per trasferire un file, utilizzare uno dei comandi seguenti.

- (DNS pubblico) Per trasferire un file utilizzando il nome DNS pubblico dell'istanza, immettere il comando seguente.

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@instance-public-dns-name:/home/instance-user-name/Sample_file.txt
```

- (IPv6) In alternativa, se l'istanza dispone di un indirizzo IPv6, per trasferire un file utilizzando l'indirizzo IPv6 dell'istanza, immettere il comando seguente. L'indirizzo IPv6 deve essere racchiuso tra parentesi quadrate (`[ ]`).

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@[instance-IPv6-address]:/home/instance-user-name/Sample_file.txt
```

Trasferimento di file all'istanza Linux tramite WinSCP

WinSCP è una utility di gestione di file basata su GUI per Windows che ti consente di caricare e trasferire file a un computer remoto utilizzando i protocolli SFTP, SCP, FTP e FTPS. Con WinSCP puoi trascinare e rilasciare i file selezionati da un computer Windows a un'istanza Linux oppure sincronizzare intere strutture di directory tra due sistemi.

Requisiti

- Devi avere la chiave privata generata in Convertire la chiave privata tramite PuTTYgen.
- Devi avere anche il nome DNS pubblico dell'istanza Linux.
- L'istanza Linux deve avere il pacchetto `scp` installato. Per alcuni sistemi operativi, installi il pacchetto `openssh-clients`. Per altri, ad esempio le AMI ottimizzate per Amazon ECS, installi il pacchetto `scp`. Controlla la documentazione per la tua distribuzione Linux.

Per connettersi all'istanza tramite WinSCP

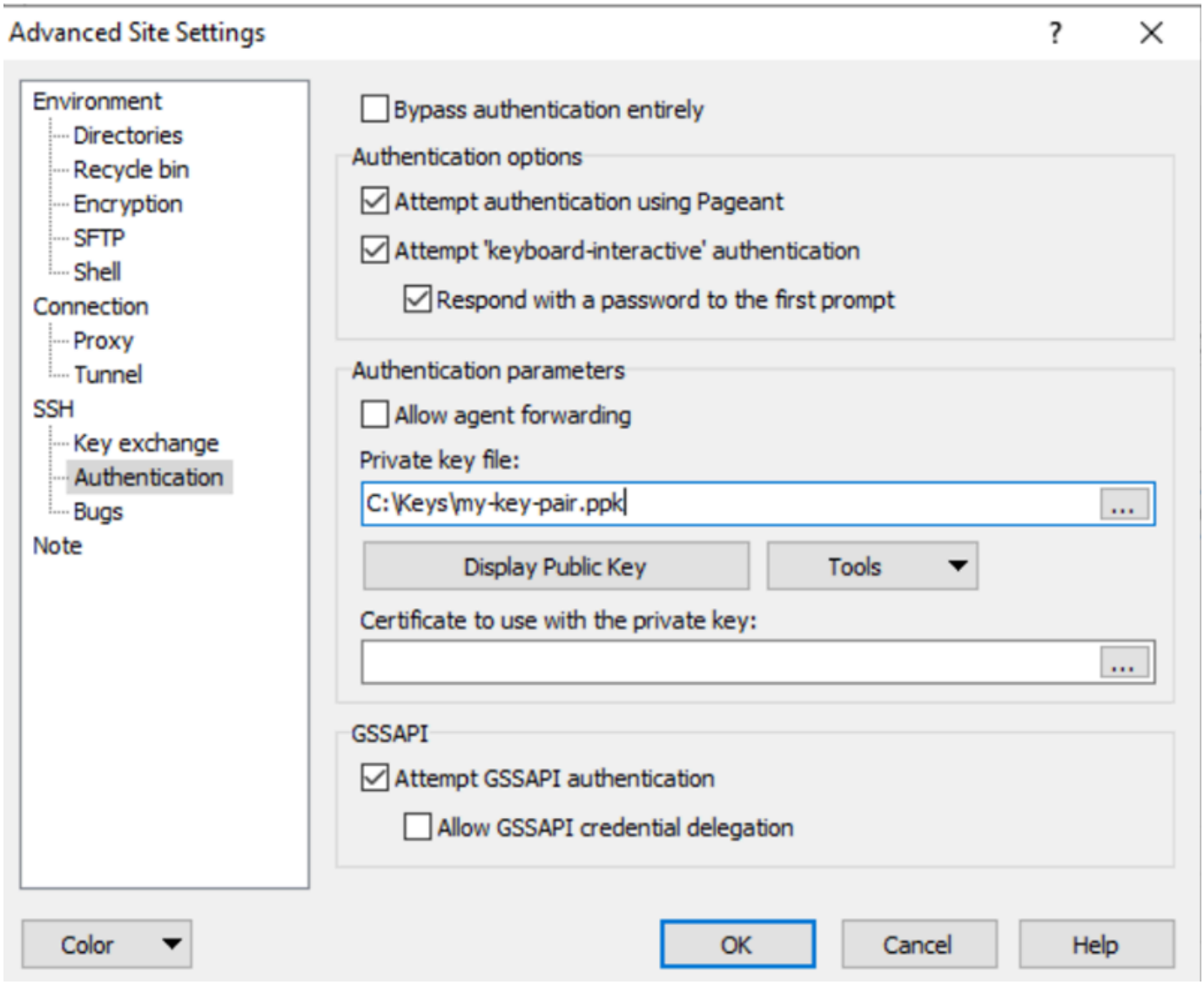
1. Scaricare e installare WinSCP dalla pagina http://winscp.net/eng/download.php. La maggior parte degli utenti può utilizzare le opzioni di installazione di default.
2. Avviare WinSCP.
3. Nella schermata di accesso WinSCP per Nome host, immettere uno dei seguenti valori:
   - (DNS pubblico o indirizzo IPv4) Per accedere utilizzando il nome DNS pubblico o l'indirizzo IPv4 pubblico dell'istanza, immettere il nome DNS pubblico o l'indirizzo IPv4 pubblico per l'istanza.
   - (IPv6) In alternativa, se l'istanza dispone di un indirizzo IPv6, per accedere utilizzando l'indirizzo IPv6 dell'istanza, immettere l'indirizzo IPv6 per l'istanza.
4. Per User name (Nome utente) immetti il nome utente di default per la tua AMI.
   - Per AL2023, Amazon Linux 2 o Amazon Linux AMI, il nome utente è `ec2-user`.
   - Per un'AMI CentOS, il nome utente è `centos` o `ec2-user`.
   - Per un'AMI Debian, il nome utente è `admin`.
   - Per un'AMI Fedora, il nome utente è `fedora` o `ec2-user`.
   - Per un'AMI RHEL, il nome utente è `ec2-user` o `root`.
   - Per un'AMI SUSE, il nome utente è `ec2-user` o `root`.
   - Per un'AMI Ubuntu, il nome utente è `ubuntu`.
   - Per un'AMI Oracle, il nome utente è `ec2-user`.
   - Per un'AMI Bitnami, il nome utente è `bitnami`.

   > **Note**
   >
   > Per trovare il nome utente predefinito per altre distribuzioni Linux, rivolgiti al provider AMI.

5. Specifica il file della chiave privata per l'istanza.
   a. Seleziona il pulsante Avanzate....
   b. In SSH, scegli Autenticazione.
   c. Specifica il percorso del file della chiave privata o utilizza il pulsante ... per accedere al file della coppia di chiavi.

d. Scegli OK.

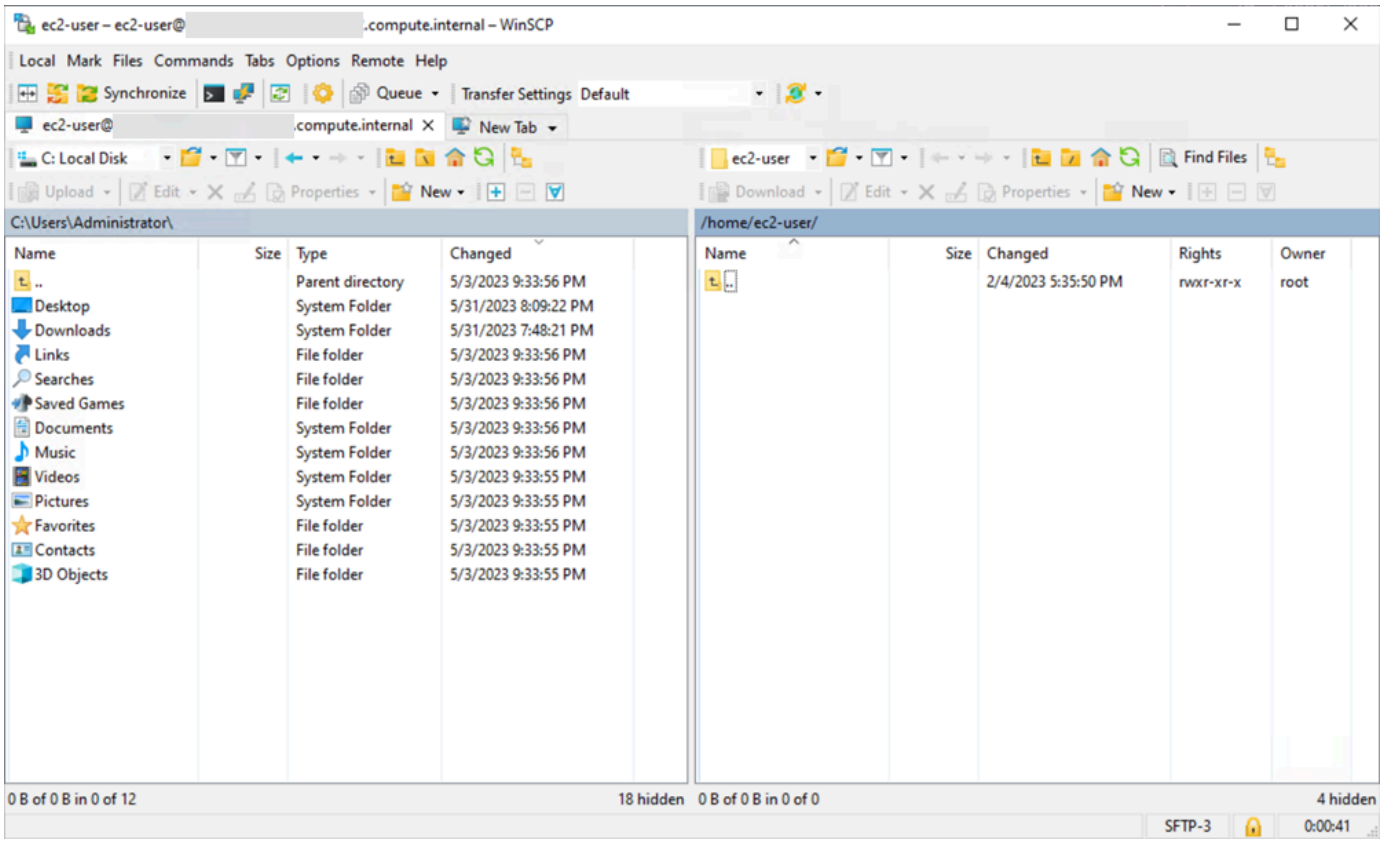
Di seguito è riportato uno screenshot di WinSCP versione 6.1:



WinSCP richiede il file della chiave privata PuTTY (`.ppk`). È possibile convertire un file della chiave di sicurezza `.pem` in formato `.ppk` utilizzando PuTTYgen. Per ulteriori informazioni, consulta Convertire la chiave privata tramite PuTTYgen.

6. (Opzionale) Nel pannello a sinistra, scegliere Directories (Directory). Per Remote directory (Directory remota), immettere il percorso alla directory in cui aggiungere i file. Per aprire le impostazioni avanzate del sito (per le versioni più recenti di WinSCP), scegliere Advanced (Avanzate). Per cercare l'impostazione Remote directory (Directory remota), in Environment (Ambiente), scegliere Directories (Directory).

7. Selezionare Login (Accesso). Per aggiungere l'impronta dell'host alla cache dell'host, scegliere Yes (Sì).



8. Dopo aver stabilito la connessione, nella finestra della connessione l'istanza Linux si trova a destra, mentre il computer locale si trova a sinistra. Puoi trascinare e rilasciare i file tra il file system remoto e il computer locale. Per ulteriori informazioni su WinSCP, consultare la documentazione del progetto all'indirizzo http://winscp.net/eng/docs/start.

   Se viene visualizzato un errore che indica che non è possibile eseguire SCP per avviare il trasferimento, verificare di avere installato scp nell'istanza Linux.

Connessione alla tua istanza Linux da Windows tramite Sottosistema Windows per Linux (WSL).

Dopo aver avviato l'istanza, è possibile connettervisi e utilizzarla come fosse un computer fisico.

Le seguenti istruzioni illustrano come stabilire una connessione a un'istanza tramite una distribuzione Linux sul Windows Subsystem per Linux (WSL). WSL è disponibile come download gratuito e ti permette di eseguire strumenti a riga di comando nativi di Linux direttamente su Windows, oltre al tradizionale desktop Windows, senza il sovraccarico di una macchina virtuale.

Installando WSL puoi utilizzare un ambiente Linux nativo per connetterti alle istanze EC2 Linux invece che tramite PuTTY o PuTTYgen. L'ambiente Linux semplifica la connessione alle istanze Linux, in quanto dotato di un client SSH nativo che si può utilizzare per connettersi alle istanze Linux e per modificare le autorizzazioni del file chiave .pem. La console Amazon EC2 fornisce il comando SSH per la connessione all'istanza Linux ed è possibile ottenere un output verbose dal comando SSH per la risoluzione dei problemi. Per ulteriori informazioni, consulta la Documentazione di Windows Subsystem per Linux.

> **Note**
>
> Dopo l'installazione di WSL, tutti i prerequisiti e i passaggi sono gli stessi descritti in Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH. è l'esperienza sarà identica all'utilizzo di Linux nativo.

Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risolvi i problemi di connessione alla tua istanza Linux.

Indice

Prerequisiti

Prima di connetterti a un'istanza Linux, è necessario soddisfare i prerequisiti seguenti:

Verificare che l'istanza sia pronta

Dopo aver avviato un'istanza, possono essere necessari alcuni minuti affinché sia pronta e sia possibile connettervisi. Verifica che l'istanza abbia superato i controlli dello stato. Puoi vedere queste informazioni nella colonna Status checks (Verifiche di stato) della pagina Instances (Istanze).

Verificare i prerequisiti generali per la connessione all'istanza

Per trovare il nome DNS pubblico o l'indirizzo IP dell'istanza e il nome utente da utilizzare per connettersi all'istanza, consulta Ottenimento di informazioni sull'istanza.

Installare Windows Subsystem per Linux (WSL) e una distribuzione Linux sul computer locale

Installare WSL e una distribuzione Linux seguendo le istruzioni della Guida all'installazione di Windows 10. L'esempio riportato nelle istruzioni installa la distribuzione Ubuntu di Linux, ma si può installare qualunque distribuzione. Affinché vengano applicate le modifiche, ti verrà chiesto di riavviare il computer.

Copia della chiave privata da Windows a WSL

In una finestra del terminale WSL, copia il file `.pem` (per la coppia di chiavi specificata quando hai avviato l'istanza) da Windows a WSL. Prendi nota del percorso completo al file `.pem` su WSL da utilizzare nella connessione all'istanza. Per informazioni su come specificare il percorso al disco rigido Windows, consultare Come faccio ad accedere alla mia unità C?. Per ulteriori informazioni sulle coppie di chiavi e sulle istanze di Windows, consulta Coppie di chiavi Amazon EC2 e istanze Windows.

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

Connessione a un'istanza Linux tramite WSL

Utilizza la procedura seguente per stabilire una connessione all'istanza Linux utilizzando Windows Subsystem per Linux (WSL). Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risolvi i problemi di connessione alla tua istanza Linux.

Per connettersi all'istanza tramite SSH

1. Nella finestra del terminale, utilizzare il comando ssh per connettersi all'istanza. Specificare il percorso e il nome del file della chiave privata (`.pem`), il nome utente per l'istanza e il nome DNS pubblico o l'indirizzo IPv6 per l'istanza. Per ulteriori informazioni su come trovare la chiave privata, il nome utente per l'istanza e il nome DNS o l'indirizzo IPv6 per un'istanza, consulta Individuazione della chiave privata e impostazione delle autorizzazioni e Ottenimento di informazioni sull'istanza. Per connettersi all'istanza, utilizzare uno dei seguenti comandi.
   - (DNS pubblico) Per connettersi utilizzando il nome DNS pubblico dell'istanza, immettere il comando seguente.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@my-instance-public-dns-name
     ```

- (IPv6) In alternativa, se l'istanza dispone di un indirizzo IPv6, è possibile connettersi utilizzando il suo indirizzo IPv6. Specificare il comando ssh con il percorso del file della chiave privata (.pem), il nome utente appropriato e l'indirizzo IPv6.

  ```
  ssh -i /path/key-pair-name.pem instance-user-name@my-instance-IPv6-address
  ```

  La risposta visualizzata sarà simile alla seguente:

  ```
  The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
  can't be established.
  RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
  Are you sure you want to continue connecting (yes/no)?
  ```

2. (Opzionale) Verificare che l'impronta riportata nell'avviso di sicurezza corrisponda all'impronta ottenuta precedentemente in (Opzionale) Ottenimento dell'impronta dell'istanza. Se queste impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco "»man-in-the-middle. Se invece corrispondono, passare alla fase successiva.
3. Specificare (sì `yes`.

   La risposta visualizzata sarà simile alla seguente:

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
   to the list of known hosts.
   ```

Trasferimento di file alle istanze Linux da Linux tramite SCP

Un modo per trasferire file tra il computer locale e un'istanza Linux è utilizzare il protocollo secure copy (SCP). Questa sezione descrive come trasferire file utilizzando la funzionalità SCP. La procedura è simile a quella valida per la connessione a un'istanza tramite SSH.

Prerequisiti

- Verificare i prerequisiti generali per il trasferimento di file all'istanza.

  Prima di trasferire file tra il computer locale e l'istanza, esegui le seguenti azioni per assicurarti di disporre di tutte le informazioni necessarie.

  - Ottenimento di informazioni sull'istanza
  - Individuazione della chiave privata e impostazione delle autorizzazioni

  - (Opzionale) Ottenimento dell'impronta dell'istanza
- Installare un client SCP

  La maggior parte dei computer Linux, Unix e Apple includono un client SCP per impostazione di default. Se il computer in uso non dispone di questo client, il progetto OpenSSH fornisce un'implementazione gratuita della suite completa di strumenti SSH, incluso un client SCP. Per ulteriori informazioni, consulta https://www.openssh.com.

La procedura seguente descrive in dettaglio le fasi da eseguire per utilizzare la funzionalità SCP per il trasferimento di un file. Se è già stata stabilita una connessione all'istanza tramite SSH e se sono già state verificate le relative impronte, è possibile iniziare con la fase contenente il comando SCP (fase 4).

Per utilizzare la funzionalità SCP per trasferire un file

1. Trasferire un file all'istanza utilizzando il nome DNS pubblico dell'istanza. Ad esempio, se il nome del file della chiave privata è `key-pair-name`, il file da trasferire è `SampleFile.txt`, il nome utente è `instance-user-name` e il nome DNS pubblico dell'istanza è `my-instance-public-dns-name` o l'indirizzo IPv6 è `my-instance-IPv6-address`, utilizzare i comandi seguenti per copiare il file nella home directory `instance-user-name`.
   - (DNS pubblico) Per trasferire un file utilizzando il nome DNS pubblico dell'istanza, immettere il comando seguente.

     ```
     scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@my-instance-public-dns-name:~
     ```
   - (IPv6) In alternativa, se l'istanza dispone di un indirizzo IPv6, è possibile trasferire un file utilizzando l'indirizzo IPv6 dell'istanza. L'indirizzo IPv6 deve essere racchiuso tra parentesi quadrate (`[ ]`), che devono essere inserite dopo un carattere di escape (\).

     ```
     scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@\[my-instance-IPv6-address\]:~
     ```

   La risposta visualizzata sarà simile alla seguente:

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)' can't be established.
   RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
   ```

```
Are you sure you want to continue connecting (yes/no)?
```

2. (Opzionale) Verificare che l'impronta riportata nell'avviso di sicurezza corrisponda all'impronta ottenuta precedentemente in (Opzionale) Ottenimento dell'impronta dell'istanza. Se queste impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco "». man-in-the-middle Se invece corrispondono, passare alla fase successiva.
3. Specificare (sì **`yes`**.

   La risposta visualizzata sarà simile alla seguente:

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
   to the list of known hosts.
   Sending file modes: C0644 20 SampleFile.txt
   Sink: C0644 20 SampleFile.txt
   SampleFile.txt                                100%   20     0.0KB/s   00:00
   ```

   Se viene visualizzato l'errore "bash: scp: command not found" (comando bash: scp: non trovato), è prima necessario installare scp sull'istanza Linux. Per alcuni sistemi operativi, si trova nel pacchetto `openssh-clients`. Per le varianti Amazon Linux, ad esempio AMI ottimizzata per Amazon ECS, utilizzare il seguente comando per installare scp:

   ```
   [ec2-user ~]$ sudo yum install -y openssh-clients
   ```
4. Per trasferire i file nell'altra direzione, ovvero dall'istanza Amazon EC2 al computer locale, invertire l'ordine dei parametri host. Ad esempio, per trasferire il file `SampleFile.txt` dall'istanza EC2 alla home directory sul computer locale come `SampleFile2.txt`, utilizzare uno dei comandi seguenti sul computer locale.
   - (DNS pubblico) Per trasferire un file utilizzando il nome DNS pubblico dell'istanza, immettere il comando seguente.

     ```
     scp -i /path/key-pair-name.pem instance-user-
     name@ec2-198-51-100-1.compute-1.amazonaws.com:~/SampleFile.txt ~/
     SampleFile2.txt
     ```
   - (IPv6) In alternativa, se l'istanza dispone di un indirizzo IPv6, per trasferire i file nella direzione opposta utilizzando l'indirizzo IPv6 dell'istanza, immettere il comando seguente.

     ```
     scp -i /path/key-pair-name.pem instance-user-name@
     \[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~/SampleFile.txt ~/SampleFile2.txt
     ```

Disinstallazione di WSL

Per informazioni su come disinstallare Windows Subsystem per Linux, consultare Come faccio a disinstallare una distribuzione WSL?.

Connessione a un'istanza Linux tramite EC2 Instance Connect

Con Amazon EC2 Instance Connect, puoi connetterti in modo semplice e sicuro alle istanze Linux tramite Secure Shell (SSH). Con EC2 Instance Connect, utilizzi policy e principi AWS Identity and Access Management (IAM) per controllare l'accesso SSH alle tue istanze, eliminando la necessità di condividere e gestire le chiavi SSH. Tutte le richieste di connessione che utilizzano EC2 Instance Connect vengono registrate AWS CloudTrail in modo da poter controllare le richieste di connessione.

Puoi utilizzare EC2 Instance Connect per collegarti alle istanze Linux tramite la console Amazon EC2 o un client SSH a scelta.

Quando ti connetti a un'istanza tramite EC2 Instance Connect, l'API di Instance Connect invia una chiave pubblica SSH ai metadati dell'istanza, dove rimane per 60 secondi. Una policy IAM collegata al tuo utente autorizza quest'ultimo a inserire la chiave pubblica tra i metadati dell'istanza. Il daemon SSH utilizza `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, configurati al momento dell'installazione di Instance Connect, per recuperare la chiave pubblica dai metadati dell'istanza al fine effettuare l'autenticazione e ti permette di collegarti all'istanza.

È possibile utilizzare EC2 Instance Connect per connettersi a istanze che dispongono di indirizzi IP pubblici o privati. Per ulteriori informazioni, consulta Connessione tramite EC2 Instance Connect.

Per un post del blog che illustra come migliorare la sicurezza degli host bastione utilizzando EC2 Instance Connect, consulta Securing your bastion hosts with Amazon EC2 Instance Connect.

> **Tip**
>
> EC2 Instance Connect è una delle opzioni per la connessione all'istanza Linux. Per altre opzioni, vedi Connessione all'istanza di Linux Per connetterti a un'istanza Windows, consulta. Connettiti all'istanza Windows

Indice

- Prerequisiti
- Concessione di un'autorizzazione IAM per EC2 Instance Connect
- Installazione di EC2 Instance Connect sulle istanze EC2
- Connessione tramite EC2 Instance Connect
- Disinstallazione di EC2 Instance Connect

Tutorial: completa la configurazione richiesta per connetterti alla tua istanza utilizzando EC2 Instance Connect

Per connetterti alla tua istanza utilizzando EC2 Instance Connect nella console Amazon EC2, devi prima completare la configurazione dei prerequisiti che ti consentirà di connetterti correttamente all'istanza. Lo scopo di questo tutorial è di guidarti attraverso le attività per completare la configurazione dei prerequisiti.

Panoramica del tutorial

In questo tutorial, completerai le seguenti quattro attività:

- Attività 1: creare e allegare una policy IAM per consentire l'utilizzo di EC2 Instance Connect

  Per prima cosa creerai una policy IAM che contenga le autorizzazioni IAM che ti consentono di inviare una chiave pubblica ai metadati dell'istanza. Allegherai questa policy alla tua identità IAM (utente, gruppo di utenti o ruolo) in modo che la tua identità IAM ottenga queste autorizzazioni.
- Attività 2: crea un gruppo di sicurezza per consentire il traffico in entrata dal servizio EC2 Instance Connect alla tua istanza

  Quindi creerai un gruppo di sicurezza che consente il traffico dal servizio EC2 Instance Connect alla tua istanza. Questo è necessario quando utilizzi EC2 Instance Connect nella console Amazon EC2 per connetterti alla tua istanza.
- Attività 3: Avvia l'istanza

  Lancerai quindi un'istanza EC2 utilizzando un'AMI preinstallata con EC2 Instance Connect e aggiungerai il gruppo di sicurezza creato nel passaggio precedente.
- Attività 4: Connettiti alla tua istanza

  Infine, utilizzerai EC2 Instance Connect nella console Amazon EC2 per connetterti alla tua istanza. Se riesci a connetterti, puoi essere certo che la configurazione dei prerequisiti che hai completato nelle attività 1, 2 e 3 abbia avuto successo.

Attività 1: creare e allegare una policy IAM per consentire l'utilizzo di EC2 Instance Connect

Quando ti connetti a un'istanza tramite EC2 Instance Connect, l'API di EC2 Instance Connect invia una chiave pubblica SSH ai metadati dell'istanza, dove rimane per 60 secondi. Hai bisogno di una policy IAM allegata alla tua identità IAM (utente, gruppo di utenti o ruolo) per concederti l'autorizzazione richiesta per inviare la chiave pubblica ai metadati dell'istanza.

Obiettivo del compito

In questa attività, creerai la policy IAM che concede l'autorizzazione a inviare la chiave pubblica all'istanza. L'azione specifica da consentire è`ec2-instance-connect:SendSSHPublicKey`. È inoltre necessario consentire l'`ec2:DescribeInstances`azione in modo da poter visualizzare e selezionare l'istanza nella console Amazon EC2.

Una volta creata la policy, la collegherai alla tua identità IAM (utente, gruppo di utenti o ruolo) in modo che la tua identità IAM ottenga le autorizzazioni.

Creerai una policy configurata come segue:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

Important

La politica IAM creata in questo tutorial è una politica altamente permissiva; consente di connettersi a qualsiasi istanza utilizzando qualsiasi nome utente AMI. Stiamo usando questa politica altamente permissiva per mantenere il tutorial semplice e focalizzato sulle configurazioni specifiche che questo tutorial insegna. Tuttavia, in un ambiente di produzione, consigliamo di configurare la policy IAM in modo da fornire autorizzazioni con privilegi minimi.

Per esempi di policy IAM, consulta Concessione di un'autorizzazione IAM per EC2 Instance Connect.

Passaggi per creare e allegare la policy IAM

Utilizza i seguenti passaggi per creare e allegare la policy IAM. Per visualizzare un'animazione dei passaggi, consulta Visualizza un'animazione: Crea una policy IAM eVisualizza un'animazione: Allega una policy IAM.

Per creare e allegare una policy IAM che ti consenta di utilizzare EC2 Instance Connect per connetterti alle tue istanze

1. Per prima cosa, crea la policy IAM
   a. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
   b. Nel pannello di navigazione, selezionare Policies (Policy).
   c. Scegli Create Policy (Crea policy).
   d. Nella pagina Specificare l'autorizzazione, procedi come segue:
      i. Per Service, scegli EC2 Instance Connect.
      ii. In Azioni consentite, nel campo di ricerca inizia a digitare **`send`** per mostrare le azioni pertinenti, quindi seleziona SendSSH. PublicKey
      iii. In Risorse, scegli Tutto. Per un ambiente di produzione, consigliamo di specificare l'istanza tramite il relativo ARN, ma per questo tutorial consentirai tutte le istanze.
      iv. Scegli Aggiungi altre autorizzazioni.
      v. Per Service (Servizio), scegli EC2.
      vi. In Azioni consentite, nel campo di ricerca inizia **`describein`** a digitare per mostrare le azioni pertinenti, quindi seleziona. DescribeInstances
      vii. Seleziona Successivo.
   e. Nella pagina Rivedi e crea, procedi come segue:
      i. In Policy name (Nome policy), immettere un nome per la policy.
      ii. Scegli Crea policy.
2. Quindi allega la politica alla tua identità
   a. Nel pannello di navigazione della console IAM seleziona Policy.

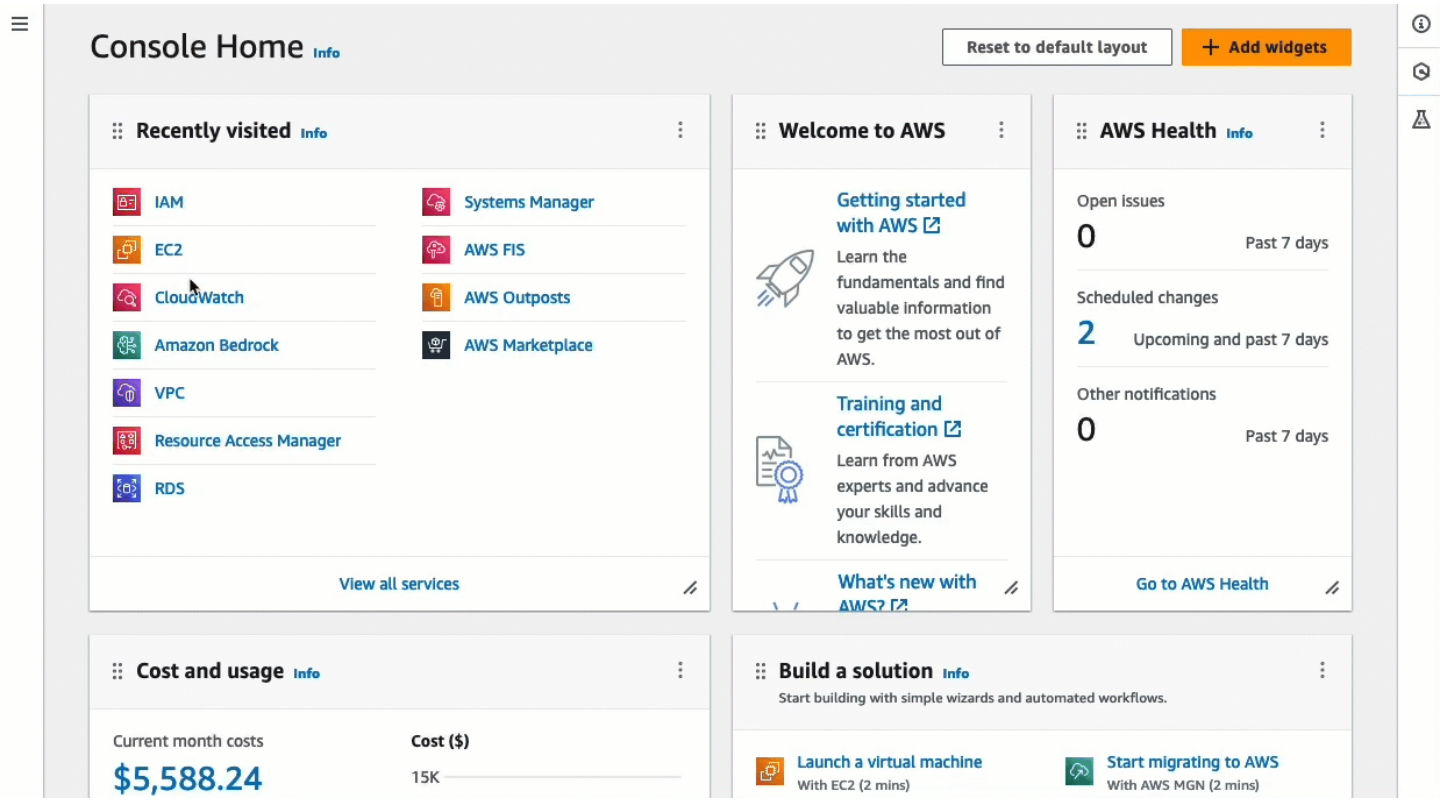
b. Nell'elenco delle politiche, seleziona il pulsante di opzione accanto al nome della politica che hai creato. Puoi utilizzare la casella di ricerca per filtrare l'elenco di policy.

c. Seleziona Operazioni, Collega.

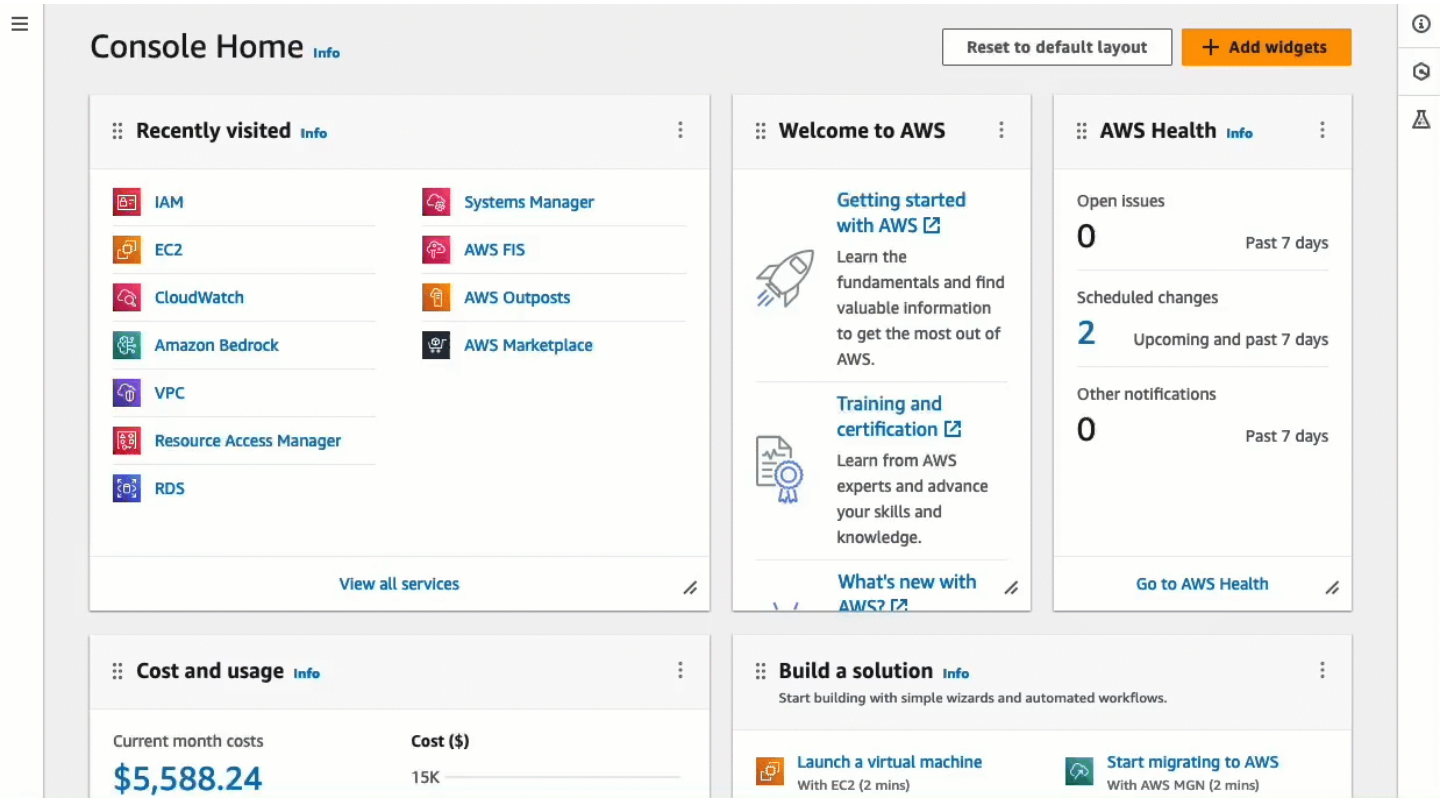
d. In Entità IAM, seleziona la casella di controllo accanto alla tua identità (utente, gruppo di utenti o ruolo). Puoi utilizzare la casella di ricerca per filtrare l'elenco delle entità.

e. Scegli Collega policy.

Visualizza un'animazione: Crea una policy IAM



Visualizza un'animazione: Allega una policy IAM



Attività 2: crea un gruppo di sicurezza per consentire il traffico in entrata dal servizio EC2 Instance Connect alla tua istanza

Quando utilizzi EC2 Instance Connect nella console Amazon EC2 per connetterti a un'istanza, il traffico a cui deve essere consentito di raggiungere l'istanza è il traffico proveniente dal servizio EC2 Instance Connect. Questa operazione è diversa dalla connessione dal computer locale a un'istanza; in tal caso, è necessario consentire il traffico dal computer locale all'istanza. Per consentire il traffico proveniente dal servizio EC2 Instance Connect, è necessario creare un gruppo di sicurezza che consenta il traffico SSH in entrata dall'intervallo di indirizzi IP per il servizio EC2 Instance Connect.

Gli intervalli di indirizzi IP per i AWS servizi sono disponibili all'indirizzo https://ip-ranges.amazonaws.com/ip-ranges.json. Gli intervalli di indirizzi IP di EC2 Instance Connect sono identificati da`"service": "EC2_INSTANCE_CONNECT"`.

Obiettivo dell'attività

In questa attività, troverai innanzitutto l'intervallo di indirizzi IP `EC2_INSTANCE_CONNECT` Regione AWS in cui si trova l'istanza. Quindi creerai un gruppo di sicurezza che consente il traffico SSH in entrata sulla porta 22 da quell'intervallo di indirizzi IP.

Passaggi per creare il gruppo di sicurezza

Utilizza i seguenti passaggi per creare il gruppo di sicurezza. Per visualizzare un'animazione dei passaggi, consulta Visualizza un'animazione: ottieni l'intervallo di indirizzi IP per EC2 Instance Connect per una regione specifica eVisualizza un'animazione: configura un gruppo di sicurezza.

Per creare un gruppo di sicurezza che consenta il traffico in entrata dal servizio EC2 Instance Connect alla tua istanza

1. Per prima cosa ottieni l'intervallo di indirizzi IP per il servizio EC2 Instance Connect

   a. Apri il file JSON degli intervalli di indirizzi AWS IP all'indirizzo https://ip-ranges.amazonaws.com/ip-ranges.json.

   b. Scegli Raw Data.

   c. Trova l'intervallo di indirizzi IP `EC2_INSTANCE_CONNECT` per l'area Regione AWS in cui si trova la tua istanza. Puoi utilizzare il campo di ricerca del browser per cercare il servizio `EC2_INSTANCE_CONNECT` e continuare a cercare finché non trovi la regione in cui si trova l'istanza.

      Ad esempio, se l'istanza si trova nella regione Stati Uniti orientali (Virginia settentrionale`us-east-1`) (), l'intervallo di indirizzi IP per quella `EC2_INSTANCE_CONNECT` regione è`18.206.107.24/29`.

      > **Note**
      >
      > Gli intervalli di indirizzi IP sono diversi per ciascuno Regione AWS.

   d. Copia l'intervallo di indirizzi IP visualizzato accanto `aip_prefix`. Questo intervallo di indirizzi IP verrà utilizzato più avanti in questa procedura.

   Per ulteriori informazioni sul download del file JSON degli intervalli di indirizzi AWS IP e sul filtraggio per servizio, consulta gli intervalli di indirizzi AWS IP nella Amazon VPC User Guide.

2. Quindi crea il gruppo di sicurezza con una regola in entrata per consentire il traffico proveniente dall'intervallo di indirizzi IP copiato

   a. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

   b. Fare clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.

   c. Scegliere Create Security Group (Crea gruppo di sicurezza).

d. In Basic details (Dettagli di base), eseguire le operazioni seguenti:

   i. Per Nome del gruppo di sicurezza, inserisci un nome significativo per il tuo gruppo di sicurezza.

   ii. Per Descrizione, inserisci una descrizione significativa per il tuo gruppo di sicurezza.

e. In Regole in entrata, procedi come segue:

   i. Scegli Aggiungi regola.

   ii. Per Type (Tipo) scegli SSH.

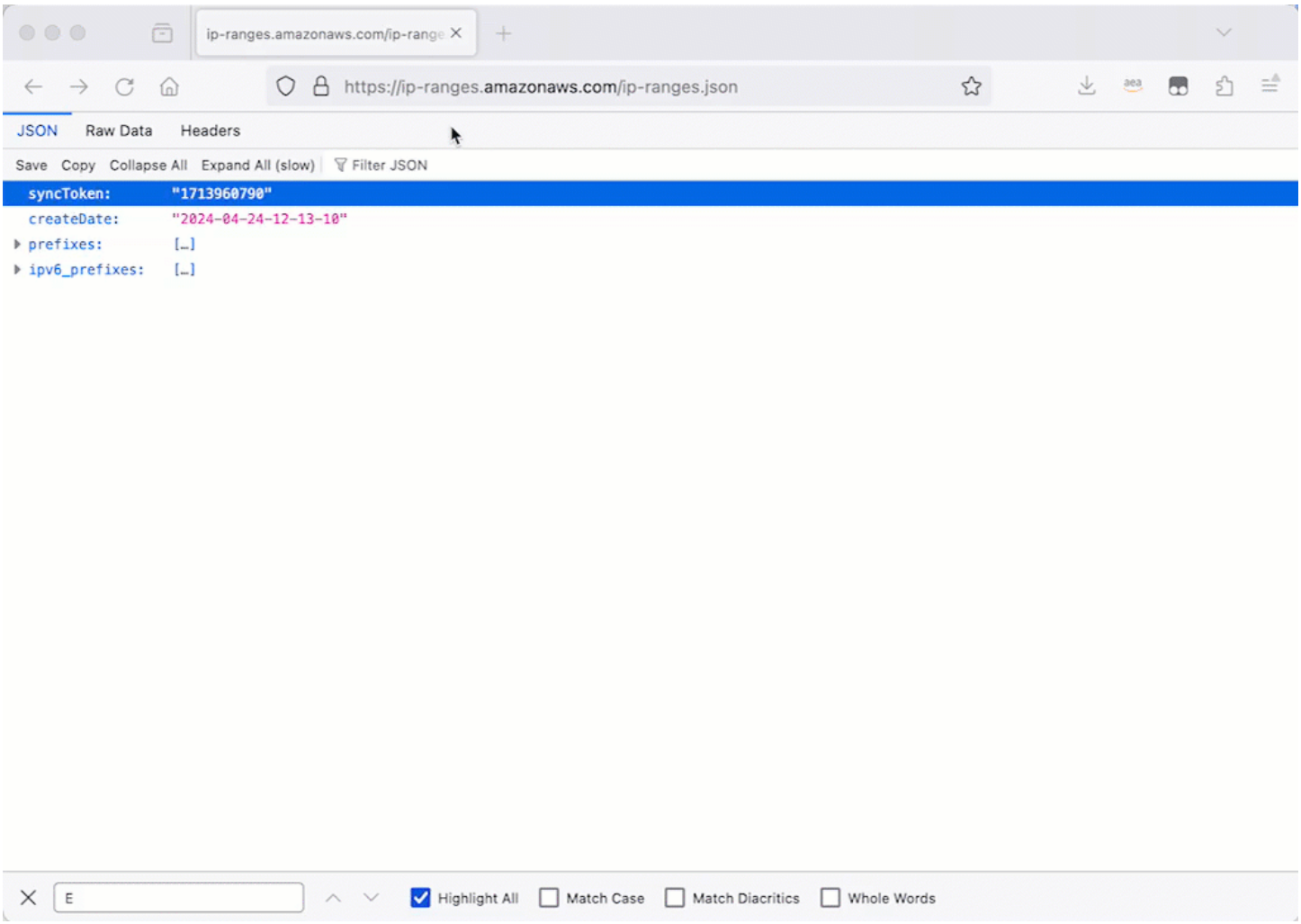
   iii. Per Source, lascia Custom.

   iv. Nel campo accanto a Source, incolla l'intervallo di indirizzi IP per il servizio EC2 Instance Connect che hai copiato in precedenza in questa procedura.

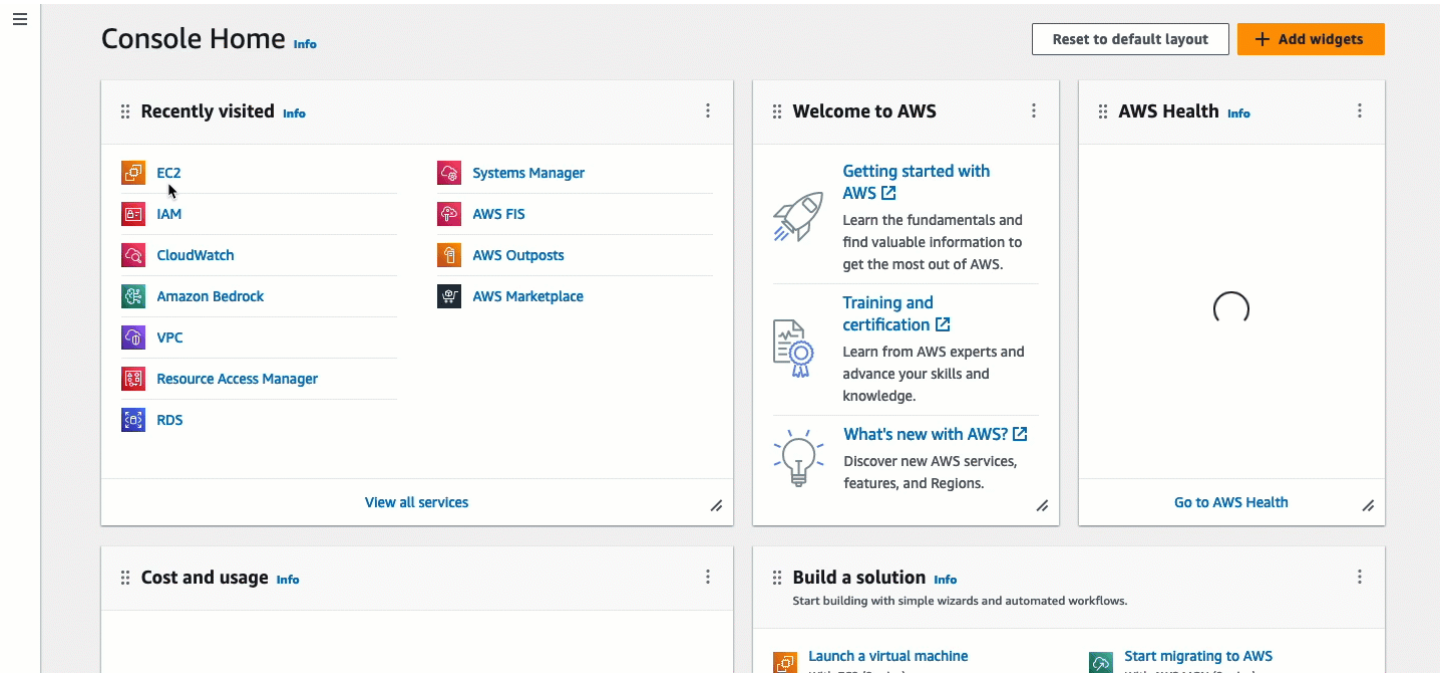
   Ad esempio, se l'istanza si trova nella regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`), incolla il seguente intervallo di indirizzi IP nel campo: `18.206.107.24/29`

f. Scegliere Create Security Group (Crea gruppo di sicurezza).

Visualizza un'animazione: ottieni l'intervallo di indirizzi IP per EC2 Instance Connect per una regione specifica



Visualizza un'animazione: configura un gruppo di sicurezza



Attività 3: Avvia l'istanza

Quando avvii un'istanza, devi specificare un AMI che contenga le informazioni necessarie per avviare l'istanza. Puoi scegliere di avviare un'istanza con o senza EC2 Instance Connect preinstallato. In questa attività, specifichiamo un'AMI preinstallata con EC2 Instance Connect.

Se avvii l'istanza senza che EC2 Instance Connect sia preinstallato e desideri utilizzare EC2 Instance Connect per connetterti alla tua istanza, dovrai eseguire passaggi di configurazione aggiuntivi. Questi passaggi non rientrano nell'ambito di questo tutorial.

Obiettivo del compito

In questa attività, lancerai un'istanza con l'AMI Amazon Linux 2023, preinstallata con EC2 Instance Connect. Specificherai anche il gruppo di sicurezza che hai creato in precedenza in modo da poter utilizzare EC2 Instance Connect nella console Amazon EC2 per connetterti alla tua istanza. Poiché utilizzerai EC2 Instance Connect per connetterti alla tua istanza, che invia una chiave pubblica ai metadati dell'istanza, non dovrai specificare una chiave SSH all'avvio dell'istanza. Tuttavia, devi assicurarti che la tua istanza abbia un indirizzo IPv4 pubblico perché l'utilizzo di EC2 Instance Connect nella console Amazon EC2 supporta la connessione solo a istanze con indirizzi IPv4 pubblici.

Passaggi per avviare l'istanza

Segui i seguenti passaggi per avviare l'istanza. Per visualizzare un'animazione dei passaggi, consultaVisualizza un'animazione: avvia la tua istanza.

Per avviare un'istanza che può utilizzare EC2 Instance Connect nella console Amazon EC2 per la connessione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore dello schermo, viene visualizzata la AWS regione corrente (ad esempio, Irlanda). Seleziona una regione in cui avviare l'istanza. Questa scelta è importante perché hai creato un gruppo di sicurezza che consente il traffico per una regione specifica, quindi devi selezionare la stessa regione in cui avviare l'istanza.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
4. (Facoltativo) in Name and tags (Nome e tag), per Name (Nome), inserire un nome descrittivo per la propria istanza.
5. In Immagini dell'applicazione e del sistema operativo (Amazon Machine Image), scegli Quick Start. Amazon Linux è selezionato per impostazione predefinita. In Amazon Machine Image (AMI), l'AMI Amazon Linux 2023 è selezionata per impostazione predefinita. Mantieni la selezione predefinita per questa attività.
6. In Tipo di istanza, per Tipo di istanza, mantieni la selezione predefinita o scegli un tipo di istanza diverso.
7. In Key pair (login), per Key pair name, scegli Procedi senza una coppia di chiavi (scelta non consigliata). Quando utilizzi EC2 Instance Connect per connetterti a un'istanza, EC2 Instance Connect invia una coppia di chiavi ai metadati dell'istanza, ed è questa coppia di chiavi che viene utilizzata per la connessione.
8. Sotto Network settings (Impostazioni di rete) effettua le seguenti operazioni:

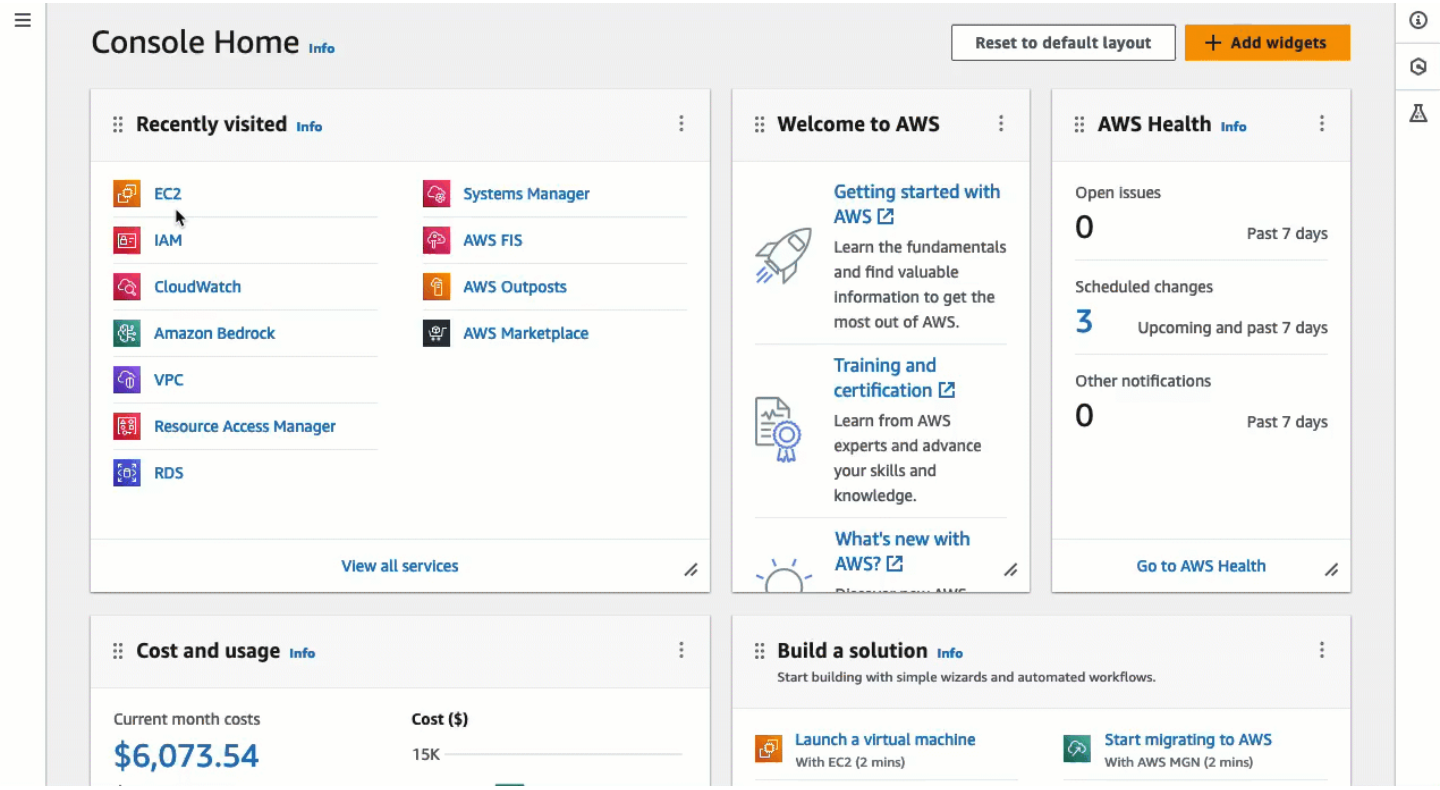
   a. Per assegnare automaticamente un IP pubblico, lascia Attiva.

   > **Note**
   >
   > Per utilizzare EC2 Instance Connect nella console Amazon EC2 per connettersi a un'istanza, l'istanza deve avere un indirizzo IPv4 pubblico.

   b. Per Firewall (gruppi di sicurezza), scegli Seleziona gruppo di sicurezza esistente.

   c. In Gruppi di sicurezza comuni, scegli il gruppo di sicurezza creato in precedenza.
9. Nel pannello Summary (Riepilogo), scegliere Launch instance (Avvia istanza).

Visualizza un'animazione: avvia la tua istanza



Attività 4: Connettiti alla tua istanza

Quando ti connetti a un'istanza tramite EC2 Instance Connect, l'API di EC2 Instance Connect invia una chiave pubblica SSH ai metadati dell'istanza, dove rimane per 60 secondi. Il demone SSH utilizza `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` cerca la chiave pubblica dai metadati dell'istanza per l'autenticazione e ti connette all'istanza.

Obiettivo del compito

In questa attività, ti connetterai alla tua istanza utilizzando EC2 Instance Connect nella console Amazon EC2. Se hai completato le attività preliminari 1, 2 e 3, la connessione dovrebbe avere successo.

Passaggi per connetterti alla tua istanza

Usa i seguenti passaggi per connetterti alla tua istanza. Per visualizzare un'animazione dei passaggi, consultaVisualizza un'animazione: Connect alla tua istanza.

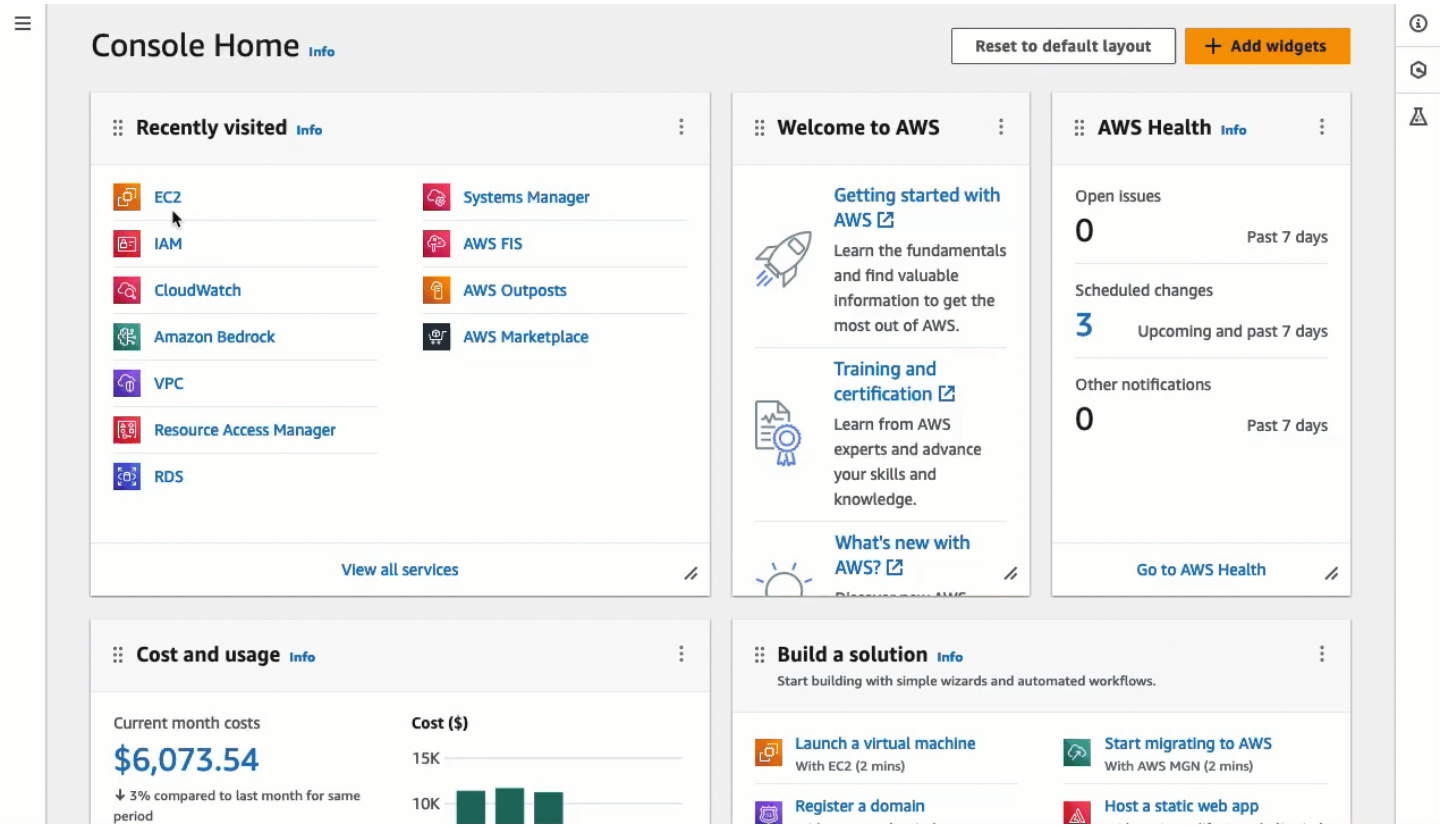
Per connettere un'istanza utilizzando EC2 Instance Connect nella console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nella barra di navigazione nella parte superiore dello schermo, viene visualizzata la AWS regione corrente (ad esempio, Irlanda). Seleziona la regione in cui si trova l'istanza.
3. Nel riquadro di navigazione, seleziona Istanze.
4. Seleziona la tua istanza e scegli Connect.
5. Scegli la scheda EC2 Instance Connect.
6. Per Tipo di connessione, scegli Connect using EC2 Instance Connect.
7. Scegli Connetti.

   Nel browser si apre una finestra di terminale e l'utente è connesso all'istanza.

Visualizza un'animazione: Connect alla tua istanza



Prerequisiti

Di seguito sono riportati i prerequisiti per installare EC2 Instance Connect e utilizzarlo per connettersi a un'istanza:

- Regioni AWS
- Zone locali

- AMI
- Installazione di EC2 Instance Connect
- Indirizzo IPv4
- Accesso alla rete
- Regola del gruppo di sicurezza
- Concessione delle autorizzazioni
- Configurazione del computer locale
- Username

Regioni AWS

Supportato in tutto Regioni AWS.

Zone locali

Non supportato.

AMI

EC2 Instance Connect è preinstallato sulle seguenti AMI:

- AL2023
- Amazon Linux 2 2.0.20190618 o versioni successive
- macOS Sonoma 14.2.1 o successivo
- macOS Ventura 13.6.3 o versioni successive
- macOS Monterey 12.7.2 o versioni successive
- Ubuntu 20.04 o versioni successive

EC2 Instance Connect non è preinstallato sulle seguenti AMI, ma è possibile installarlo su istanze avviate utilizzando le seguenti AMI:

- Amazon Linux 2 precedente alla versione 2.0.20190618
- CentOS Stream 8 e 9
- macOS Sonoma prima della 14.2.1, Ventura prima della 13.6.3 e Monterey prima della 12.7.2
- Red Hat Enterprise Linux (RHEL) 8 e 9
- Ubuntu 16.04 o 18.04

Installazione di EC2 Instance Connect

Per utilizzare EC2 Instance Connect per connettersi a un'istanza, è necessario che EC2 Instance Connect sia installato sull'istanza. Puoi avviare l'istanza utilizzando un'AMI preinstallata con EC2 Instance Connect oppure puoi installare EC2 Instance Connect su istanze avviate con AMI supportate. Per le AMI supportate, consulta la sezione precedente. Per le istruzioni di installazione, consulta Installazione di EC2 Instance Connect sulle istanze EC2.

Indirizzo IPv4

L'istanza deve disporre di un indirizzo IPv4 (privato o pubblico). EC2 Instance Connect non supporta la connessione mediante un indirizzo IPv6.

Accesso alla rete

Le istanze possono essere configurate per consentire agli utenti di connettersi all'istanza tramite Internet o tramite l'indirizzo IP privato dell'istanza. A seconda del modo in cui gli utenti si connettono all'istanza tramite EC2 Instance Connect, devi configurare il seguente accesso alla rete:

- Se gli utenti si connettono all'istanza tramite Internet, l'istanza deve avere un indirizzo IP pubblico e trovarsi in una sottorete pubblica. Per ulteriori informazioni, consulta Abilitazione dell'accesso a Internet nella Guida per l'utente di Amazon VPC.
- Se i tuoi utenti si connetteranno alla tua istanza tramite l'indirizzo IP privato dell'istanza, devi stabilire una connettività di rete privata al tuo VPC, ad esempio utilizzando o il peering VPC AWS Direct Connect AWS Site-to-Site VPN, in modo che gli utenti possano raggiungere l'indirizzo IP privato dell'istanza.

Se la tua istanza non dispone di un indirizzo IPv4 pubblico e preferisci non configurare l'accesso alla rete come descritto sopra, puoi considerare l'endpoint EC2 Instance Connect come alternativa a EC2 Instance Connect. L'endpoint EC2 Instance Connect consente di connetterti a un'istanza tramite SSH o RDP senza la necessità che l'istanza disponga di un indirizzo IPv4 pubblico. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite la console Amazon EC2.

Regola del gruppo di sicurezza

Verificare che il gruppo di sicurezza associato all'istanza consenta il traffico SSH in entrata dalla porta 22 dell'indirizzo IP o dalla rete. Per impostazione predefinita, il gruppo di sicurezza predefinito per il VPC non consente il traffico SSH in entrata. Per impostazione predefinita, il gruppo di sicurezza creato dalla procedura guidata di avvio dell'istanza abilita il traffico SSH. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.

EC2 Instance Connect utilizza intervalli di indirizzi IP specifici per le connessioni SSH all'istanza tramite browser (quando gli utenti utilizzano la console Amazon EC2 per connettersi a un'istanza). Se gli utenti utilizzano la console Amazon EC2 per connettersi a un'istanza, assicurati che il gruppo di sicurezza associato all'istanza consenta il traffico SSH in entrata dall'intervallo di indirizzi IP per `EC2_INSTANCE_CONNECT`. Per identificare l'intervallo di indirizzi, scarica il file JSON fornito da AWS e filtra il sottoinsieme per EC2 Instance Connect, utilizzandolo `EC2_INSTANCE_CONNECT` come valore del servizio. Questi intervalli di indirizzi IP differiscono tra. Regioni AWS Per ulteriori informazioni sul download del file JSON e il filtro in base al servizio, consulta Intervalli di indirizzi IP AWS nella Guida per l'utente di Amazon VPC.

Concessione delle autorizzazioni

Devi concedere le autorizzazioni richieste a tutti gli utenti IAM che utilizzano EC2 Instance Connect per connettersi a un'istanza. Per ulteriori informazioni, consulta Concessione di un'autorizzazione IAM per EC2 Instance Connect.

Configurazione del computer locale

Se gli utenti si connettono tramite SSH, devono assicurarsi che il loro computer locale disponga di un client SSH.

Il computer locale di un utente probabilmente include un client SSH installato per impostazione predefinita. Possono verificare la presenza di un client SSH digitando ssh nella linea di comando. Se il computer locale non riconosce il comando, possono installare un client SSH. Per informazioni sull'installazione di un client SSH su Linux o macOS X, consulta http://www.openssh.com. Per informazioni sull'installazione di un client SSH in Windows 10, consulta OpenSSH in Windows.

Non è necessario installare un client SSH sul computer locale se gli utenti utilizzano la console Amazon EC2 per la connessione a un'istanza.

Username

Quando si utilizza EC2 Instance Connect per connettersi a un'istanza, il nome utente deve soddisfare i seguenti prerequisiti:

- Primo carattere: deve essere una lettera (`A-Z`,`a-z`), una cifra (`0-9`) o un carattere di sottolineatura () `_`
- Caratteri successivi: possono essere lettere (`A-Z`, `a-z`), cifre (`0-9`) o i seguenti caratteri: `@ . _ -`
- Lunghezza minima: 1 carattere
- Lunghezza massima: 31 caratteri

Concessione di un'autorizzazione IAM per EC2 Instance Connect

Per connetterti all'istanza tramite EC2 Instance Connect, devi creare una policy IAM che concede agli utenti le autorizzazioni per le seguenti operazioni e condizioni:

- Operazione `ec2-instance-connect:SendSSHPublicKey`: concede l'autorizzazione per inviare la chiave pubblica a un'istanza.
- Condizione `ec2:osuser`: specifica il nome dell'utente del sistema operativo che può inviare la chiave pubblica a un'istanza. Usa il nome utente predefinito per l'AMI che hai usato per avviare l'istanza. Il nome utente predefinito per AL2023 e Amazon Linux 2 è`ec2-user`, e per Ubuntu è`ubuntu`.
- Operazione `ec2:DescribeInstances`: obbligatoria quando si utilizza la console EC2 perché il wrapper richiama questa operazione. Gli utenti potrebbero già disporre dell'autorizzazione per richiamare questa operazione da un'altra policy.

Considera la possibilità di limitare l'accesso a specifiche istanze EC2. In caso contrario, tutti i principali IAM con l'autorizzazione per l'operazione `ec2-instance-connect:SendSSHPublicKey` possono connettersi a tutte le istanze EC2. Puoi limitare l'accesso specificando gli ARN delle risorse o utilizzando i tag risorsa come chiavi di condizione.

Per ulteriori informazioni, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2 Instance Connect.

Per informazioni sulla creazione di una policy IAM, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Consentire agli utenti di connettersi a istanze specifiche

La seguente policy IAM concede l'autorizzazione per connettersi a istanze specifiche, identificate dai relativi ARN delle risorse.

Nel seguente esempio di policy IAM, vengono specificate le operazioni e le condizioni seguenti:

- L'operazione `ec2-instance-connect:SendSSHPublicKey` concede agli utenti l'autorizzazione per connettersi a due istanze, specificate dagli ARN delle risorse. Per concedere agli utenti l'autorizzazione per connettersi a tutte le istanze EC2, sostituisci gli ARN della risorsa con il carattere jolly `*`.
- La condizione `ec2:osuser` concede l'autorizzazione per connettersi alle istanze solo se *`ami-username`* è specificato durante la connessione.

- L'operazione `ec2:DescribeInstances` è specificata per concedere l'autorizzazione agli utenti che utilizzano la console per connettersi alle tue istanze. Se gli utenti utilizzano solo un client SSH per connettersi alle istanze, puoi omettere `ec2:DescribeInstances`. Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly `*` è quindi necessario nell'elemento `Resource`.

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "ec2-instance-connect:SendSSHPublicKey",
   "Resource": [
    "arn:aws:ec2:region:account-id:instance/i-1234567890abcdef0",
    "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
   ],
   "Condition": {
    "StringEquals": {
     "ec2:osuser": "ami-username"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeInstances",
   "Resource": "*"
  }
 ]
}
```

Consentire agli utenti di connettersi alle istanze con tag specifici

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base a tag che possono essere allegati a utenti e risorse. AWS Puoi utilizzare i tag delle risorse per controllare l'accesso a un'istanza. Per ulteriori informazioni sull'utilizzo dei tag per controllare l'accesso alle AWS risorse, consulta Controlling access to AWS resources nella IAM User Guide.

Nel seguente esempio di policy IAM, l'operazione `ec2-instance-connect:SendSSHPublicKey` concede agli utenti l'autorizzazione per connettersi a qualsiasi

istanza (indicata dal carattere jolly * nell'ARN della risorsa) a condizione che l'istanza abbia un tag di risorsa con key=`tag-key` e value=`tag-value`.

L'operazione `ec2:DescribeInstances` è specificata per concedere l'autorizzazione agli utenti che utilizzano la console per connettersi alle tue istanze. Se gli utenti utilizzano solo un client SSH per connettersi alle istanze, puoi omettere `ec2:DescribeInstances`. Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly * è quindi necessario nell'elemento `Resource`.

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "ec2-instance-connect:SendSSHPublicKey",
   "Resource": "arn:aws:ec2:region:account-id:instance/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/tag-key": "tag-value"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeInstances",
   "Resource": "*"
  }
 ]
}
```

Installazione di EC2 Instance Connect sulle istanze EC2

Per connettersi all'istanza tramite EC2 Instance Connect, è necessario che Instance Connect sia installato sull'istanza.

Le seguenti AMI sono preinstallate con EC2 Instance Connect:

- AMI standard AL2023
- Amazon Linux 2 2.0.20190618 o versioni successive
- macOS Sonoma 14.2.1 o successivo
- macOS Ventura 13.6.3 o versioni successive
- macOS Monterey 12.7.2 o versioni successive

- Ubuntu 20.04 o versioni successive

Se hai avviato l'istanza utilizzando una di queste AMI, puoi saltare questa procedura.

> **Note**
>
> Se hai configurato le impostazioni `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` per l'autenticazione SSH, l'installazione di EC2 Instance Connect non le aggiorna. Di conseguenza, non puoi utilizzare EC2 Instance Connect.

Prerequisiti per l'installazione di EC2 Instance Connect

- Avvia l'istanza con una delle seguenti AMI supportate:

  Amazon Linux 2 precedente alla versione 2.0.20190618

  AMI minima AL2023 o AMI ottimizzata per Amazon ECS

  CentOS Stream 8 e 9

  macOS Sonoma prima della 14.2.1, Ventura prima della 13.6.3 e Monterey prima della 12.7.2

  Red Hat Enterprise Linux (RHEL) 8 e 9

  Ubuntu 16.04 e 18.04

  Se la tua istanza è stata lanciata con una versione successiva di Amazon Linux 2, macOS Sonoma, Ventura o Monterey o Ubuntu, viene preinstallata con EC2 Instance Connect e puoi saltare questa procedura.
- Verifica i prerequisiti generali per EC2 Instance Connect.

  Per ulteriori informazioni, consulta Prerequisiti.
- Verifica i prerequisiti generali per la connessione all'istanza tramite un client SSH sul tuo computer locale.

  Se il tuo computer locale è Linux o macOS, consulta Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH.. Se il tuo computer locale è Windows, consulta Prerequisiti.

  Per ulteriori informazioni, consulta Prerequisiti per la connessione SSH.

- Ottieni l'ID dell'istanza.

  Puoi ottenere l'ID dell'istanza mediante la console Amazon EC2 (dalla colonna Instance ID [ID dell'istanza]). Se preferisci, puoi usare il comando describe-instances () o ().AWS CLIGet-EC2InstanceAWS Tools for Windows PowerShell

- Installare un client SSH sul computer locale.

  Il tuo computer locale probabilmente include un client SSH installato di default. È possibile verificare la presenza di un client SSH digitando ssh nella riga di comando. Se il computer locale non riconosce il comando, è possibile installare un client SSH. Per informazioni sull'installazione di un client SSH su Linux o macOS X, consulta http://www.openssh.com. Per informazioni sull'installazione di un client SSH in Windows 10, consulta OpenSSH in Windows.

- (Ubuntu) Installalo sulla tua istanza. AWS CLI

  Per installare EC2 Instance Connect su un'istanza di Ubuntu, è necessario utilizzare l'istanza AWS CLI sull'istanza. Per ulteriori informazioni sull'installazione di AWS CLI, consulta Installazione di AWS CLI nella Guida per l'AWS Command Line Interface utente.

Installazione di EC2 Instance Connect

Tramite l'installazione di EC2 Instance Connect, si configura il daemon SSH sull'istanza.

Segui una di queste procedure per installare EC2 Instance Connect, a seconda del sistema operativo dell'istanza.

Amazon Linux 2

Per installare EC2 Instance Connect su un'istanza avviata tramite Amazon Linux 2

1. Connettiti all'istanza tramite SSH.

   Sostituisci i valori di esempio nel seguente comando con i tuoi. Usa la coppia di chiavi SSH che è stata assegnata all'istanza al momento del lancio e il nome utente predefinito dell'AMI che hai usato per avviare l'istanza. Per Amazon Linux 2, il nome utente predefinito è`ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH..

2. Installare il pacchetto EC2 Instance Connect sull'istanza.

```
[ec2-user ~]$ sudo yum install ec2-instance-connect
```

Verranno visualizzati tre nuovi script nella cartella `/opt/aws/bin/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

3. (Opzionale) Verificare che l'installazione di EC2 Instance Connect sull'istanza sia riuscita correttamente.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config
```

EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza
- `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

CentOS

Per installare EC2 Instance Connect su un'istanza avviata tramite CentOS

1. Connettiti all'istanza tramite SSH.

   Sostituisci i valori di esempio nel seguente comando con i tuoi. Usa la coppia di chiavi SSH che è stata assegnata all'istanza al momento del lancio e il nome utente predefinito dell'AMI che hai usato per avviare l'istanza. Per CentOS, il nome utente predefinito è `centos` o. `ec2-user`

   ```
   $ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH..

2. Se si utilizza un proxy HTTP o HTTPS, è necessario impostare l'`http_proxy`o`https_proxy`nella sessione della shell corrente.

   Se non si utilizza un proxy, questa fase può essere ignorata.

   - Per un server proxy HTTP, eseguire i comandi seguenti:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Per un server proxy HTTPS, eseguire i comandi seguenti:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Installare il pacchetto EC2 Instance Connect sull'istanza eseguendo i seguenti comandi.

   I file di configurazione di EC2 Instance Connect per CentOS sono disponibili in un pacchetto Red Hat Package Manager (RPM); i pacchetti sono diversi per CentOS 8 e CentOS 9 e per i tipi di istanza eseguiti su Intel/AMD (x86_64) o ARM (AArch64).

   Utilizza il blocco di comando per il tuo sistema operativo e la tua architettura della CPU.

   - CentOS 8

Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /
tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /
tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- CentOS 9

Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Verrà visualizzato il seguente nuovo script nella cartella `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opzionale) Verificare che l'installazione di EC2 Instance Connect sull'istanza sia riuscita correttamente.

   - Per CentOS 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
     ```

   - Per CentOS 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

   - `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza

- `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

macOS

Per installare EC2 Instance Connect su un'istanza avviata tramite macOS

1. Connettiti all'istanza tramite SSH.

   Sostituisci i valori di esempio nel seguente comando con i tuoi. Usa la coppia di chiavi SSH che è stata assegnata all'istanza al momento del lancio e il nome utente predefinito dell'AMI che hai usato per avviare l'istanza. Per le istanze macOS, il nome utente predefinito è. `ec2-user`

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH..

2. Aggiornare Homebrew utilizzando il seguente comando. L'aggiornamento elencherà i software conosciuti da Homebrew. Il pacchetto EC2 Instance Connect viene fornito tramite Homebrew su istanze macOS. Per ulteriori informazioni, consulta Aggiorna il sistema operativo e il software sulle istanze Mac.

   ```
   [ec2-user ~]$ brew update
   ```

3. Installare il pacchetto EC2 Instance Connect sull'istanza. In questo modo il software verrà installato e configurato per essere utilizzato da sshd.

   ```
   [ec2-user ~]$ brew install ec2-instance-connect
   ```

Verrà visualizzato il seguente nuovo script nella cartella `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opzionale) Verificare che l'installazione di EC2 Instance Connect sull'istanza sia riuscita correttamente.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza
- `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

RHEL

Per installare EC2 Instance Connect su un'istanza avviata tramite Red Hat Enterprise Linux (RHEL)

1. Connettiti all'istanza tramite SSH.

   Sostituisci i valori di esempio nel seguente comando con i tuoi. Usa la coppia di chiavi SSH che è stata assegnata all'istanza al momento del lancio e il nome utente predefinito dell'AMI

che hai usato per avviare l'istanza. Per RHEL, il nome utente predefinito è `ec2-user` o. `root`

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH..

2. Se si utilizza un proxy HTTP o HTTPS, è necessario impostare l'`http_proxy`o`https_proxy`nella sessione della shell corrente.

   Se non si utilizza un proxy, questa fase può essere ignorata.

   - Per un server proxy HTTP, eseguire i comandi seguenti:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Per un server proxy HTTPS, eseguire i comandi seguenti:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Installare il pacchetto EC2 Instance Connect sull'istanza eseguendo i seguenti comandi.

   I file di configurazione di EC2 Instance Connect per RHEL sono disponibili in un pacchetto Red Hat Package Manager (RPM); i pacchetti sono diversi per RHEL 8 e RHEL 9 e per i tipi di istanza eseguiti su Intel/AMD (x86_64) o ARM (AArch64).

   Utilizza il blocco di comando per il tuo sistema operativo e la tua architettura della CPU.

   - RHEL 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /
     tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     ```

```
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /
tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- RHEL 9

  Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

  ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
```

```
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Verrà visualizzato il seguente nuovo script nella cartella `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opzionale) Verificare che l'installazione di EC2 Instance Connect sull'istanza sia riuscita correttamente.

   - Per RHEL 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-
     connect.conf
     ```

   - Per RHEL 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

   - `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza
   - `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

Ubuntu

Per installare EC2 Instance Connect su un'istanza avviata con Ubuntu 16.04 o versioni successive

1. Connettiti all'istanza tramite SSH.

   Sostituisci i valori di esempio nel seguente comando con i tuoi. Usa la coppia di chiavi SSH che è stata assegnata alla tua istanza al momento del lancio e usa il nome utente predefinito dell'AMI che hai usato per avviare l'istanza. Per un'AMI Ubuntu, il nome utente è`ubuntu`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH..

2. (Opzionale) Verificare che l'istanza disponga dell'AMI Ubuntu più recente.

   Eseguire i seguenti comandi per aggiornare tutti i pacchetti dell'istanza.

   ```
   ubuntu:~$ sudo apt-get update
   ```

   ```
   ubuntu:~$ sudo apt-get upgrade
   ```

3. Installare il pacchetto EC2 Instance Connect sull'istanza.

   ```
   ubuntu:~$ sudo apt-get install ec2-instance-connect
   ```

   Verranno visualizzati tre nuovi script nella cartella `/usr/share/ec2-instance-connect/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

4. (Opzionale) Verificare che l'installazione di Instance Connect sull'istanza sia riuscita correttamente.

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %
%u %%f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza
- `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

Per ulteriori informazioni sul pacchetto EC2 Instance Connect, consulta aws/aws-ec2 - sul sito Web. instance-connect-config GitHub

Connessione tramite EC2 Instance Connect

Le seguenti istruzioni illustrano come stabilire una connessione a un'istanza Linux tramite EC2 Instance Connect.

Decidi quale opzione di connessione utilizzare.L'opzione di connessione da utilizzare dipende dal fatto che l'istanza abbia un indirizzo IPv4 pubblico o meno:

- Console Amazon EC2: per la connessione tramite la console Amazon EC2, l'istanza deve disporre di un indirizzo IPv4 pubblico.
- Client SSH: se l'istanza non dispone di un indirizzo IP pubblico, puoi connetterti all'istanza su una rete privata utilizzando un client SSH. Ad esempio, è possibile connettersi dallo stesso VPC o tramite una connessione VPN, un Transit Gateway o AWS Direct Connect.

EC2 Instance Connect non supporta la connessione mediante un indirizzo IPv6.

> **Tip**
>
> EC2 Instance Connect è una delle opzioni per la connessione all'istanza Linux. Per altre opzioni, vedi Connessione all'istanza di Linux Per connetterti a un'istanza Windows, consulta. Connettiti all'istanza Windows

Opzioni di connessione per EC2 Instance Connect

- Connessione tramite la console Amazon EC2
- Connessione tramite la propria chiave e un client SSH
- Connect utilizzando AWS CLI
- Risoluzione dei problemi

Connessione tramite la console Amazon EC2

Puoi collegarti a un'istanza tramite la console Amazon EC2 selezionando l'istanza dalla console e scegliendo di collegarti tramite EC2 Instance Connect. Instance Connect gestisce le autorizzazioni e fornisce una connessione valida.

Per la connessione tramite la console Amazon EC2, l'istanza deve disporre di un indirizzo IPv4 pubblico. Prima di eseguire la connessione, assicurarsi di verificare tutti i prerequisiti.

Per connettersi all'istanza utilizzando il client basato su browser dalla console Amazon EC2

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).

3. Selezionare l'istanza, quindi scegliere Collegarsi.
4. Scegli la scheda EC2 Instance Connect.
5. Per Tipo di connessione, scegli Connect using EC2 Instance Connect.
6. Per Nome utente, verifica il nome utente.
7. Scegli Connetti per aprire una finestra del terminale.

Connessione tramite la propria chiave e un client SSH

È possibile utilizzare la propria chiave SSH e connettersi all'istanza dal client SSH preferito durante l'utilizzo dell'API EC2 Instance Connect. In questo modo è possibile sfruttare la capacità di Instance Connect di inviare una chiave pubblica all'istanza. Questo metodo di connessione funziona per istanze con indirizzi IP pubblici e privati.

Requisiti

- Requisiti delle coppie di chiavi
  - Tipi supportati: RSA (OpenSSH e SSH2) e ED25519
  - Le lunghezze supportate sono 2048 e 4096.
  - Per ulteriori informazioni, consulta Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2.
- Quando ci si connette a un'istanza che dispone solo di indirizzi IP privati, il computer locale da cui si avvia la sessione SSH deve disporre di connettività all'endpoint del servizio EC2 Instance Connect (per inviare la chiave pubblica SSH nell'istanza) nonché della connettività di rete all'indirizzo IP privato dell'istanza per stabilire la sessione SSH. L'endpoint del servizio EC2 Instance Connect è raggiungibile tramite Internet o tramite un'interfaccia virtuale pubblica AWS Direct Connect . Per connettersi all'indirizzo IP privato dell'istanza, è possibile utilizzare servizi come AWS Direct Connect, AWS Site-to-Site VPN o il peering VPC.

Prima di eseguire la connessione, assicurarsi di verificare tutti i prerequisiti.

Per connettersi all'istanza tramite la propria chiave e un client SSH

1. (Opzionale) Generazione di nuove chiavi SSH private e pubbliche

   È possibile generare nuove chiavi SSH private e pubbliche, `my_key` e `my_key.pub`, utilizzando il comando seguente:

```
ssh-keygen -t rsa -f my_key
```

2. Invio della chiave pubblica SSH all'istanza

   Utilizza il comando send-ssh-public-key per inviare la chiave pubblica SSH all'istanza. Se hai avviato l'istanza utilizzando AL2023 o Amazon Linux 2, il nome utente predefinito per l'AMI è`ec2-user`. Se hai avviato l'istanza utilizzando Ubuntu, il nome utente predefinito per l'AMI è`ubuntu`.

   L'esempio seguente invia la chiave pubblica all'istanza specificata nella zona di disponibilità specificata, per autenticare `ec2-user`.

   ```
   aws ec2-instance-connect send-ssh-public-key \
       --region us-west-2 \
       --availability-zone us-west-2b \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --instance-os-user ec2-user \
       --ssh-public-key file://my_key.pub
   ```

3. Connessione all'istanza tramite la chiave privata

   Utilizzare il comando ssh per connettersi all'istanza tramite la chiave privata prima che la chiave pubblica venga rimossa dai metadati dell'istanza (si dispone di un intervallo di tempo di 60 secondi). Specificate la chiave privata che corrisponde alla chiave pubblica, il nome utente predefinito per l'AMI che avete usato per avviare l'istanza e il nome DNS pubblico dell'istanza (se vi connettete tramite una rete privata, specificate il nome DNS privato o l'indirizzo IP). Aggiungi l'opzione `IdentitiesOnly=yes` per garantire che solo i file nella configurazione ssh e la chiave specificata vengano utilizzati per la connessione.

   ```
   ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

Connect utilizzando AWS CLI

Se conosci l'ID della tua istanza, puoi usare il AWS CLI comando ec2-instance-connect per connetterti all'istanza utilizzando un client SSH. Se non specifichi un tipo di connessione, EC2 Instance Connect tenta automaticamente di connettersi all'indirizzo IPv4 pubblico dell'istanza. Se la tua istanza non dispone di un indirizzo IPv4 pubblico, EC2 Instance Connect prova a connettersi

all'indirizzo IPv4 privato dell'istanza tramite un endpoint EC2 Instance Connect. Se la tua istanza non dispone di un indirizzo IPv4 privato o il tuo VPC non dispone di un endpoint EC2 Instance Connect, quest'ultimo tenta di connettersi all'indirizzo IPv6 dell'istanza.

> **Important**
>
> Prima di connetterti con questo metodo, assicurati di aver configurato il AWS CLI, comprese le credenziali che utilizza, e di utilizzare la versione più recente di. AWS CLI Per ulteriori informazioni, consulta Installing or updating the latest version of the AWS CLI e Configuring the AWS CLI nella Guida per l'utente dell'AWS Command Line Interface .

Tipi di connessione

`auto` (predefinito)

La CLI tenta di connettersi utilizzando gli indirizzi IP dell'istanza nel seguente ordine e con il tipo di connessione corrispondente:

- IPv4 pubblico: `direct`
- IPv4 privato: `eice`
- IPv6: `direct`

`direct`

La CLI tenta di connettersi utilizzando gli indirizzi IP dell'istanza nel seguente ordine (non si connette tramite un endpoint EC2 Instance Connect):

- IPv4 pubblico
- IPv6
- IPv4 privato

`eice`

La CLI utilizza sempre l'indirizzo IPv4 privato dell'istanza.

> **Note**
>
> In futuro, potremmo modificare il comportamento del tipo di connessione `auto`. Per assicurarti che venga utilizzato il tipo di connessione desiderato, consigliamo di impostare esplicitamente il `--connection-type` su `direct` o `eice`.

Quando ti connetti a un'istanza tramite EC2 Instance Connect, l'API di EC2 Instance Connect invia una chiave pubblica SSH ai metadati dell'istanza, dove rimane per 60 secondi. Una policy IAM collegata al tuo utente autorizza quest'ultimo a inserire la chiave pubblica tra i metadati dell'istanza.

Per la connessione un'istanza tramite l'ID istanza

Se conosci solo l'ID dell'istanza e desideri lasciare che EC2 Instance Connect determini il tipo di connessione da utilizzare per la connessione alla tua istanza, usa il comando CLI ec2-instance-connect e specifica il parametro e l'ID dell'istanza. `ssh`

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

> **Tip**
>
> Se ricevi un errore durante l'utilizzo di questo comando, assicurati di utilizzare la versione 2. AWS CLI Il `ssh` parametro è disponibile solo nella AWS CLI versione 2. Per ulteriori informazioni, vedere Informazioni sulla AWS CLI versione 2 nella Guida AWS Command Line Interface per l'utente.

Per la connessione all'istanza tramite l'ID istanza e un endpoint EC2 Instance Connect

Se desideri connetterti all'istanza tramite un endpoint EC2 Instance Connect, utilizza il comando precedente e specifica anche il parametro `--connection-type` con il valore `eice`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

Per la connessione a un'istanza utilizzando l'ID istanza e il proprio file di chiave privata

Se desideri connetterti alla tua istanza tramite un endpoint EC2 Instance Connect utilizzando la tua chiave privata, specifica l'ID istanza e il percorso del file della chiave privata. Non includere *`file://`* nel percorso; l'esempio seguente genererà un errore: *`file:///path/to/key`*.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /
path/to/key.pem
```

Risoluzione dei problemi

Se ricevi un errore mentre tenti di connetterti all'istanza, consulta l'argomento seguente:

- Risolvi i problemi di connessione alla tua istanza Linux
- In che modo posso risolvere i problemi di connessione alla mia istanza EC2 utilizzando EC2 Instance Connect?

Disinstallazione di EC2 Instance Connect

Per disabilitare EC2 Instance Connect, connettiti all'istanza e disinstalla il pacchetto `ec2-instance-connect` installato sul sistema operativo. Se la configurazione di `sshd` corrisponde a quella impostata al momento dell'installazione di EC2 Instance Connect, la disinstallazione di `ec2-instance-connect` rimuove anche la configurazione di `sshd`. Se la configurazione di `sshd` è stata modificata dopo l'installazione di EC2 Instance Connect, è necessario eseguire manualmente l'aggiornamento.

Amazon Linux

Puoi disinstallare EC2 Instance Connect su AL2023 e Amazon Linux 2 versione 2.0.20190618 o successiva, dove EC2 Instance Connect è preconfigurata.

Per disinstallare EC2 Instance Connect su un'istanza avviata tramite Amazon Linux 2

1. Connettiti all'istanza tramite SSH. Specificate la coppia di chiavi SSH che avete usato per l'istanza al momento del lancio e il nome utente predefinito per l'AMI AL2023 o Amazon Linux 2, che è. `ec2-user`

   Ad esempio, il comando ssh seguente si connette all'istanza con il nome DNS pubblico `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, utilizzando la coppia di chiavi `my_ec2_private_key.pem`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Disinstallare il pacchetto `ec2-instance-connect` utilizzando il comando yum.

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

Ubuntu

Per disinstallare EC2 Instance Connect su un'istanza avviata tramite un'AMI Ubuntu

1. Connettiti all'istanza tramite SSH. Specificate la coppia di chiavi SSH che avete usato per l'istanza al momento del lancio e il nome utente predefinito per l'AMI Ubuntu, che è`ubuntu`.

   Ad esempio, il comando ssh seguente si connette all'istanza con il nome DNS pubblico `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, utilizzando la coppia di chiavi `my_ec2_private_key.pem`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Disinstallare il pacchetto `ec2-instance-connect` utilizzando il comando apt-get.

   ```
   ubuntu:~$ sudo apt-get remove ec2-instance-connect
   ```

Connettiti all'istanza Windows

È possibile connettersi alle istanze Amazon EC2 create dalla maggior parte delle Amazon Machine Image (AMI) per Windows tramite Desktop remoto. Desktop remoto utilizza il protocollo RDP (Remote Desktop Protocol) per connettersi e utilizzare l'istanza con le stesse procedure usate per un computer vero e proprio. È disponibile per la maggior parte delle versioni di Windows e anche per Mac OS.

La licenza per il sistema operativo di Windows Server consente due connessioni remote simultanee per attività amministrative. Il costo della licenza per Windows Server è incluso nel costo della tua istanza Windows. Se servono più di due connessioni remote simultanee, devi acquistare una licenza di Remote Desktop Services (RDS). Se tenti di stabilire una terza connessione, si verifica un errore.

> **Tip**
>
> Se è necessario collegarsi alla tua istanza per risolvere problemi di avvio, configurazione di rete e altri problemi per le istanze basate su AWS Nitro System, puoi utilizzare Console seriale EC2 per istanze Amazon EC2.

Indice

Connect alla tua istanza Windows utilizzando un client RDP

La sezione seguente descrive i prerequisiti e il processo per connettersi all'istanza utilizzando l'indirizzo IPv4 o IPv6 con un client RDP.

Prerequisiti

È necessario soddisfare i seguenti prerequisiti per connettersi all'istanza di Windows utilizzando un client RDP.

- Installare un client RDP
  - (Windows) Windows include un client RDP per impostazione predefinita. Per verificare, digitare mstsc nella finestra del prompt dei comandi. Se il computer in uso non riconosce questo comando, consultare la home page di Windows e cercare il download per l'app Desktop remoto Microsoft.
  - (macOS X) Scarica l'app Microsoft Remote Desktop dal Mac App Store.
  - (Linux) Usa Remmina.
- Individuazione della la chiave privata

  Ottieni il percorso pienamente qualificato alla posizione nel tuo computer del file `.pem` per una coppia di chiavi che hai specificato quando hai avviato l'istanza. Per ulteriori informazioni, consulta the section called “Identificazione della chiave pubblica specificata al momento dell'avvio”.

  Se non riesci a trovare il file della tua chiave privata, vedi

Quando ci si connette a un'istanza di Windows appena avviata, decodificare la password per l'account amministratore utilizzando la chiave privata per la coppia di chiavi specificata all'avvio dell'istanza.

Se si perde la password dell'amministratore e non si dispone più della chiave privata, è necessario reimpostare la password o creare una nuova istanza. Per ulteriori informazioni, consulta Reimpostazione di una password amministratore Windows persa o scaduta. Per la procedura di reimpostazione della password utilizzando un documento Systems Manager, consulta Reimpostazione di password e chiavi SSH sulle istanze EC2 nella Guida per l'utente di AWS Systems Manager .

- Abilitare il traffico RDP in entrata dall'indirizzo IP all'istanza

  Verifica che il gruppo di sicurezza associato alla tua istanza consenta il traffico RDP (`port 3389`) in entrata dal tuo indirizzo IP. Per impostazione predefinita, il gruppo di sicurezza predefinito non consente il traffico RDP in entrata. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.

> **Tip**
>
> Puoi creare un endpoint EC2 Instance Connect per connetterti alla tua istanza Windows utilizzando RDP senza un indirizzo IPv4 pubblico.

Connect a un'istanza Windows utilizzando RDP e il relativo indirizzo IPv4

Per connetterti a un'istanza Windows, devi recuperare la password di amministratore iniziale e utilizzarla quando ti connetti all'istanza tramite Remote Desktop. Dopo l'avvio dell'istanza, dovrai attendere alcuni minuti prima che la password sia disponibile.

Il nome utente predefinito per l'account Administrator dipende dalla lingua del sistema operativo (OS) contenuto nell'AMI. Per verificare il nome utente corretto, identifica la lingua del sistema operativo dell'AMI, quindi scegli il nome utente corrispondente. Ad esempio, per un sistema operativo inglese, il nome utente è`Administrator`, per un sistema operativo francese è `Administrateur` e per un sistema operativo portoghese è`Administrador`. Se una versione linguistica del sistema operativo non ha un nome utente nella stessa lingua, scegli il nome utente`Administrator (Other)`. Per ulteriori informazioni, vedere Nomi localizzati per l'account amministratore in Windows in Microsoft TechNet Wiki.

Se l'istanza è stata aggiunta a un dominio, è possibile connettersi all'istanza utilizzando le credenziali di dominio definite in AWS Directory Service. Nella schermata di accesso a Desktop remoto, anziché utilizzare il nome del computer locale e la password generata, utilizzare il nome utente completo per l'amministratore (ad esempio, **`corp.example.com\Admin`**) e la password per questo account.

Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta the section called “Il desktop remoto non può connettersi al computer remoto”.

Per connetterti alla tua istanza Windows utilizzando un client RDP

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza quindi scegli Connect (Connetti).
4. Nella pagina Connect to instance, scegli la scheda Client RDP.
5. Per Nome utente, scegli il nome utente predefinito per l'account amministratore. Il nome utente scelto deve corrispondere alla lingua del sistema operativo (OS) contenuto nell'AMI che hai usato per avviare l'istanza. Se non esiste un nome utente nella stessa lingua del sistema operativo, scegli Amministratore (Altro).
6. Scegli Ottieni password.
7. Nella pagina Ottieni la password di Windows, procedi come segue:

    a. Scegli Carica file di chiave privata e vai al file di chiave privata (`.pem`) che hai specificato all'avvio dell'istanza. Selezionare il file e scegliere Open (Apri) per copiare l'intero contenuto del file in questa finestra.

    b. Scegli Decrittografa la password. La pagina Ottieni la password di Windows si chiude e la password di amministratore predefinita per l'istanza viene visualizzata in Password, sostituendo il collegamento Ottieni password mostrato in precedenza.

    c. Copia la password e salvala in un posto sicuro. Questa password ti servirà per connetterti all'istanza.
8. Seleziona Download remote desktop file (Scarica file per desktop remoto). Al termine del download del file, scegli Cancel (Annulla) per tornare alla pagina Instances (Istanze). Vai alla directory dei download e apri il file RDP.
9. Potrebbe essere visualizzato un avviso che informa che l'identità di chi ha pubblicato la connessione remota non è nota. Scegli Connect (Connetti) per collegarti all'istanza.
10. Per impostazione predefinita è selezionato l'account amministratore. Incolla la password che hai copiato in precedenza, quindi scegli OK.

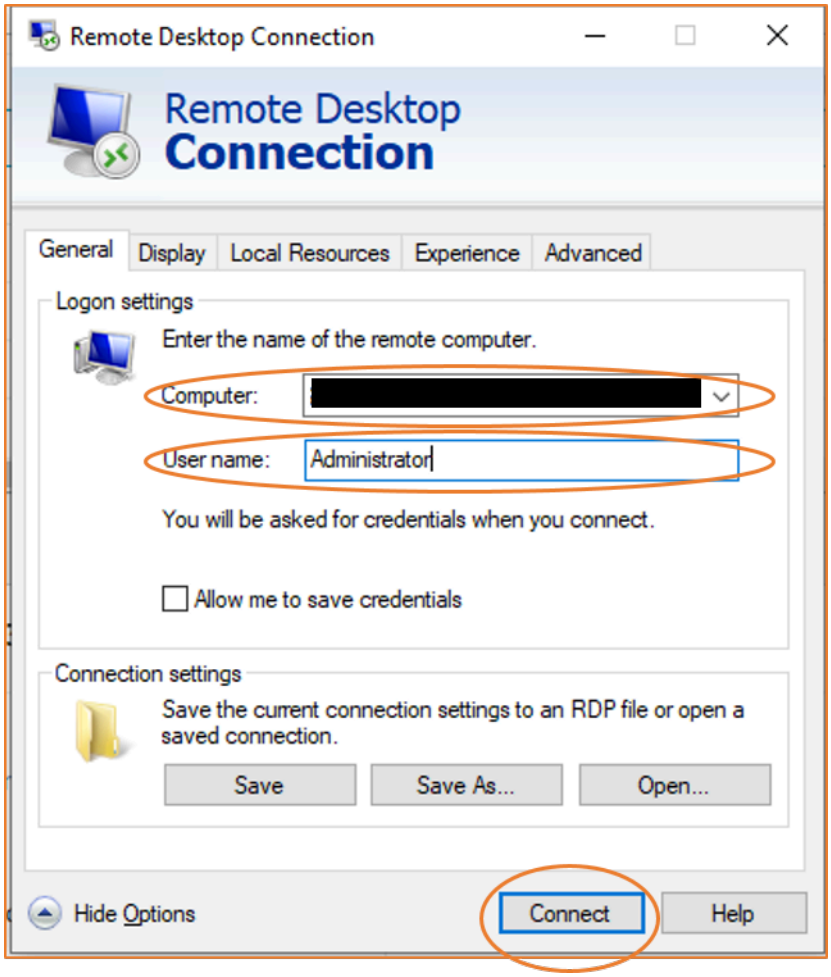
11. Data la natura dei certificati autofirmati, è possibile che venga visualizzato un avviso relativo all'impossibilità di autenticare il certificato di sicurezza. Esegui una di queste operazioni:
    - Se ritieni attendibile il certificato, scegli Sì per connetterti alla tua istanza.
    - [Windows] Prima di procedere, confronta l'impronta digitale del certificato con il valore nel registro di sistema per confermare l'identità del computer remoto. Scegli Visualizza certificato, quindi scegli Thumbprint dalla scheda Dettagli. Confronta questo valore con quello di **`RDPCERTIFICATE-THUMBPRINT`** Azioni, Monitoraggio e risoluzione dei problemi, Get system log.
    - [Mac OS X] Prima di procedere, confronta l'impronta digitale del certificato con il valore nel registro di sistema per confermare l'identità del computer remoto. Scegliete Mostra certificato, espandete Dettagli e scegliete SHA1 Fingerprints. Confronta questo valore con il valore di **`RDPCERTIFICATE-THUMBPRINT`** in Azioni, Monitor e risoluzione dei problemi, Get system log.

Connect a un'istanza Windows utilizzando RDP e il relativo indirizzo IPv6

Se hai abilitato il VPC per IPv6 e hai assegnato un indirizzo IPv6 all'istanza Windows, puoi utilizzare un client RDP per connetterti all'istanza utilizzando il relativo indirizzo IPv6 (ad esempio, `2001:db8:1234:1a00:9691:9503:25ad:1761`) anziché un indirizzo IPv4 pubblico o un nome host DNS pubblico.

Per connettersi a un'istanza Windows tramite il relativo indirizzo IPv6

1. Ottenere la password di amministratore iniziale per l'istanza, come descritto in Connect alla tua istanza Windows utilizzando un client RDP. Questa password è necessaria per effettuare la connessione all'istanza.
2. (Windows) Aprite il client RDP sul computer Windows, scegliete Mostra opzioni ed effettuate le seguenti operazioni:



- Per Computer, immettere l'indirizzo IPv6 dell'istanza Windows.
- Per User Name (Nome utente), immettere Administrator (Amministratore).
- Scegliere Connetti.
- Quando richiesto, immettere la password salvata in precedenza.

(macOS X) Apri il client RDP sul tuo computer ed esegui le seguenti operazioni:

- Scegli New (Nuovo).
- Per PC Name (Nome PC), immettere l'indirizzo IPv6 dell'istanza Windows.
- Per User Name (Nome utente), immettere Administrator (Amministratore).
- Chiudere la finestra di dialogo. In My Desktops (Desktop personali), selezionare la connessione, quindi scegliere Start (Avvia).
- Quando richiesto, immettere la password salvata in precedenza.

3. Data la natura dei certificati autofirmati, è possibile che venga visualizzato un avviso relativo all'impossibilità di autenticare il certificato di sicurezza. Se si considera attendibile il certificato, è possibile scegliere Yes (Sì) o Continue (Continua). In caso contrario, è possibile verificare l'identità del computer remoto, come descritto in Connect alla tua istanza Windows utilizzando un client RDP.

Connessione a un'istanza Windows utilizzando Fleet Manager

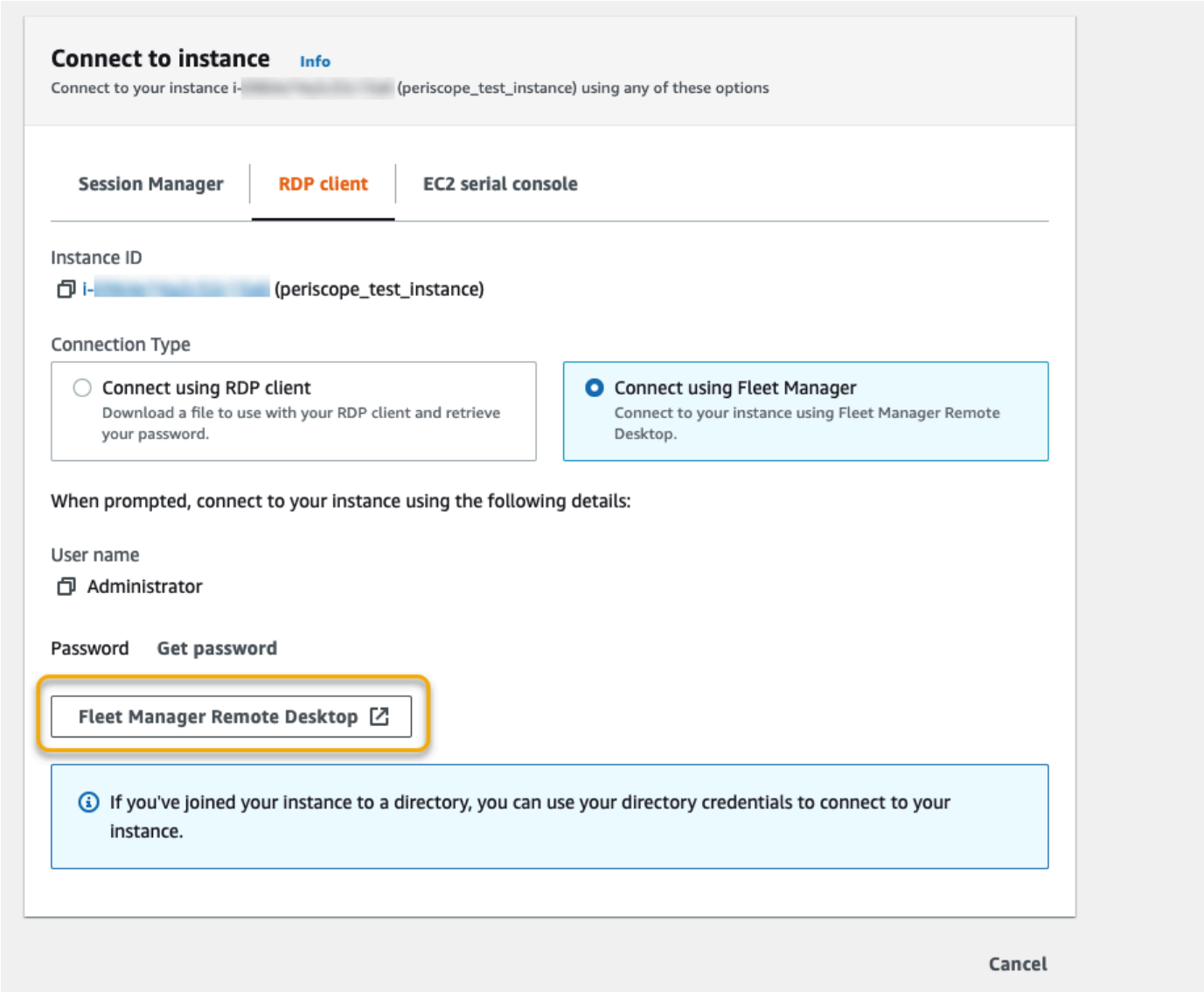
È possibile utilizzare Fleet Manager, una funzionalità di AWS Systems Manager, per connettersi a istanze Windows utilizzando il Remote Desktop Protocol (RDP) e visualizzare fino a quattro istanze di Windows sulla stessa pagina di. AWS Management Console Puoi connetterti alla prima istanza nel desktop remoto della Gestione dei gruppi di nodi direttamente dalla pagina Istanze nella console Amazon EC2. Per ulteriori informazioni sulla Gestione dei gruppi di nodi, consulta la pagina Connessione a un nodo gestito tramite desktop remoto nella Guida per l'utente di AWS Systems Manager .

Prima di tentare di connetterti a un'istanza utilizzando la Gestione dei gruppi di nodi, assicurati che i passaggi di configurazione necessari siano stati completati. Per ulteriori informazioni, consulta la pagina Configurazione della Gestione dei gruppi di nodi.

> **Note**
>
> Nello specifico, non è necessario che tu consenta il traffico RDP in entrata dal tuo indirizzo IP, se utilizzi Fleet Manager per la connessione. Fleet Manager lo gestisce al posto tuo.

Per connetterti alle istanze utilizzando RDP con Fleet Manager (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Instances (Istanze).
3. Seleziona l'istanza quindi scegli Connect (Connetti).
4. Nella pagina Connect to instance (Connettiti all'istanza), scegli l'opzione Connect using Fleet Manager (Connettiti tramite Fleet Manager), quindi scegli Fleet Manager Remote Desktop. Si apre la pagina Fleet Manager Remote Desktop nella console AWS Systems Manager .



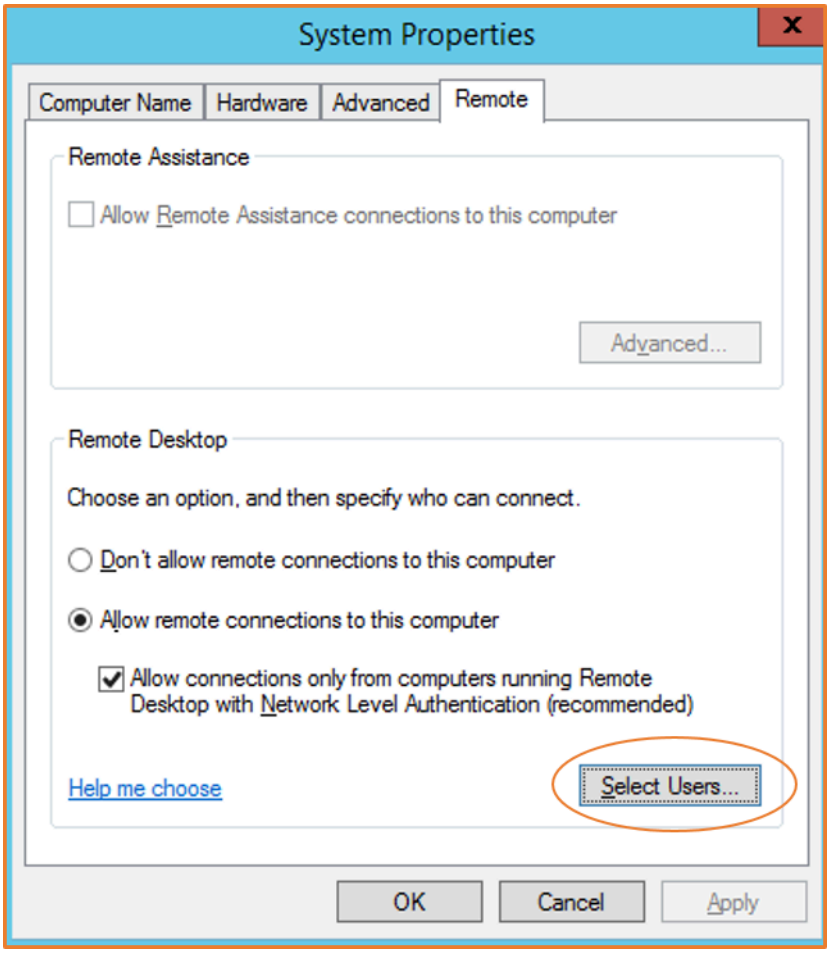
Per ulteriori informazioni sulla connessione alle istanze Windows dalla pagina Fleet Manager Remote Desktop, vedi Connessione tramite desktop remoto nella Guida per l'utente di AWS Systems Manager .

Configurazione degli account

Dopo la connessione tramite RDP, si consiglia di eseguire le seguenti operazioni:

- Modificare la password dell'amministratore rispetto al valore di default. Modificare la password mentre si è connessi all'istanza, usando le stesse procedure valide per qualsiasi computer che esegua Windows Server.

- Crea un altro utente con privilegi di amministratore sull'istanza. Questo rappresenta una garanzia se ci si dimentica la password dell'amministratore o se si verifica un problema a livello di account dell'amministratore. Il nuovo account deve essere autorizzato ad accedere all'istanza da remoto. Aprire System Properties (Proprietà di sistema) facendo clic con il tasto destro sull'icona Questo PC sul desktop Windows o su File Explorer e selezionare Properties (Proprietà). Scegliere Remote settings (Impostazioni remote), quindi Select Users (Seleziona utenti) per aggiungere l'utente al gruppo Utenti desktop remoti.



Trasferimento di file alle istanze Windows

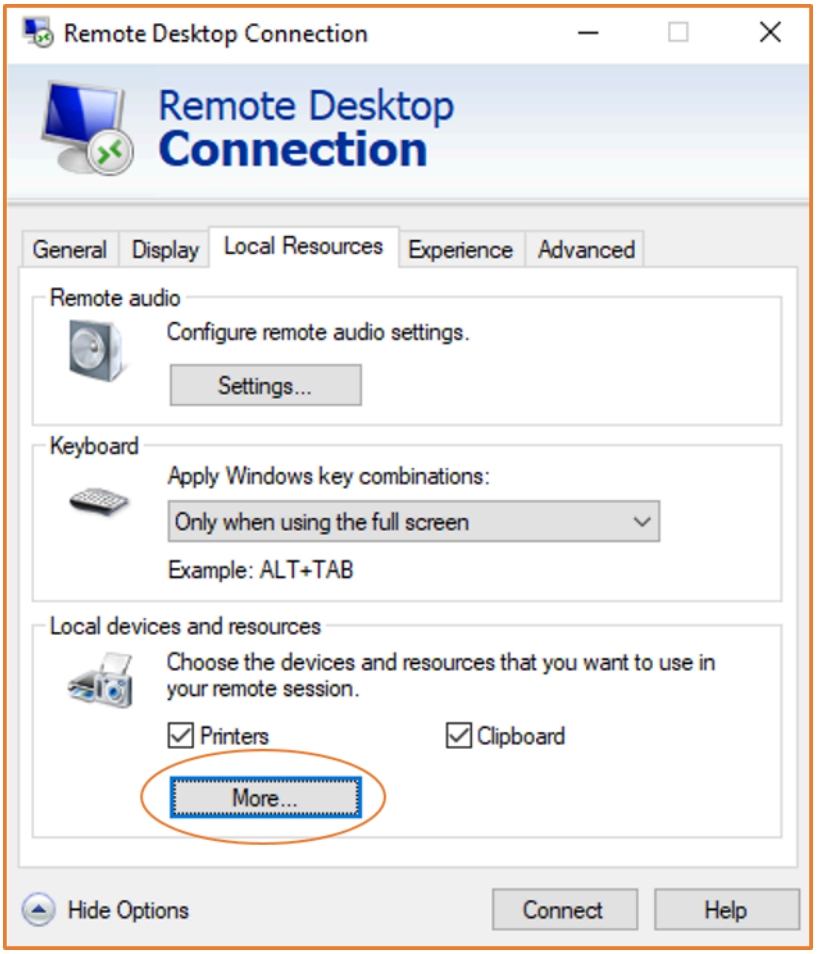
Puoi usare l'istanza Windows con le stesse procedure valide per qualsiasi server Windows. Ad esempio, è possibile trasferire file tra un'istanza di Windows e il computer locale utilizzando la funzionalità di condivisione file locale del software Microsoft Remote Desktop Connection (RDP). Puoi accedere ai file locali su unità disco rigido (HDD), unità DVD, unità audio/video portatili e unità di rete mappate.

Per accedere ai file locali dalle istanze di Windows, devi abilitare la caratteristica di condivisione file locale mappando l'unità di sessione remota sull'unità locale. I passaggi sono leggermente diversi, a seconda che il sistema operativo del computer locale sia Windows o macOS X.

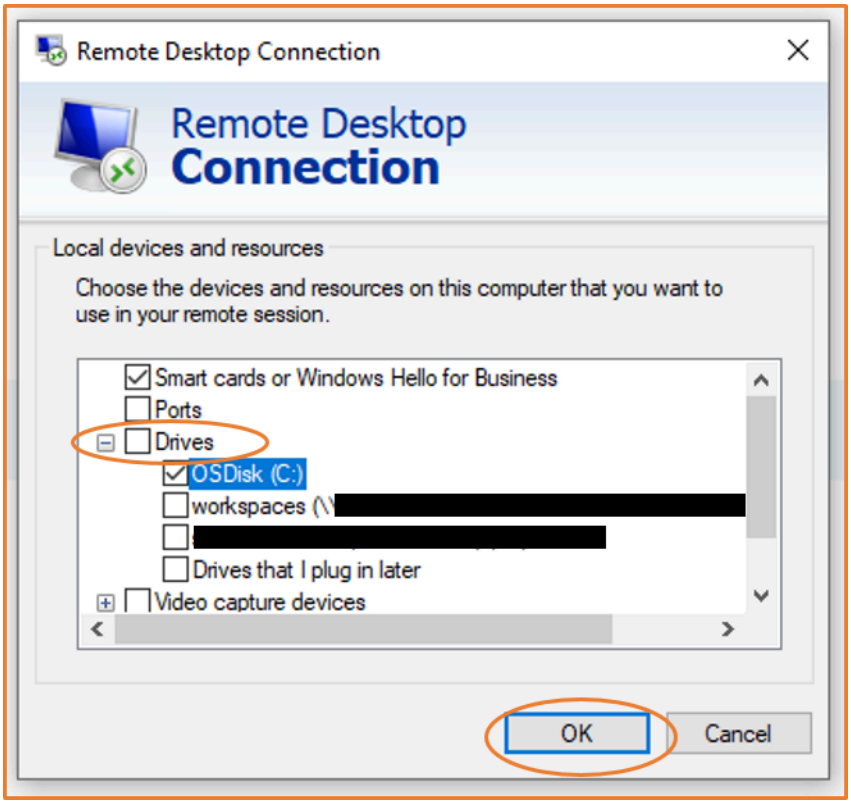
Windows

Per mappare l'unità di sessione remota all'unità locale sul computer Windows locale

1. Apri il client di connessione remota desktop.
2. Scegliere Show options (Mostra opzioni).
3. Aggiungi il nome host dell'istanza al campo Computer e il nome utente per al campo User name (Nome utente), come riportato di seguito:
    a. Nella sezione Connection settings (Impostazioni connessione), scegli Open... (Apri...) e passa al file di collegamento RDP scaricato dalla console Amazon EC2. Il file contiene il nome host DNS IPv4 pubblico, che identifica l'istanza e il nome utente dell'amministratore.
    b. Scegli il file e seleziona Open (Apri). I campi Computer e User name (Nome utente) vengono compilati con i valori del file di collegamento RDP.
    c. Selezionare Salva.
4. Scegliere la scheda Local Resources (Risorse locali).
5. In Local Devices and resources (Dispositivi e risorse locali), scegli More... (Altro...).



6. Apri Drives (Unità) e seleziona l'unità locale per mappare la tua istanza di Windows.
7. Seleziona OK.

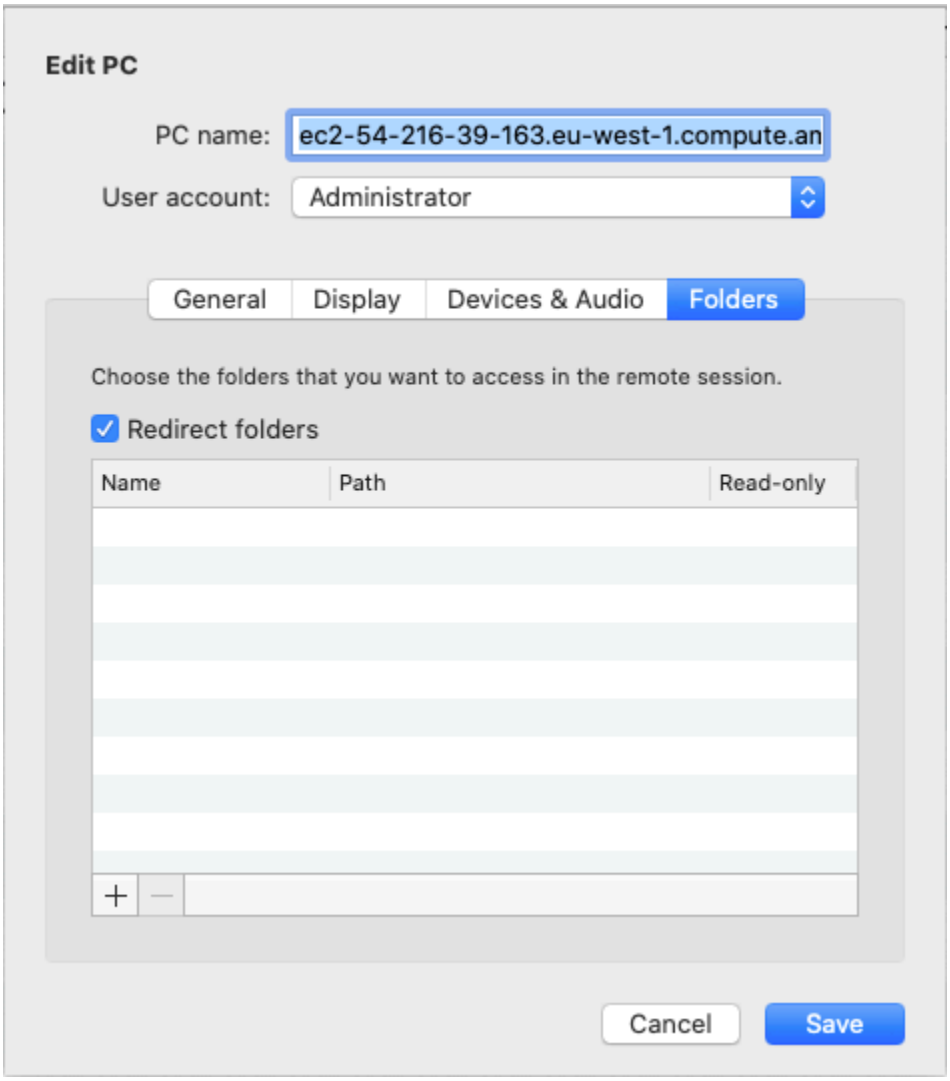


8. Scegli Connect (Connetti) per collegarti all'istanza di Windows.

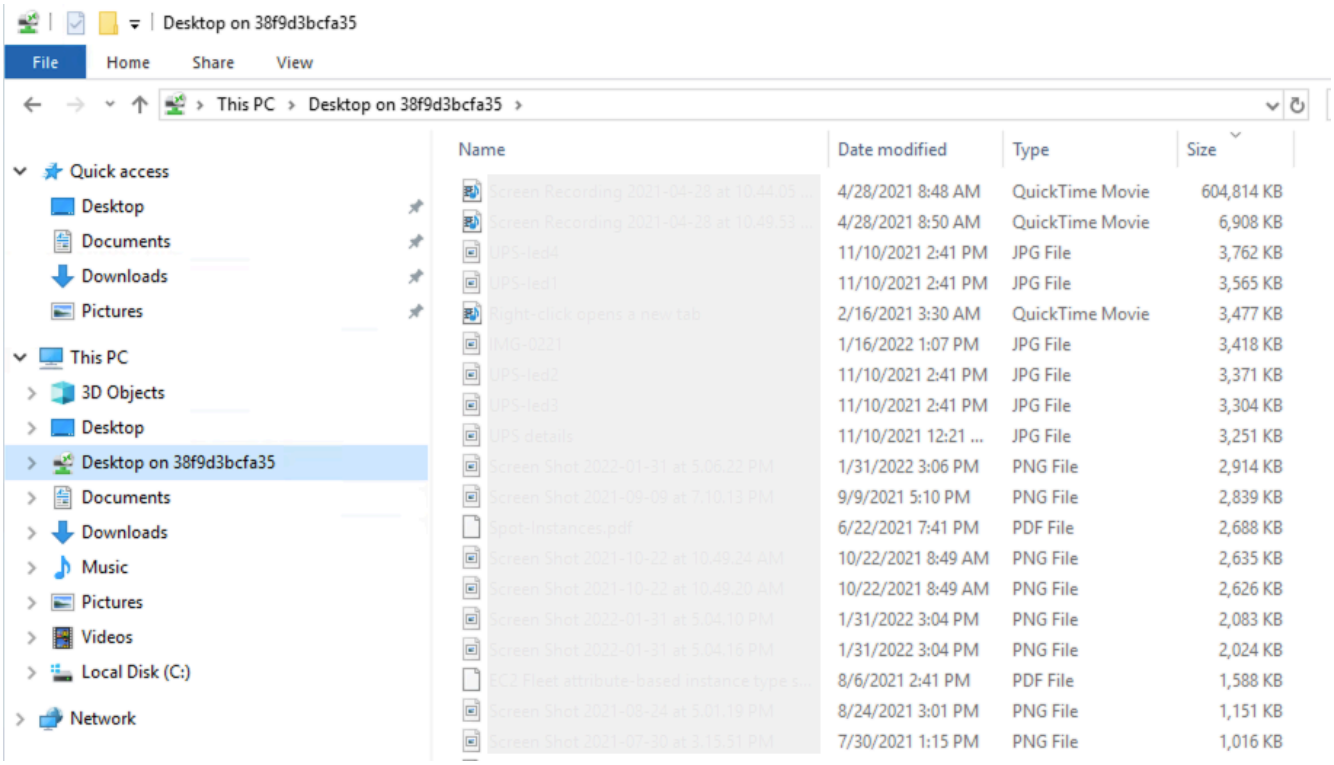
macOS X

Per mappare l'unità di sessione remota alla cartella locale sul computer macOS X locale

1. Apri il client di connessione remota desktop.
2. Individua il file RDP scaricato dalla console Amazon EC2 (quando ti sei connesso inizialmente all'istanza) e trascinalo sul client di Connessione Desktop remoto.
3. Fai clic con il pulsante destro del mouse sul file RDP e scegli Edit (Modifica).
4. Seleziona la scheda Folders (Cartelle) e poi la casella di controllo Redirect folders (Reindirizza cartelle).



5. Seleziona l'icona + in basso a sinistra, vai alla cartella da mappare e scegli Open (Apri). Ripeti questo passaggio per eseguire la mappatura di ogni cartella da mappare.
6. Selezionare Salva.
7. Scegli Connect (Connetti) per collegarti all'istanza di Windows. Ti verrà richiesta la password.
8. Nell'istanza, in Esplora file espandi This PC (Questo PC) e cerca la cartella condivisa da cui puoi accedere ai file locali. Nello screenshot seguente, la cartella Desktop del computer locale è stata mappata all'unità di sessione remota sull'istanza.



Per ulteriori informazioni su come rendere disponibili i dispositivi locali per una sessione remota su un computer Mac, consulta Get started with the macOS client (Nozioni di base sul client macOS).

Connessione tramite Session Manager

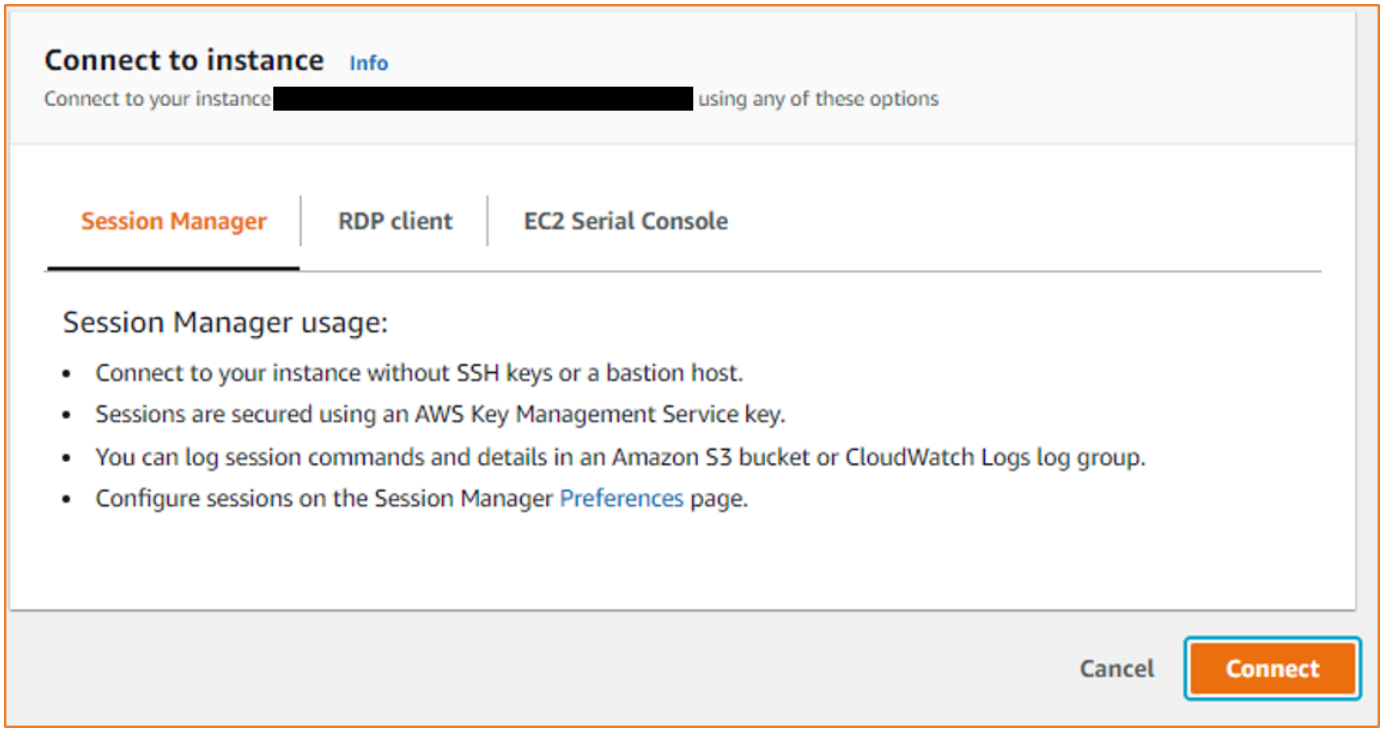
Session Manager è una AWS Systems Manager funzionalità completamente gestita per la gestione delle istanze Amazon EC2 tramite una shell interattiva basata su browser con un solo clic o tramite. AWS CLI Puoi utilizzare Session Manager per avviare una sessione con un'istanza nel tuo account. Dopo l'avvio della sessione, puoi eseguire comandi interattivi sull'istanza come faresti per qualsiasi altro tipo di connessione. Per ulteriori informazioni su Session Manager, consulta AWS Systems Manager Session Manager nella Guida per l'utente di AWS Systems Manager .

Prima di tentare di connetterti a un'istanza utilizzando Session Manager, assicurati che i passaggi di installazione necessari siano stati completati. Per ulteriori informazioni e istruzioni, consulta Setting up Session Manager (Impostazione di Session Manager).

Per connettersi a un'istanza Amazon EC2 utilizzando Session Manager sulla console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).

3. Selezionare l'istanza, quindi scegliere Collegarsi.
4. Per Connection method (Metodo di connessione), selezionare Session Manager.
5. Scegliere Connetti.



> **Tip**
>
> Se viene visualizzato un errore che non si è autorizzati a eseguire una o più operazioni Systems Manager (`ssm:command-name`), è necessario aggiornare le policy per consentire l'avvio delle sessioni dalla console Amazon EC2. Per ulteriori informazioni e istruzioni, consulta Guida rapida sulle policy IAM predefinite per Session Manager nella Guida per l'utente di AWS Systems Manager .

Connettiti alle tue istanze utilizzando EC2 Instance Connect Endpoint

EC2 Instance Connect Endpoint ti consente di connetterti in modo sicuro a un'istanza da Internet, senza utilizzare un bastion host o richiedere che il tuo cloud privato virtuale (VPC) disponga di una connettività Internet diretta.

Vantaggi

- Puoi connetterti alle tue istanze senza richiedere che le istanze abbiano un indirizzo IPv4 pubblico. AWS costi per tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.
- Puoi connetterti alle tue istanze da Internet senza richiedere che il tuo VPC disponga di una connettività Internet diretta tramite un gateway Internet.
- Puoi controllare l'accesso alla creazione e all'uso degli endpoint EC2 Instance Connect per connetterti alle istanze utilizzando le policy e le autorizzazioni IAM.
- Tutti i tentativi di connessione alle istanze, riusciti o meno, vengono registrati in. CloudTrail

Prezzi

Non sono previsti costi aggiuntivi per l'utilizzo degli endpoint EC2 Instance Connect. Se utilizzi un endpoint EC2 Instance Connect per connetterti a un'istanza in una zona di disponibilità diversa, è previsto un costo aggiuntivo per il trasferimento dei dati tra le zone di disponibilità.

Indice

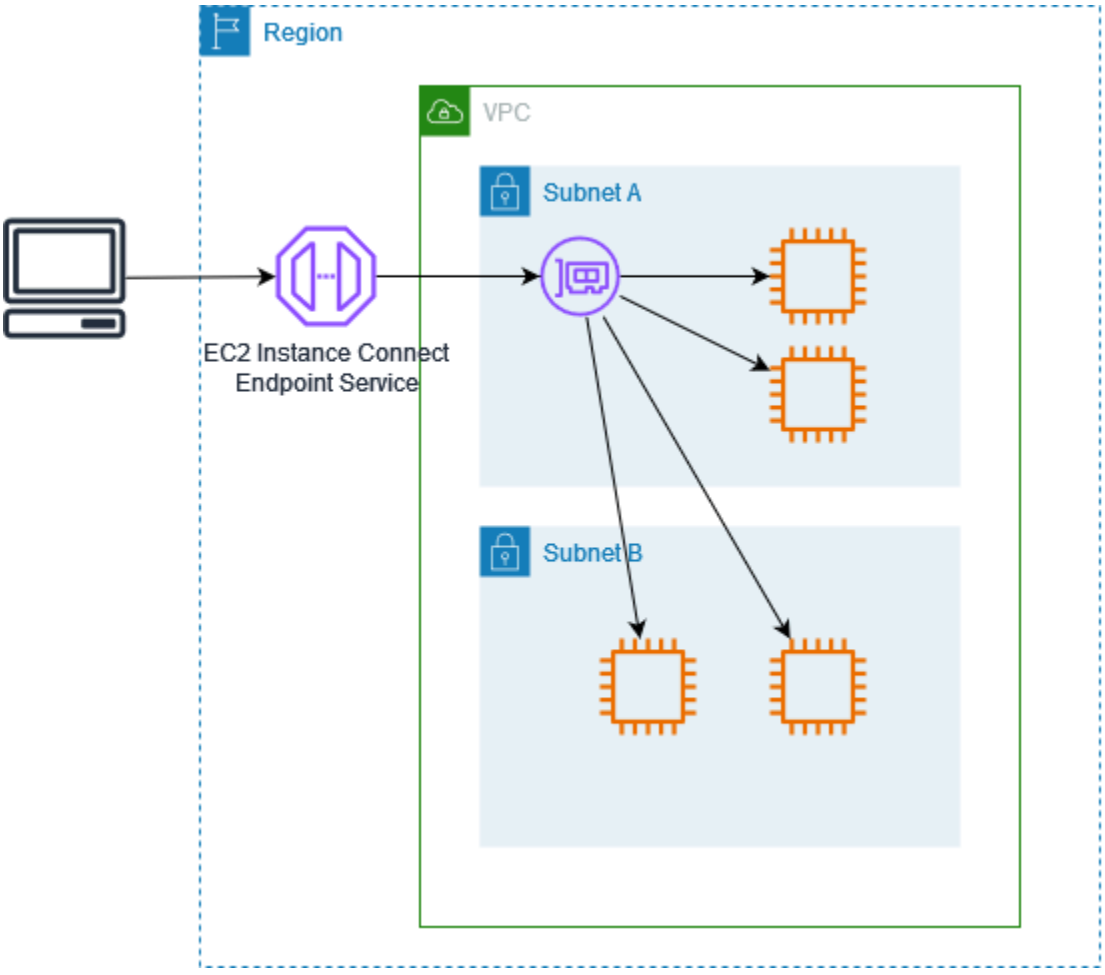
Come funziona

EC2 Instance Connect Endpoint è un proxy TCP con riconoscimento dell'identità. L'EC2 Instance Connect Endpoint Service stabilisce un tunnel privato dal computer all'endpoint utilizzando le credenziali per l'entità IAM. Il traffico viene autenticato e autorizzato prima di raggiungere il tuo VPC.

Puoi configurare regole aggiuntive per i gruppi di sicurezza per limitare il traffico in entrata alle tue istanze. Ad esempio, puoi utilizzare le regole in entrata per consentire il traffico sulle porte di gestione solo dall'endpoint EC2 Instance Connect.

Puoi configurare le regole della tabella di routing per consentire all'endpoint di connettersi a qualsiasi istanza in qualsiasi sottorete del VPC.

Il diagramma seguente mostra come un utente può connettersi alle proprie istanze da Internet utilizzando un endpoint EC2 Instance Connect. Innanzitutto, crea un endpoint EC2 Instance Connect nella sottorete A. Creiamo un'interfaccia di rete per l'endpoint nella sottorete, che funge da punto di ingresso per il traffico destinato alle tue istanze nel VPC. Se la tabella di routing per la sottorete B consente il traffico proveniente dalla sottorete A, allora puoi utilizzare l'endpoint per raggiungere le istanze nella sottorete B.



Considerazioni

Prima di iniziare, considera quanto segue.

- EC2 Instance Connect Endpoint è destinato specificamente ai casi d'uso del traffico di gestione, non ai trasferimenti di dati ad alto volume. I trasferimenti di grandi volumi di dati sono limitati.
- L'istanza deve disporre di un indirizzo IPv4 (privato o pubblico). L'endpoint EC2 Instance Connect non supporta la connessione a istanze che utilizzano indirizzi IPv6.
- (Istanze Linux) Se usi la tua key pair, puoi usare qualsiasi AMI Linux. Altrimenti, sulla tua istanza deve essere installato EC2 Instance Connect. Per informazioni su quali AMI includono EC2 Instance Connect e su come installarlo su altre AMI supportate, consulta. Installazione di EC2 Instance Connect
- Puoi assegnare un gruppo di sicurezza a un endpoint EC2 Instance Connect al momento della creazione. Altrimenti, utilizziamo il gruppo di sicurezza predefinito per il VPC. Il gruppo di sicurezza per un endpoint EC2 Instance Connect deve consentire il traffico in uscita verso le istanze di destinazione. Per ulteriori informazioni, consulta Gruppi di sicurezza per l'endpoint EC2 Instance Connect.
- Puoi configurare un endpoint EC2 Instance Connect per preservare gli indirizzi IP di origine dei client durante l'instradamento delle richieste verso le istanze. Altrimenti, l'indirizzo IP dell'interfaccia di rete diventa l'indirizzo IP del client per tutto il traffico in entrata.
  - Se si attiva la conservazione degli IP dei client, i gruppi di sicurezza per le istanze devono consentire il traffico proveniente dai client. Inoltre, le istanze devono trovarsi nello stesso VPC dell'endpoint EC2 Instance Connect.
  - Se disattivi la conservazione dell'IP del client, i gruppi di sicurezza per le istanze devono consentire il traffico proveniente dal VPC. Questa è l'impostazione predefinita.
  - I seguenti tipi di istanza non supportano la conservazione degli IP dei client: C1, CG1, CG2, G1, HI1, M1, M2, M3 e T1. Se attivi la conservazione dell'IP del client e tenti di connetterti a un'istanza con uno di questi tipi di istanza utilizzando EC2 Instance Connect Endpoint, la connessione fallisce.
  - La conservazione dell'IP del client non è supportata quando il traffico viene instradato attraverso un gateway di transito.
- Quando crei un endpoint EC2 Instance Connect, viene creato automaticamente un ruolo collegato al servizio Amazon EC2 in (IAM). AWS Identity and Access Management Amazon EC2 utilizza il ruolo collegato ai servizi per fornire interfacce di rete nell'account, necessarie per creare endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Ruolo collegato ai servizi per l'endpoint EC2 Instance Connect.
- Ogni endpoint EC2 Instance Connect può supportare fino a 20 connessioni simultanee.

- La durata massima per una connessione TCP stabilita è di 1 ora (3.600 secondi). È possibile specificare la durata massima consentita in una policy IAM, che può arrivare fino a 3.600 secondi. Per ulteriori informazioni, consulta Autorizzazioni per utilizzare EC2 Instance Connect Endpoint per connettersi alle istanze.

Concedi le autorizzazioni per utilizzare EC2 Instance Connect Endpoint

Per impostazione predefinita, le entità IAM non dispongono dell'autorizzazione per creare, descrivere o modificare gli endpoint EC2 Instance Connect. Un amministratore IAM può creare policy IAM che concedono le autorizzazioni necessarie per eseguire azioni specifiche sulle risorse di cui ha bisogno.

Per informazioni sulla creazione di una policy IAM, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

I seguenti esempi di policy mostrano che è possibile controllare le autorizzazioni degli utenti per gli endpoint EC2 Instance Connect.

Esempi

- Autorizzazioni per creare, descrivere ed eliminare gli endpoint EC2 Instance Connect
- Autorizzazioni per utilizzare EC2 Instance Connect Endpoint per connettersi alle istanze
- Autorizzazioni per la connessione solo da un intervallo di indirizzi IP specifico

Autorizzazioni per creare, descrivere ed eliminare gli endpoint EC2 Instance Connect

Per creare un endpoint EC2 Instance Connect, gli utenti hanno bisogno delle autorizzazioni per le seguenti operazioni:

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `iam:CreateServiceLinkedRole`

Per descrivere ed eliminare gli endpoint EC2 Instance Connect, gli utenti hanno bisogno delle autorizzazioni per le seguenti operazioni:

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2:DeleteInstanceConnectEndpoint`

Puoi creare una policy che concede le autorizzazioni per creare, descrivere ed eliminare gli endpoint EC2 Instance Connect in tutte le sottoreti. In alternativa, puoi limitare le operazioni per le sottoreti specificate solo indicando gli ARN della sottorete come `Resource` consentita o utilizzando la chiave di condizione `ec2:SubnetID`. Puoi anche utilizzare la chiave di condizione `aws:ResourceTag` per consentire o negare esplicitamente la creazione di endpoint con determinati tag. Per ulteriori informazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM .

Policy IAM di esempio

Nel seguente esempio di policy IAM, la sezione `Resource` concede l'autorizzazione per creare ed eliminare gli endpoint in tutte le sottoreti, specificati dall'asterisco (*). Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly * è quindi necessario nell'elemento `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "GrantAllActionsInAllSubnets",
            "Action": [
                "ec2:CreateInstanceConnectEndpoint",
                "ec2:DeleteInstanceConnectEndpoint",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:subnet/*"
        },
        {
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:::security-group/*"
        },
        {
            "Sid": "DescribeInstanceConnectEndpoints",
            "Action": [
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
```

```
        }
    ]
}
```

Autorizzazioni per utilizzare EC2 Instance Connect Endpoint per connettersi alle istanze

L'operazione `ec2-instance-connect:OpenTunnel` concede l'autorizzazione per stabilire una connessione TCP a un'istanza da connettere tramite l'endpoint EC2 Instance Connect. Puoi specificare l'endpoint EC2 Instance Connect da utilizzare. In alternativa, una `Resource` con un asterisco (*) consente agli utenti di utilizzare qualsiasi endpoint EC2 Instance Connect disponibile. È inoltre possibile limitare l'accesso alle istanze in base alla presenza o all'assenza di tag risorsa come chiavi di condizione.

Condizioni

- `ec2-instance-connect:remotePort`— La porta dell'istanza che può essere utilizzata per stabilire una connessione TCP. Quando viene utilizzata questa chiave di condizione, il tentativo di connessione a un'istanza su una porta diversa da quella specificata nella policy genera un errore.
- `ec2-instance-connect:privateIpAddress`— L'indirizzo IP privato di destinazione associato all'istanza con cui si desidera stabilire una connessione TCP. Puoi specificare un singolo indirizzo IP, ad esempio `10.0.0.1/32` oppure un intervallo di IP tramite CIDR, ad esempio `10.0.1.0/28`. Quando viene utilizzata questa chiave di condizione, il tentativo di connessione a un'istanza con un indirizzo IP privato diverso o al di fuori dell'intervallo CIDR genera un errore.
- `ec2-instance-connect:maxTunnelDuration`— La durata massima di una connessione TCP stabilita. L'unità è in secondi e la durata varia da un minimo di 1 secondo a un massimo di 3.600 secondi (1 ora). Se la condizione non è specificata, la durata predefinita è impostata su 3.600 secondi (1 ora). Il tentativo di connessione a un'istanza per un periodo superiore alla durata specificata nella policy IAM o per un periodo superiore al valore massimo predefinito genera un errore. La connessione viene interrotta dopo la durata specificata.

  Se `maxTunnelDuration` è specificato nella policy IAM e il valore indicato è inferiore a 3.600 secondi (impostazione predefinita), devi specificare `--max-tunnel-duration` nel comando quando ti connetti a un'istanza. Per informazioni su come connettersi a un'istanza, consulta Connettiti a un'istanza Amazon EC2 utilizzando EC2 Instance Connect Endpoint.

Puoi anche concedere a un utente l'accesso per stabilire connessioni alle istanze in base alla presenza di tag di risorsa sull'endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM .

Per le istanze Linux, l'`ec2-instance-connect:SendSSHPublicKey`azione concede l'autorizzazione a inviare la chiave pubblica a un'istanza. La condizione `ec2:osuser` specifica il nome dell'utente del sistema operativo (SO) che può inviare la chiave pubblica a un'istanza. Usa il nome utente predefinito per l'AMI che hai usato per avviare l'istanza. Per ulteriori informazioni, consulta Concessione di un'autorizzazione IAM per EC2 Instance Connect.

Policy IAM di esempio

I seguenti esempi di policy IAM consentono a un principale IAM di connettersi a un'istanza utilizzando solo l'endpoint EC2 Instance Connect specificato, identificato dall'ID endpoint specificato. `eice-123456789abcdef` La connessione viene stabilita con successo solo se tutte le condizioni sono soddisfatte.

> **Note**
>
> Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly `*` è quindi necessario nell'elemento `Resource`.

Linux

Questo esempio valuta se la connessione all'istanza è stabilita sulla porta 22 (SSH), se l'indirizzo IP privato dell'istanza è compreso nell'intervallo di `10.0.1.0/31` (tra `10.0.1.0` e`10.0.1.1`) ed `maxTunnelDuration` è minore o uguale a secondi. `3600` La connessione viene interrotta dopo `3600` secondi (1 ora).

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
```

```
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Windows

Questo esempio valuta se la connessione all'istanza è stabilita sulla porta 3389 (RDP), se l'indirizzo IP privato dell'istanza è compreso nell'intervallo di `10.0.1.0/31` (tra `10.0.1.0` e`10.0.1.1`) ed `maxTunnelDuration` è inferiore o uguale a `3600` secondi. La connessione viene interrotta dopo `3600` secondi (1 ora).

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
```

```
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "3389"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Autorizzazioni per la connessione solo da un intervallo di indirizzi IP specifico

L'esempio seguente di policy IAM consente a un principale IAM di connettersi a un'istanza a condizione che si connetta da un indirizzo IP all'interno dell'intervallo di indirizzi IP specificato nella policy. Se il principale IAM chiama `OpenTunnel` da un indirizzo IP non compreso `192.0.2.0/24` (l'intervallo di indirizzi IP di esempio in questa policy), la risposta è`Access Denied`. Per ulteriori informazioni, consulta la sezione `aws:SourceIp` nella Guida per l'utente di IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
```

```
                },
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Gruppi di sicurezza per l'endpoint EC2 Instance Connect

Un gruppo di sicurezza controlla il traffico consentito per raggiungere e lasciare le risorse a cui è associato. Ad esempio, neghiamo il traffico da e verso un'istanza Amazon EC2 a meno che non sia specificamente consentito dai gruppi di sicurezza associati all'istanza.

Gli esempi seguenti mostrano come configurare le regole dei gruppi di sicurezza per l'endpoint EC2 Instance Connect e le istanze di destinazione.

Esempi

- Regole del gruppo di sicurezza EC2 Instance Connect Endpoint
- Regole del gruppo di sicurezza dell'istanza Target

Regole del gruppo di sicurezza EC2 Instance Connect Endpoint

Le regole del gruppo di sicurezza per un endpoint EC2 Instance Connect devono consentire al traffico in uscita destinato alle istanze di destinazione di lasciare l'endpoint. È possibile specificare il gruppo di sicurezza dell'istanza o l'intervallo di indirizzi IPv4 del VPC come destinazione.

Il traffico verso l'endpoint proviene dal servizio Endpoint EC2 Instance Connect ed è consentito indipendentemente dalle regole in entrata per il gruppo di sicurezza degli endpoint. Per controllare chi può utilizzare EC2 Instance Connect Endpoint per connettersi a un'istanza, utilizza una policy IAM. Per ulteriori informazioni, consulta Autorizzazioni per utilizzare EC2 Instance Connect Endpoint per connettersi alle istanze.

Esempio di regola in uscita: riferimento ai gruppi di sicurezza

L'esempio seguente utilizza il riferimento ai gruppi di sicurezza, il che significa che la destinazione è un gruppo di sicurezza associato alle istanze di destinazione. Questa regola consente il traffico in uscita dall'endpoint verso tutte le istanze che utilizzano questo gruppo di sicurezza.

Protocollo	Destinazione	Intervallo porte	Commento
TCP	*ID del gruppo di sicurezza dell'istanza*	22	Consente il traffico SSH in uscita verso tutte le istanze associate al gruppo di sicurezza dell'istanza

Esempio di regola in uscita: intervallo di indirizzi IPv4

L'esempio seguente consente il traffico in uscita verso l'intervallo di indirizzi IPv4 specificato. Gli indirizzi IPv4 di un'istanza vengono assegnati dalla relativa sottorete, quindi è possibile utilizzare l'intervallo di indirizzi IPv4 del VPC.

Protocollo	Destinazione	Intervallo porte	Commento
TCP	*CIDR IPv4 del VPC*	22	Consente il traffico SSH in uscita verso il VPC

Regole del gruppo di sicurezza dell'istanza Target

Le regole del gruppo di sicurezza per le istanze di destinazione devono consentire il traffico in entrata dall'endpoint EC2 Instance Connect. È possibile specificare il gruppo di sicurezza dell'endpoint o un intervallo di indirizzi IPv4 come origine. Se si specifica un intervallo di indirizzi IPv4, l'origine dipende dal fatto che la conservazione dell'IP del client sia attivata o disattivata. Per ulteriori informazioni, consulta Considerazioni.

Poiché i gruppi di sicurezza sono dotati di stato, il traffico di risposta può lasciare il VPC indipendentemente dalle regole in uscita per il gruppo di sicurezza dell'istanza.

Esempio di regola in entrata: riferimento al gruppo di sicurezza

L'esempio seguente utilizza il riferimento ai gruppi di sicurezza, il che significa che l'origine è il gruppo di sicurezza associato all'endpoint. Questa regola consente il traffico SSH in entrata dall'endpoint verso tutte le istanze che utilizzano questo gruppo di sicurezza, indipendentemente dal fatto che la conservazione dell'IP del client sia attivata o disattivata. Se non esistono altre regole del gruppo di sicurezza in entrata per SSH, le istanze accettano il traffico SSH solo dall'endpoint.

Protocollo	Origine	Intervallo porte	Commento
TCP	*ID del gruppo di sicurezza dell'endpoint*	22	Consente il traffico SSH in entrata dalle risorse associate al gruppo di sicurezza degli endpoint

Esempio di regola in entrata: conservazione dell'IP del client disattivata

L'esempio seguente consente il traffico SSH in entrata dall'intervallo di indirizzi IPv4 specificato. Poiché la conservazione dell'IP del client è disattivata, l'indirizzo IPv4 di origine è l'indirizzo dell'interfaccia di rete dell'endpoint. L'indirizzo dell'interfaccia di rete dell'endpoint viene assegnato dalla relativa sottorete, quindi è possibile utilizzare l'intervallo di indirizzi IPv4 del VPC per consentire le connessioni a tutte le istanze del VPC.

Protocollo	Origine	Intervallo porte	Commento
TCP	*CIDR IPv4 del VPC*	22	Consente il traffico SSH in entrata dal VPC

Esempio di regola in entrata: conservazione dell'IP del client attiva

L'esempio seguente consente il traffico SSH in entrata dall'intervallo di indirizzi IPv4 specificato. Poiché la conservazione dell'IP del client è attiva, l'indirizzo IPv4 di origine è l'indirizzo del client.

Protocollo	Origine	Intervallo porte	Commento
TCP	*Intervallo di indirizzi IPv4 pubblico*	22	Consente il traffico in entrata dall'intervallo di indirizzi IPv4 del client specificato

Creazione di un endpoint EC2 Instance Connect

Puoi creare un endpoint EC2 Instance Connect per consentire una connessione sicura alle tue istanze.

Non puoi modificare un endpoint EC2 Instance Connect dopo averlo creato. È invece necessario eliminare l'endpoint EC2 Instance Connect e crearne uno nuovo con le impostazioni necessarie.

Prerequisiti

Devi disporre delle autorizzazioni IAM necessarie per creare un endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Autorizzazioni per creare, descrivere ed eliminare gli endpoint EC2 Instance Connect.

Sottoreti condivise

Puoi creare un endpoint EC2 Instance Connect in una sottorete condivisa con te. Non puoi utilizzare un endpoint EC2 Instance Connect creato dal proprietario del VPC in una sottorete condivisa con te.

Crea l'endpoint utilizzando la console

Utilizza la seguente procedura per creare un endpoint EC2 Instance Connect.

Per creare un endpoint EC2 Instance Connect

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Endpoints (Endpoint).
3. Scegli Crea endpoint, quindi specifica le impostazioni dell'endpoint come segue:
   a. (Facoltativo) in Tag nome, inserisci un nome per l'endpoint.
   b. In Categoria del servizio, scegli Endpoint EC2 Instance Connect.
   c. Per VPC, seleziona il VPC con le istanze di destinazione.
   d. (Facoltativo) Per conservare gli indirizzi IP dei client, espandi Impostazioni aggiuntive e seleziona la casella di controllo. Altrimenti, l'impostazione predefinita prevede l'utilizzo dell'interfaccia di rete dell'endpoint come indirizzo IP del client.
   e. (Facoltativo) in Gruppi di sicurezza, scegli il gruppo di sicurezza da associare all'endpoint. Altrimenti, l'impostazione predefinita prevede l'utilizzo del gruppo di sicurezza predefinito per il VPC. Per ulteriori informazioni, consulta Gruppi di sicurezza per l'endpoint EC2 Instance Connect.
   f. In Sottorete, seleziona la sottorete in cui creare l'endpoint.
   g. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
4. Controlla le impostazioni e poi scegli Crea endpoint.

   Lo stato iniziale dell'endpoint è In sospeso. Prima di poterti connettere a un'istanza utilizzando questo endpoint, devi attendere che lo stato dell'endpoint sia Disponibile. Ciò può richiedere alcuni minuti.
5. Per connetterti a un'istanza utilizzando il tuo endpoint, vedi. Connessione a un'istanza

Crea l'endpoint utilizzando il AWS CLI

Usa il create-instance-connect-endpointcomando per creare un endpoint EC2 Instance Connect.

Prerequisiti

Installa AWS CLI la versione 2 e configurala utilizzando le tue credenziali. Per ulteriori informazioni, consulta Installare o aggiornare alla versione più recente di AWS CLI e configurarla AWS CLI nella Guida per l'AWS Command Line Interface utente. In alternativa, apri AWS CloudShell ed AWS CLI esegui i comandi nella sua shell preautenticata.

Per creare l'endpoint

Usa il seguente comando per creare un'interfaccia di rete endpoint per il tuo endpoint EC2 Instance Connect nella sottorete specificata.

```
aws ec2 create-instance-connect-endpoint --subnet-id subnet-0123456789example
```

Di seguito è riportato un output di esempio.

```
 {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "create-complete",
        "StateMessage": "",
        "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-endpoint.us-
east-1.amazonaws.com",
        "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "NetworkInterfaceIds": [
            "eni-0123abcd"
        ],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1a",
        "CreatedAt": "2023-04-07T15:43:53.000Z",
        "SubnetId": "subnet-0123abcd",
        "PreserveClientIp": false,
        "SecurityGroupIds": [
            "sg-0123abcd"
        ],
        "Tags": []
}
```

Per monitorare lo stato della creazione

Il valore iniziale per il campo `State` è `create-in-progress`. Prima di connetterti a un'istanza utilizzando questo endpoint, devi attendere che lo stato sia `create-complete`. Usa il describe-instance-connect-endpointscomando per monitorare lo stato dell'endpoint EC2 Instance Connect. Il parametro --query filtra i risultati nel campo. `State`

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-
ids eice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

Di seguito è riportato un output di esempio.

```
create-complete
```

Connettiti a un'istanza Amazon EC2 utilizzando EC2 Instance Connect Endpoint

Puoi utilizzare EC2 Instance Connect Endpoint per connetterti a un'istanza Amazon EC2 che supporta SSH o RDP.

Indice

Prerequisiti

- Devi disporre dell'autorizzazione IAM richiesta per connetterti a un endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Autorizzazioni per utilizzare EC2 Instance Connect Endpoint per connettersi alle istanze.
- L'endpoint EC2 Instance Connect deve essere nello stato Disponibile (console) o `create-complete` (AWS CLI). Se non disponi di un endpoint EC2 Instance Connect per il tuo VPC, puoi crearne uno. Per ulteriori informazioni, consulta Creazione di un endpoint EC2 Instance Connect.
- (istanze Linux) Per utilizzare la console EC2 per connettersi all'istanza o per utilizzare la CLI per connettersi e fare in modo che EC2 Instance Connect gestisca la chiave temporanea, è necessario che nell'istanza sia installato EC2 Instance Connect. Per ulteriori informazioni, consulta Installazione di EC2 Instance Connect.
- Assicurati che il gruppo di sicurezza dell'istanza consenta il traffico SSH in entrata dall'endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza dell'istanza Target.

Connessione a un'istanza Linux tramite la console Amazon EC2

Puoi connetterti a un'istanza utilizzando la console Amazon EC2 come segue.

Per connetterti alla tua istanza utilizzando il client basato su browser

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza, scegli Connect.
4. Scegli la scheda EC2 Instance Connect.
5. In Tipo di connessione, scegli Connetti tramite endpoint EC2 Instance Connect.
6. Per l'endpoint EC2 Instance Connect, scegli l'ID dell'endpoint EC2 Instance Connect.
7. Per Nome utente, se l'AMI che hai usato per avviare l'istanza utilizza un nome utente diverso da `ec2-user`, inserisci il nome utente corretto.
8. In Durata massima del tunnel (secondi), inserisci la durata massima consentita per la connessione SSH.

   La durata deve soddisfare qualsiasi `maxTunnelDuration` condizione specificata nella policy IAM. Se non hai accesso alla policy IAM, contatta il tuo amministratore.
9. Scegli Connetti. Si apre una finestra di terminale per la tua istanza.

Connessione a un'istanza Linux tramite SSH

Puoi utilizzare l'SSH per connetterti all'istanza Linux e usare il comando `open-tunnel` per stabilire un tunnel privato. Puoi utilizzare il `open-tunnel` in modalità connessione singola o multipla.

Per informazioni sull'utilizzo di AWS CLI per connettersi all'istanza tramite SSH, consultaConnect utilizzando AWS CLI.

Nell'esempio seguente viene utilizzato OpenSSH. Puoi usare qualsiasi altro client SSH che supporti una modalità proxy.

Connessione singola

Per consentire solo una connessione singola a un'istanza utilizzando l'SSH e il comando **`open-tunnel`**

Usa `ssh` il open-tunnel AWS CLI comando and come segue. Il comando proxy `-o` racchiude il comando `open-tunnel` che crea il tunnel privato verso l'istanza.

```
ssh -i my-key-pair.pem ec2-user@i-0123456789example \
```

```
    -o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-
id i-0123456789example'
```

Per:

- `-i`: specifica la coppia di chiavi utilizzata per avviare l'istanza.
- *`ec2-user`*`@`*`i-0123456789example`*: specifica il nome utente dell'AMI utilizzata per avviare l'istanza e l'ID istanza.
- `--instance-id`: specifica l'ID istanza a cui connetterti. In alternativa, specifica `%h` che estrae l'ID istanza dall'utente.

Connessione multipla

Per consentire più connessioni a un'istanza, esegui prima il open-tunnel AWS CLI comando per iniziare ad ascoltare nuove connessioni TCP, quindi utilizzalo per `ssh` creare una nuova connessione TCP e un tunnel privato verso l'istanza.

Per consentire connessioni multiple all'istanza tramite SSH e il comando **`open-tunnel`**

1. Inserisci il comando seguente per avviare l'ascolto di nuove connessioni TCP sulla porta specificata del computer locale.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-0123456789example \
       --local-port 8888
   ```

   Output previsto

   ```
   Listening for connections on port 8888.
   ```

2. In una nuova finestra del terminale, esegui il seguente comando `ssh` per creare una nuova connessione TCP e un tunnel privato verso la tua istanza.

   ```
   ssh -i my-key-pair.pem ec2-user@localhost -p 8888
   ```

   Output previsto: nella prima finestra del terminale, visualizzi le seguenti informazioni:

   ```
   [1] Accepted new tcp connection, opening websocket tunnel.
   ```

Potresti anche visualizzare le seguenti informazioni:

```
[1] Closing tcp connection.
```

Connect alla propria istanza Linux utilizzando AWS CLI

Se conosci solo l'ID dell'istanza, puoi usare il AWS CLI comando ec2-instance-connect per connetterti all'istanza utilizzando un client SSH. Per ulteriori informazioni sull'uso del comando ec2-instance-connect, consulta. Connect utilizzando AWS CLI

Prerequisiti

Installa la AWS CLI versione 2 e configurala utilizzando le tue credenziali. Per ulteriori informazioni, consulta Installare o aggiornare alla versione più recente di AWS CLI e configurarla AWS CLI nella Guida per l'AWS Command Line Interface utente. In alternativa, apri AWS CloudShell ed AWS CLI esegui i comandi nella sua shell preautenticata.

Per la connessione all'istanza tramite l'ID istanza e un endpoint EC2 Instance Connect

Se conosci solo l'ID dell'istanza, usa il comando CLI ec2-instance-connect e specifica `ssh` il comando, l'ID dell'istanza e il parametro con il valore. `--connection-type eice`

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

> **Tip**
>
> Se ricevi un errore durante l'utilizzo di questo comando, assicurati di utilizzare la versione 2. AWS CLI Il `ssh` parametro è disponibile solo nella AWS CLI versione 2. Per ulteriori informazioni, vedere Informazioni sulla AWS CLI versione 2 nella Guida AWS Command Line Interface per l'utente.

Connettiti alla tua istanza Windows utilizzando EC2 Instance Connect Endpoint

Puoi utilizzare il Remote Desktop Protocol (RDP) sull'endpoint EC2 Instance Connect per connetterti a un'istanza Windows senza un indirizzo IPv4 o un nome DNS pubblici.

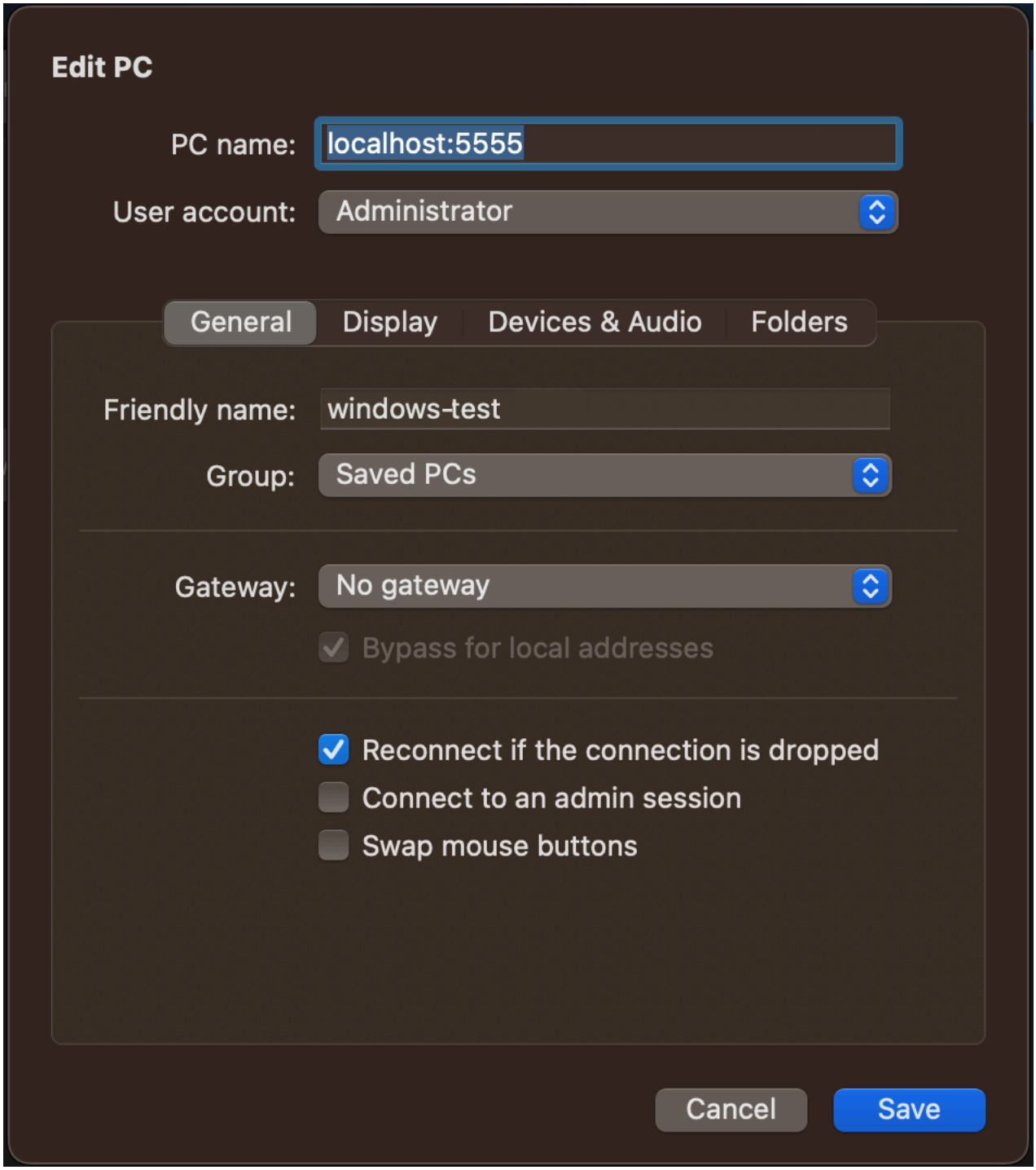
Per connetterti alla tua istanza Windows utilizzando un client RDP

1. Completa i passaggi da 1 a 8 in Connect to your Windows using RDP. Dopo aver scaricato il file desktop RDP al passaggio 8, riceverai il messaggio Impossibile connettersi, il che è prevedibile perché l'istanza non dispone di un indirizzo IP pubblico.
2. Esegui il comando seguente per stabilire un tunnel privato verso il VPC in cui si trova l'istanza. `--remote-port` deve essere `3389` perché il protocollo RDP utilizza la porta 3389 per impostazione predefinita.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-0123456789example \
       --remote-port 3389 \
       --local-port any-port
   ```

3. Nella cartella Download, trova il file desktop RDP che hai scaricato e trascinalo nella finestra del client RDP.
4. Fai clic con il pulsante destro del mouse sul file desktop RDP e scegli Modifica.
5. Nella finestra Modifica PC, per il nome del PC (l'istanza a cui connetterti)`localhost:`*`local-port`*, inserisci, where *`local-port`* utilizza lo stesso valore specificato nel passaggio 2, quindi scegli Salva.

   Nota che la seguente schermata della finestra Modifica PC proviene da Microsoft Remote Desktop su un Mac. Se utilizzi un client Windows, la finestra potrebbe essere diversa.



6. Nel client RDP, fai clic con il pulsante destro del mouse sul PC (che hai appena configurato) e scegli Connetti per connetterti alla tua istanza.
7. Nel prompt, specifica la password decriptata dell'account dell'amministratore.

Risoluzione dei problemi

Utilizza le seguenti informazioni per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo dell'endpoint EC2 Instance Connect per connettere un'istanza.

Impossibile connettersi all'istanza

Di seguito sono riportati i motivi più comuni per cui potresti non essere in grado di connetterti alla tua istanza.

- Gruppi di sicurezza: controlla i gruppi di sicurezza assegnati all'endpoint EC2 Instance Connect e alla tua istanza. Per ulteriori informazioni sulle regole necessarie del gruppo di sicurezza, consulta Gruppi di sicurezza per l'endpoint EC2 Instance Connect.
- Stato dell'istanza: varica che la tua istanza abbia lo stato `running`.
- Coppia di chiavi: se il comando che stai utilizzando per la connessione richiede una chiave privata, verifica che l'istanza disponga di una chiave pubblica e di disporre della chiave privata corrispondente.
- Autorizzazioni IAM: verifica di disporre delle autorizzazioni IAM richieste. Per ulteriori informazioni, consulta Concedi le autorizzazioni per utilizzare EC2 Instance Connect Endpoint.

Per ulteriori suggerimenti per la risoluzione dei problemi relativi alle istanze Linux, consultaRisolvi i problemi di connessione alla tua istanza Linux. Per suggerimenti sulla risoluzione dei problemi relativi alle istanze Windows, consulta. the section called “Connettiti all'istanza Windows ”

ErrorCode: AccessDeniedException

Se ricevi un errore `AccessDeniedException` e la condizione `maxTunnelDuration` è specificata nella policy IAM, assicurati di indicare il parametro `--max-tunnel-duration` quando ti connetti a un'istanza. Per ulteriori informazioni su questo parametro, consulta open-tunnel in AWS CLI Command Reference.

Connessioni di log stabilite tramite endpoint EC2 Instance Connect

Puoi registrare le operazioni sulle risorse e controllare le connessioni stabilite sull'endpoint EC2 Instance Connect con AWS CloudTrail i log.

Per ulteriori informazioni sull'utilizzo AWS CloudTrail con Amazon EC2, consulta. Registra le chiamate API di Amazon EC2 utilizzando AWS CloudTrail

Registra le chiamate API EC2 Instance Connect Endpoint con AWS CloudTrail

Le operazioni relative alle risorse dell'endpoint EC2 Instance Connect vengono registrate CloudTrail come eventi di gestione. Quando vengono effettuate le seguenti chiamate API, l'attività viene registrata come CloudTrail evento nella cronologia degli eventi:

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

Utilizzo di AWS CloudTrail per controllare gli utenti che si connettono a un'istanza tramite endpoint EC2 Instance Connect

I tentativi di connessione alle istanze tramite EC2 Instance Connect Endpoint vengono registrati nella CloudTrail cronologia degli eventi. Quando viene avviata una connessione a un'istanza tramite un endpoint EC2 Instance Connect, la connessione viene registrata come evento di CloudTrail gestione con il comando of. `eventName` `OpenTunnel`

Puoi creare EventBridge regole Amazon che indirizzino l' CloudTrail evento verso un obiettivo. Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Di seguito è riportato un esempio di evento `OpenTunnel` gestionale a cui è stato effettuato l'accesso. CloudTrail


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name"
    },
    "eventTime": "2023-04-11T23:50:40Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
```

```
     "eventName": "OpenTunnel",
     "awsRegion": "us-east-1",
     "sourceIPAddress": "1.2.3.4",
     "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
     "requestParameters": {
         "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
         "maxTunnelDuration": "3600",
         "remotePort": "22",
         "privateIpAddress": "10.0.1.1"
     },
     "responseElements": null,
     "requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
     "eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
     "readOnly": false,
     "resources": [{
         "accountId": "123456789012",
         "type": "AWS::EC2::InstanceConnectEndpoint",
         "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
     }],
     "eventType": "AwsApiCall",
     "managementEvent": true,
     "recipientAccountId": "123456789012",
     "eventCategory": "Management"
}
```

Eliminare un endpoint EC2 Instance Connect

Quando hai finito con un endpoint EC2 Instance Connect, puoi eliminarlo.

Devi disporre delle autorizzazioni IAM necessarie per creare un endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Autorizzazioni per creare, descrivere ed eliminare gli endpoint EC2 Instance Connect.

Quando elimini un endpoint EC2 Instance Connect utilizzando la console, questo entra nello stato di eliminazione. Se l'eliminazione ha esito positivo, l'endpoint eliminato non viene più visualizzato. Se l'eliminazione non riesce, lo stato è `delete-failed` e il messaggio di stato fornisce il motivo dell'errore.

Quando elimini un endpoint EC2 Instance Connect utilizzando il AWS CLI, esso entra nello `delete-in-progress` stato. Se l'eliminazione ha esito positivo, entra nello `delete-complete` stato. Se l'eliminazione non riesce, lo stato è `delete-failed` e `StateMessage` fornisce il motivo dell'errore.

Console

Per eliminare un endpoint EC2 Instance Connect

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Endpoints (Endpoint).
3. Seleziona l'endpoint.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **delete**.
6. Scegli Elimina.

AWS CLI

Per eliminare un endpoint EC2 Instance Connect

Utilizza il delete-instance-connect-endpoint AWS CLI comando e specifica l'ID dell'endpoint EC2 Instance Connect da eliminare.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-
id eice-03f5e49b83924bbc7
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
        "SubnetId": "subnet-0123abcd"
    }
}
```

Ruolo collegato ai servizi per l'endpoint EC2 Instance Connect

Amazon EC2 utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente ad Amazon EC2. I ruoli collegati ai servizi sono predefiniti da Amazon EC2 e includono tutte le autorizzazioni necessarie affinché Amazon EC2 possa chiamare altri per tuo conto. Servizi AWS Per ulteriori informazioni, consulta Utilizzo di ruoli collegati a servizi nella Guida per l'utente di IAM .

Autorizzazioni di ruolo collegate ai servizi per EC2 Instance Connect Endpoint

Amazon EC2 utilizza AWSServiceRoleForEC2InstanceConnectper creare e gestire le interfacce di rete nel tuo account richieste da EC2 Instance Connect Endpoint.

Il ruolo AWSServiceRoleForEC2InstanceConnectcollegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `ec2-instance-connect.amazonaws.com`

Il ruolo AWSServiceRoleForEC2InstanceConnectcollegato al servizio utilizza la politica gestita Ec2. InstanceConnectEndpoint Per visualizzare le autorizzazioni per questa politica, consulta Ec2 InstanceConnectEndpoint nel Managed Policy Reference.AWS

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Crea un ruolo collegato al servizio per EC2 Instance Connect Endpoint

Non devi creare manualmente il ruolo collegato al servizio . Quando crei un endpoint EC2 Instance Connect, Amazon EC2 crea il ruolo collegato al servizio per te.

Modifica un ruolo collegato al servizio per EC2 Instance Connect Endpoint

EC2 Instance Connect Endpoint non consente di modificare il ruolo collegato al AWSServiceRoleForEC2InstanceConnectservizio.

Eliminare un ruolo collegato al servizio per EC2 Instance Connect Endpoint

Se non hai più bisogno di utilizzare EC2 Instance Connect Endpoint, ti consigliamo di eliminare il ruolo collegato al AWSServiceRoleForEC2InstanceConnectservizio.

È necessario eliminare tutte le risorse dell'endpoint EC2 Instance Connect prima di poter eliminare il ruolo collegato al servizio.

Per eliminare il ruolo collegato al servizio, consulta Eliminazione di un ruolo collegato al servizio nella Guida per l'utente IAM.

Quote per EC2 Instance Connect Endpoint

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica.

Hai le Account AWS seguenti quote relative a EC2 Instance Connect Endpoint.

Nome	Predefinita	Adattabile
Numero massimo di endpoint EC2 Instance Connect per utente Account AWS Regione AWS	5	No
Numero massimo di endpoint EC2 Instance Connect per VPC	1	No
Numero massimo di endpoint EC2 Instance Connect per sottorete	1	No
Numero massimo di connessioni simultanee per endpoint EC2 Instance Connect	20	No

Connessione dell'istanza EC2 a una risorsa AWS

Dopo aver avviato un'istanza, puoi collegarla a una o più AWS risorse.

Questa sezione descrive solo come connettere automaticamente un'istanza Amazon EC2 a un database Amazon RDS.

Connessione automatica di un'istanza EC2 a un database RDS

Nella console Amazon EC2 puoi utilizzare la funzionalità di connessione automatica per connettere rapidamente una o più istanze EC2 a un database RDS così da consentire il traffico tra queste.

Per ulteriori informazioni, consulta Come viene configurata automaticamente la connessione. Per una procedura guidata e dettagliata, che comprende altri modi per connettere un'istanza EC2 e un database RDS, consulta Tutorial: Connessione di un'istanza Amazon EC2 a un database Amazon RDS.

Argomenti

Costi

Sebbene la connessione automatica dell'istanza EC2 a un database RDS sia gratuita, ti verranno addebitati i costi per i servizi sottostanti. Verranno applicati costi per il trasferimento di dati se l'istanza EC2 e il database RDS si trovano in zone di disponibilità diverse. Per informazioni sui costi per il trasferimento di dati, consulta Trasferimento dati sulla pagina dei prezzi on demand di Amazon EC2.

Prerequisiti

Prima di connettere automaticamente un'istanza EC2 a un database RDS, verifica quanto segue:

- lo stato delle istanze EC2 deve essere Running (In esecuzione). Non puoi connettere un'istanza EC2 che si trovi in un altro stato.
- Le istanze EC2 e il database RDS devono essere nello stesso cloud privato virtuale (VPC). La funzione di connessione automatica non è supportata se un'istanza EC2 e un database RDS si trovano in VPC diversi.

Connessione automatica di un'istanza e un database

Puoi connettere automaticamente un'istanza EC2 a un database RDS subito dopo aver avviato l'istanza oppure in un secondo momento.

Connessione automatica dopo l'avvio

Per connettere automaticamente un'istanza EC2 a un database RDS subito dopo aver avviato l'istanza EC2, attieniti ai passaggi seguenti.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: connessione automatica di un'istanza EC2 appena avviata a un database RDS.

Connessione automatica di un'istanza EC2 appena avviata a un database RDS utilizzando la console EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di controllo della console seleziona Launch instance (Avvia istanza), quindi segui i passaggi per avviare un'istanza.
3. Nella pagina di conferma di avvenuto avvio dell'istanza seleziona Connect an RDS database (Connessione di un database RDS).
4. Nella finestra di dialogo Connect RDS Database (Connetti un database RDS), segui questi passaggi:

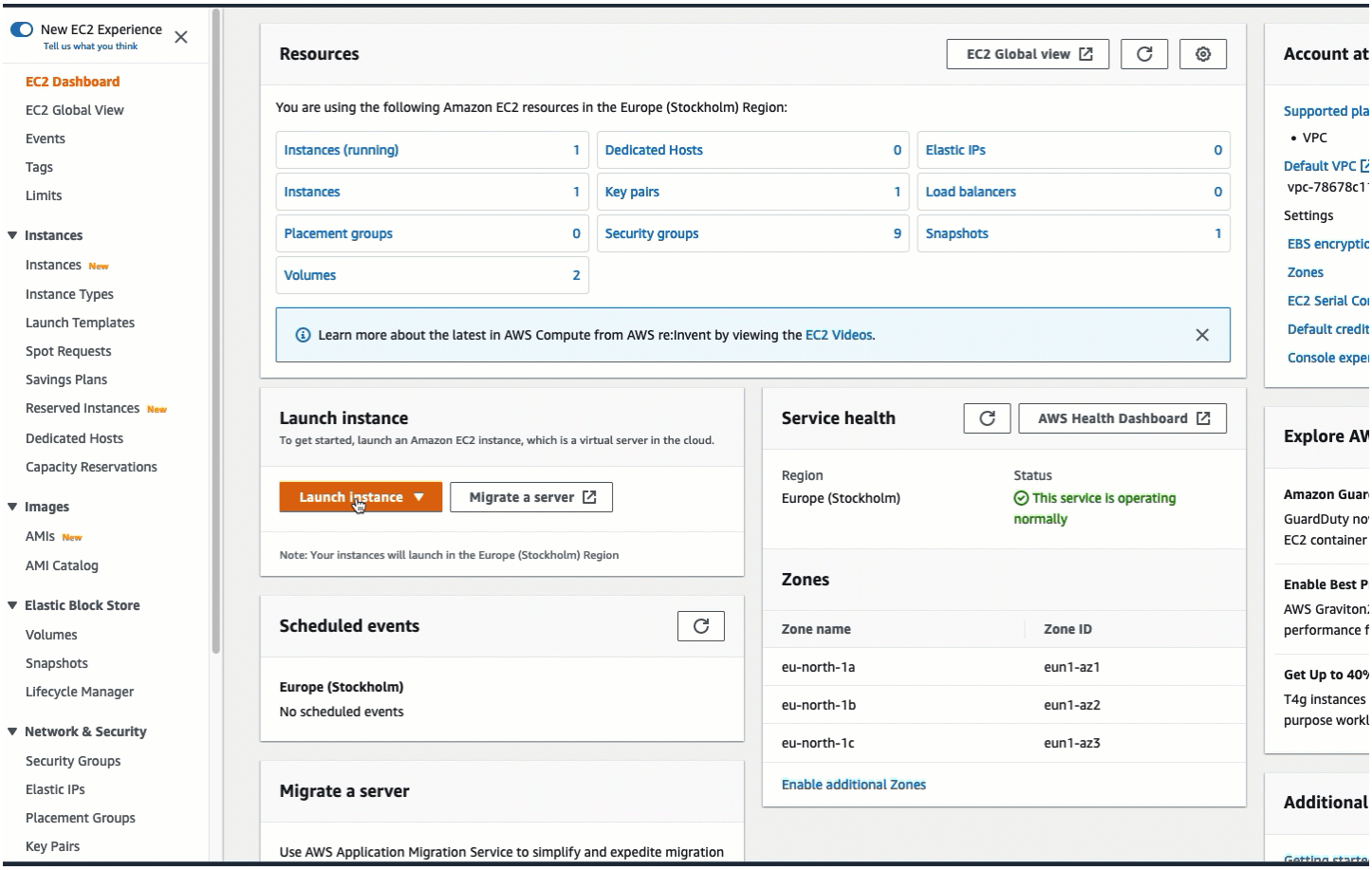
   a. Per il Database role (Ruolo del database) seleziona Cluster o Instance (Istanza).

   b. Per il RDS database (Database RDS), seleziona un database a cui connettersi.

      > **Note**
      >
      > Le istanze EC2 e il database RDS devono trovarsi nello stesso VPC per connettersi tra di loro.

   c. Scegli Connetti.

Visualizzazione di un'animazione: connessione automatica di un'istanza EC2 appena avviata a un database RDS



Connessione automatica a un'istanza esistente

Per connettere automaticamente un'istanza EC2 esistente a un database RDS, attieniti ai passaggi seguenti.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: connessione automatica di un'istanza EC2 esistente a un database RDS.

Connessione automatica di un'istanza EC2 esistente a un database RDS utilizzando la console EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona una o più istanze EC2 per connetterle a un database RDS, quindi seleziona Actions (Azioni), Networking (Reti), Connect RDS database (Connetti database RDS).

Se Connect RDS database (Connetti database RDS) non è disponibile, controlla che le istanze EC2 siano nello stato Running (In esecuzione) e che si trovino nello stesso VPC.

4. Nella finestra di dialogo Connect RDS Database (Connetti un database RDS), segui questi passaggi:

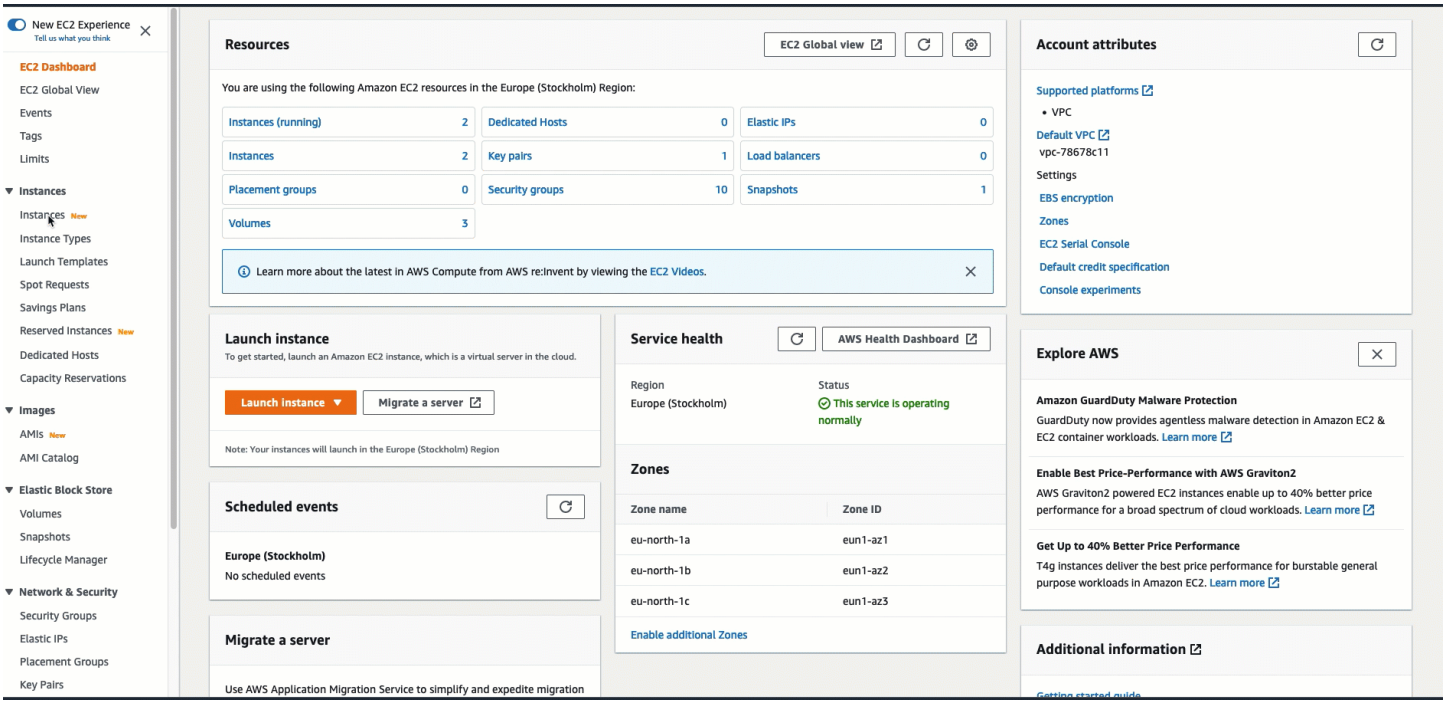
   a. Per il Database role (Ruolo del database) seleziona Cluster o Instance (Istanza).

   b. Per il RDS database (Database RDS), seleziona un database a cui connettersi.

   > **Note**
   >
   > Le istanze EC2 e il database RDS devono trovarsi nello stesso VPC per connettersi tra di loro.

   c. Scegli Connetti.

Visualizzazione di un'animazione: connessione automatica di un'istanza EC2 esistente a un database RDS



Per informazioni su come usare la console Amazon RDS per connettere automaticamente un'istanza EC2 a un database RDS, consulta Configurazione della connettività di rete automatica con un'istanza EC2 nella Guida per l'utente di Amazon RDS.

Come viene configurata automaticamente la connessione

Quando usi la console EC2 per la configurazione automatica della connessione tra un'istanza EC2 e un database RDS, tale connessione, necessaria per il traffico tra questi, viene configurata dai gruppi di sicurezza.

I gruppi di sicurezza vengono creati automaticamente e aggiunti all'istanza EC2 e al database RDS, come descritto di seguito:

- Amazon EC2 crea un gruppo di sicurezza chiamato ec2-rds-*x* e lo aggiunge all'istanza EC2. Una regola in uscita consente il traffico verso il database specificando rds-ec2-*x* (il gruppo di sicurezza del database) come destinazione.
- Amazon RDS crea un gruppo di sicurezza chiamato *rds-ec2-*x e lo aggiunge al database. Una regola in entrata consente il traffico dall'istanza EC2 specificando ec2-rds-*x* (il gruppo di sicurezza dell'istanza EC2) come origine.

I gruppo di sicurezza si riferiscono vicendevolmente come destinazione e origine e consentono il traffico solo sulla porta del database. Puoi riutilizzare questi gruppi di sicurezza in modo che qualsiasi database con il gruppo di sicurezza rds-ec2-*x* possa comunicare con qualsiasi istanza EC2 attraverso il gruppo di sicurezza ec2-rds-*x*.

I nomi dei gruppi di sicurezza seguono uno schema. Per i gruppi di sicurezza creati da Amazon EC2 il pattern è ec2-rds-*x*, mentre per i gruppi di sicurezza creati da Amazon RDS il pattern è rds-ec2-*x*. *x* è un numero che aumenta di 1 ogni volta che viene creato automaticamente un nuovo gruppo di sicurezza.

Tutorial: Connessione di un'istanza Amazon EC2 a un database Amazon RDS

Obiettivo del tutorial

L'obiettivo di questo tutorial è imparare a configurare una connessione sicura tra un'istanza Amazon EC2 e un database Amazon RDS utilizzando AWS Management Console.

Ci sono diverse opzioni per configurare la connessione. In questo tutorial esploriamo queste tre:

- Opzione 1: connessione automatica dell'istanza EC2 al database RDS utilizzando la console EC2

  Usa la funzione di connessione automatica nella console EC2 per configurare automaticamente la connessione tra l'istanza EC2 e il database RDS così da consentire il traffico tra l'istanza EC2 e il database RDS.

- Opzione 2: connessione automatica dell'istanza EC2 al database RDS utilizzando la console RDS

  Usa la funzione di connessione automatica nella console RDS per configurare automaticamente la connessione tra l'istanza EC2 e il database RDS così da consentire il traffico tra l'istanza EC2 e il database RDS.

- Opzione 3: connessione manuale dell'istanza EC2 al database RDS imitando la funzione di connessione automatica

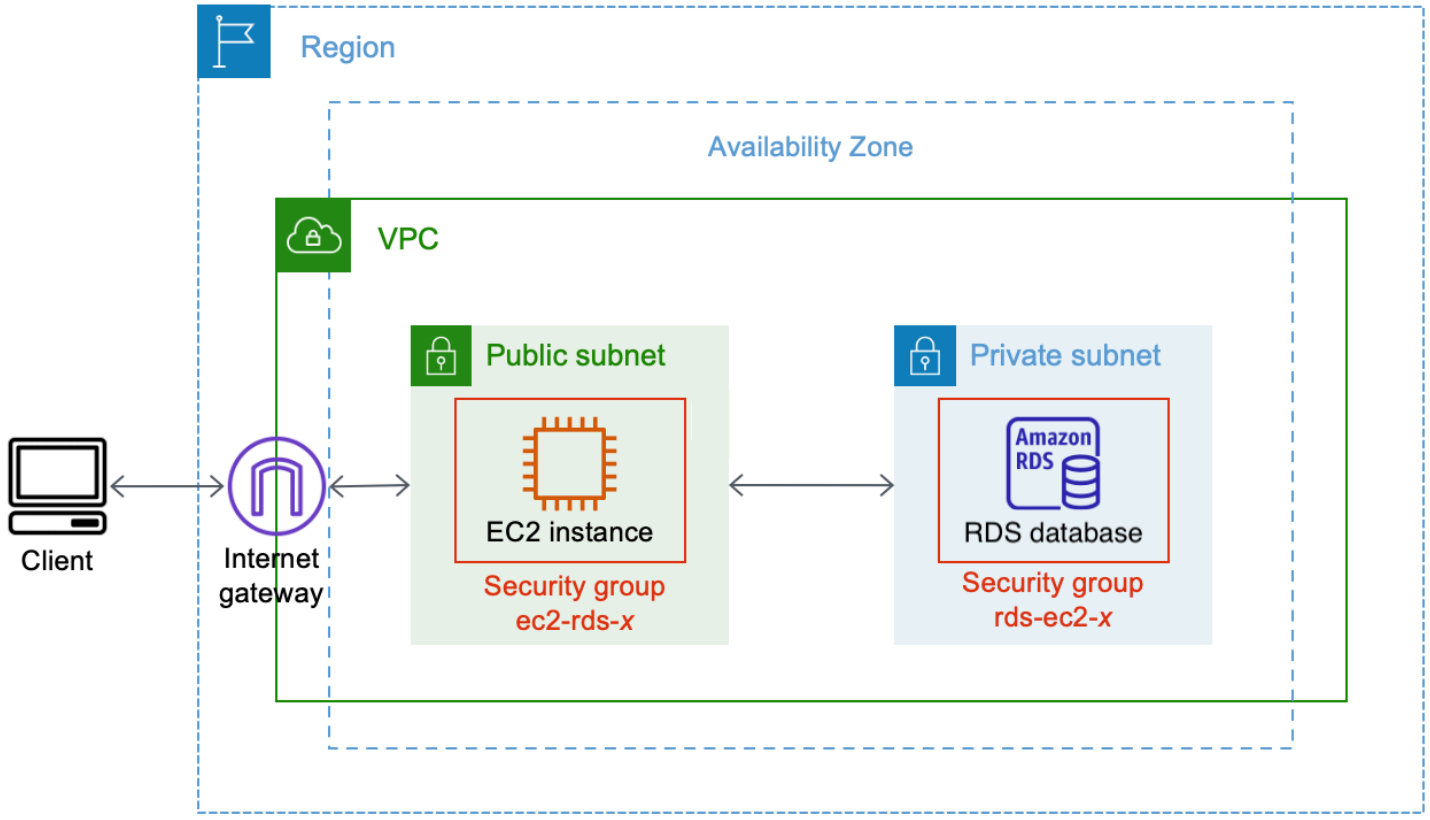
  Configura la connessione tra l'istanza EC2 e il database RDS configurando e assegnando manualmente i gruppi di sicurezza per riprodurre la configurazione creata automaticamente dalla funzione di connessione automatica nelle opzioni 1 e 2.

Context

Consideriamo il seguente scenario come il motivo per cui vorresti configurare una connessione tra la tua istanza EC2 e un database RDS: il tuo sito Web presenta un modulo che gli utenti devono compilare. Devi acquisire i dati del modulo in un database. Puoi ospitare il tuo sito Web su un'istanza EC2 configurata come server Web e puoi acquisire i dati del modulo in un database RDS. L'istanza EC2 e il database RDS devono essere connessi tra di loro in modo che i dati del modulo possano passare dall'istanza EC2 al database RDS. Questo tutorial spiega come configurare tale connessione. Nota che questo è solo un esempio di un caso d'uso per connettere un'istanza EC2 e un database RDS.

Architettura

Il diagramma seguente mostra le risorse create e la configurazione architettonica risultante dal completamento di tutti i passaggi di questo tutorial.



Il diagramma illustra le seguenti risorse che creerai:

- Creerai un'istanza EC2 e un database RDS nello stesso Regione AWS VPC e nella stessa zona di disponibilità.
- Creerai l'istanza EC2 in una sottorete pubblica.
- Creerai il database RDS in una sottorete privata.

  Quando utilizzi la console RDS per creare il database RDS e connettere automaticamente l'istanza EC2, il VPC, il gruppo di sottorete database e le impostazioni di accesso pubblico per il database vengono selezionate automaticamente. Il database RDS viene creato automaticamente in una sottorete privata all'interno dello stesso VPC dell'istanza EC2.
- Gli utenti di Internet possono connettersi all'istanza EC2 utilizzando SSH o HTTP/HTTPS tramite un gateway Internet.
- Gli utenti di Internet non possono connettersi direttamente al database RDS; solo l'istanza EC2 è connessa al database RDS.
- Quando utilizzi la funzione di connessione automatica per consentire il traffico tra l'istanza EC2 e il database RDS, vengono creati e aggiunti automaticamente i gruppi di sicurezza seguenti:

- Il gruppo di sicurezza ec2-rds-*x* viene creato e aggiunto all'istanza EC2. Una regola in uscita che considera il gruppo di sicurezza rds-ec2-*x* come destinazione. Ciò consente al traffico proveniente dall'istanza EC2 di raggiungere il database RDS con il gruppo di sicurezza ***rds-ec2-x***.
- Il gruppo di sicurezza rds-ec2-*x* viene creato e aggiunto all'istanza EC2. Una regola in uscita considera il gruppo di sicurezza ec2-rds-*x* come origine. Ciò consente al traffico proveniente dall'istanza EC2 con il gruppo di sicurezza ec2-rds-*x* di raggiungere il database RDS.

Utilizzando gruppi di sicurezza separati (uno per l'istanza EC2 e uno per il database RDS) hai un migliore controllo sulla sicurezza dell'istanza e del database. Se dovessi utilizzare lo stesso gruppo di sicurezza sia sull'istanza sia sul database e quindi modificassi il gruppo di sicurezza per adattarlo, ad esempio, solo al database, la modifica influirebbe sia sull'istanza sia sul database. In altre parole, se dovessi utilizzare un gruppo di sicurezza, potresti modificare involontariamente la sicurezza di una risorsa (l'istanza o il database) avendo dimenticato che il gruppo di sicurezza era associato a tale risorsa.

I gruppi di sicurezza creati automaticamente rispettano inoltre i privilegi minimi in quanto consentono solo la connessione reciproca per tale carico di lavoro sulla porta del database creando una coppia di gruppi di sicurezza specifica per il carico di lavoro.

Considerazioni

Considera quanto segue quando completi i passaggi di questo tutorial:

- Due console: per questo tutorial utilizzerai le due console seguenti:
  - Console Amazon EC2: utilizzerai la console EC2 per avviare istanze, per connettere automaticamente un'istanza EC2 a un database RDS e per l'opzione manuale di configurazione della connessione attraverso la creazione di gruppi di sicurezza.
  - Console Amazon RDS: utilizzerai la console RDS per creare un database RDS e connettere automaticamente un'istanza EC2 a un database RDS.
- Un VPC: per utilizzare la funzione di connessione automatica, l'istanza EC2 e il database RDS devono trovarsi nello stesso VPC.

  Se dovessi configurare manualmente la connessione tra l'istanza EC2 e il database RDS, potresti avviare l'istanza EC2 in un VPC e il database RDS in un altro VPC; tuttavia, dovresti configurare instradamento e configurazione VPC aggiuntivi. Questo scenario non è trattato in questo tutorial.
- Uno Regione AWS: l'istanza EC2 e il database RDS devono trovarsi nella stessa regione.

- Due gruppi di sicurezza: la connettività tra l'istanza EC2 e il database RDS viene configurata da due gruppi di sicurezza: un gruppo di sicurezza per l'istanza EC2 e un gruppo di sicurezza per il database RDS.

  Quando utilizzi la funzione di connessione automatica nella console EC2 o nella console RDS per configurare la connettività (opzione 1 e opzione 2 di questo tutorial), i gruppi di sicurezza vengono creati e assegnati automaticamente all'istanza EC2 e al database RDS.

  Se non utilizzi la funzione di connessione automatica, dovrai creare e assegnare manualmente i gruppi di sicurezza. Puoi farlo nell'opzione 3 di questo tutorial.

È ora di completare il tutorial

30 minutes

Puoi completare l'intero tutorial in una sola sessione oppure puoi completarlo facendo un passo per volta.

Costi

Completando questo tutorial, potresti incorrere in costi per AWS le risorse che crei.

Puoi utilizzare Amazon EC2 con il piano gratuito a condizione che il tuo AWS account abbia meno di 12 mesi e configuri le tue risorse in base ai requisiti del piano gratuito.

Ti verranno applicati costi per il trasferimento di dati se l'istanza EC2 e il database RDS si trovano in zone di disponibilità diverse. Per evitare di incorrere in questi costi, l'istanza EC2 e il database RDS devono trovarsi nella stessa zona di disponibilità. Per informazioni sui costi per il trasferimento di dati, consulta Trasferimento dati sulla pagina dei prezzi on demand di Amazon EC2.

Per evitare di incorrere in costi dopo aver completato il tutorial, assicurati di eliminare le risorse se non sono più necessarie. Per le fasi di eliminazione delle risorse, consulta Eliminazione.

Opzione 1: connessione automatica dell'istanza EC2 al database RDS utilizzando la console EC2

Obiettivo

L'obiettivo dell'opzione 1 è comprendere la funzionalità di connessione automatica nella console EC2 che configura automaticamente la connessione tra l'istanza EC2 e il database RDS per consentire il traffico dall'istanza EC2 al database RDS. Nell'opzione 3 imparerai come configurare manualmente la connessione.

Prima di iniziare

Per completare questo tutorial, avrai bisogno di quanto segue:

- un database RDS nello stesso VPC dell'istanza EC2. Puoi utilizzare un database RDS esistente o seguire i passaggi illustrati nell'Attività 1 per creare un nuovo database RDS.
- un'istanza EC2 nello stesso VPC del database RDS. Puoi utilizzare un'istanza EC2 esistente o seguire i passaggi illustrati nell'Attività 2 per creare una nuova istanza EC2.
- Autorizzazioni per effettuare le seguenti operazioni:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Attività per completare l'opzione 1

- Attività 1: creazione di un database RDS (opzionale)
- Attività 2: avvio di un'istanza EC2 (opzionale)
- Attività 3: connessione automatica dell'istanza EC2 al database RDS
- Attività 4: verifica della configurazione della connessione

Attività 1: creazione di un database RDS (opzionale)

> **Note**
>
> La creazione di un database Amazon RDS non è l'obiettivo di questo tutorial. Se già disponi di un database RDS e vorresti utilizzarlo in questo tutorial, puoi ignorare questa attività.

Obiettivo dell'attività

L'obiettivo di questa attività è creare un database RDS in modo da poter completare l'Attività 3 che prevede la configurazione della connessione tra l'istanza EC2 e il database RDS. Se disponi di un database RDS che puoi utilizzare, puoi saltare questa attività.

> **Important**
>
> Se utilizzi un database RDS esistente, assicurati che si trovi nello stesso VPC dell'istanza EC2 in modo da poter utilizzare la funzione di connessione automatica.

Procedura per creare un database RDS

Attieniti ai passaggi seguenti per creare un database RDS.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: creazione di un database RDS.

Configurazione del database RDS

I passaggi di questa attività illustrano la configurazione del database RDS come segue:

- Tipo di motore: MySQL
- Modello: livello gratuito
- DB Instance Identifier (Identificatore istanze database): **`tutorial-database-1`**
- DB instance class (Classe istanza database): `db.t3.micro`

> **Important**
>
> In un ambiente di produzione, dovrai configurare il database in base alle tue esigenze specifiche.

Creazione di un database MySQL RDS

1. Apri la console di Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Dal selettore di regione (in alto a destra), scegli un Regione AWS. Per poter utilizzare la funzione di connessione automatica nella console EC2, il database e l'istanza EC2 devono trovarsi nella stessa regione.
3. Sul pannello di controllo seleziona Create database (Crea database).
4. Sotto Choose a database creation method (Seleziona metodo di creazione del database), assicurati che Standard create (Creazione standard) sia selezionato. Il selettore VPC non è disponibile, se scegli Easy create (Creazione facile). Per utilizzare la funzione di connessione automatica nella console EC2, assicurati che il database si trovi nello stesso VPC dell'istanza EC2.
5. Sotto Engine options (Opzioni del motore) per Engine type (Tipo di motore) scegli MySQL.
6. Sotto Templates (Modelli), scegli un modello di esempio che soddisfi le tue esigenze. Per questo tutorial scegli il Free tier (Livello gratuito) in modo da creare un database gratuitamente. Tuttavia tieni presente che il piano gratuito è disponibile solo se il tuo account ha meno di 12 mesi. Si applicano altre restrizioni. Puoi saperne di più selezionando il link Info (Informazioni) nel campo Free tier (Livello gratuito).
7. In Settings (Impostazioni), procedere come segue:
   a. Per il DB instance identifier (Identificatore istanze database) inserire un nome per il database. Per questo tutorial, digita **`tutorial-database-1`**.
   b. Per il Master username (Nome utente principale), lascia il nome predefinito, che è **`admin`**.
   c. Come Master password (Password principale) inserisci una password per questo tutorial che riesci a ricordare quindi per Confirm password (Conferma password) inserisci nuovamente la password.
8. In Configurazione dell'istanza, per la classe di istanze DB, lascia il valore predefinito, che è db.t3.micro. Se il tuo account è inferiore a 12 mesi, puoi utilizzare questa classe di database

gratuitamente. Si applicano altre restrizioni. Per ulteriori informazioni, consulta Piano gratuito di AWS.

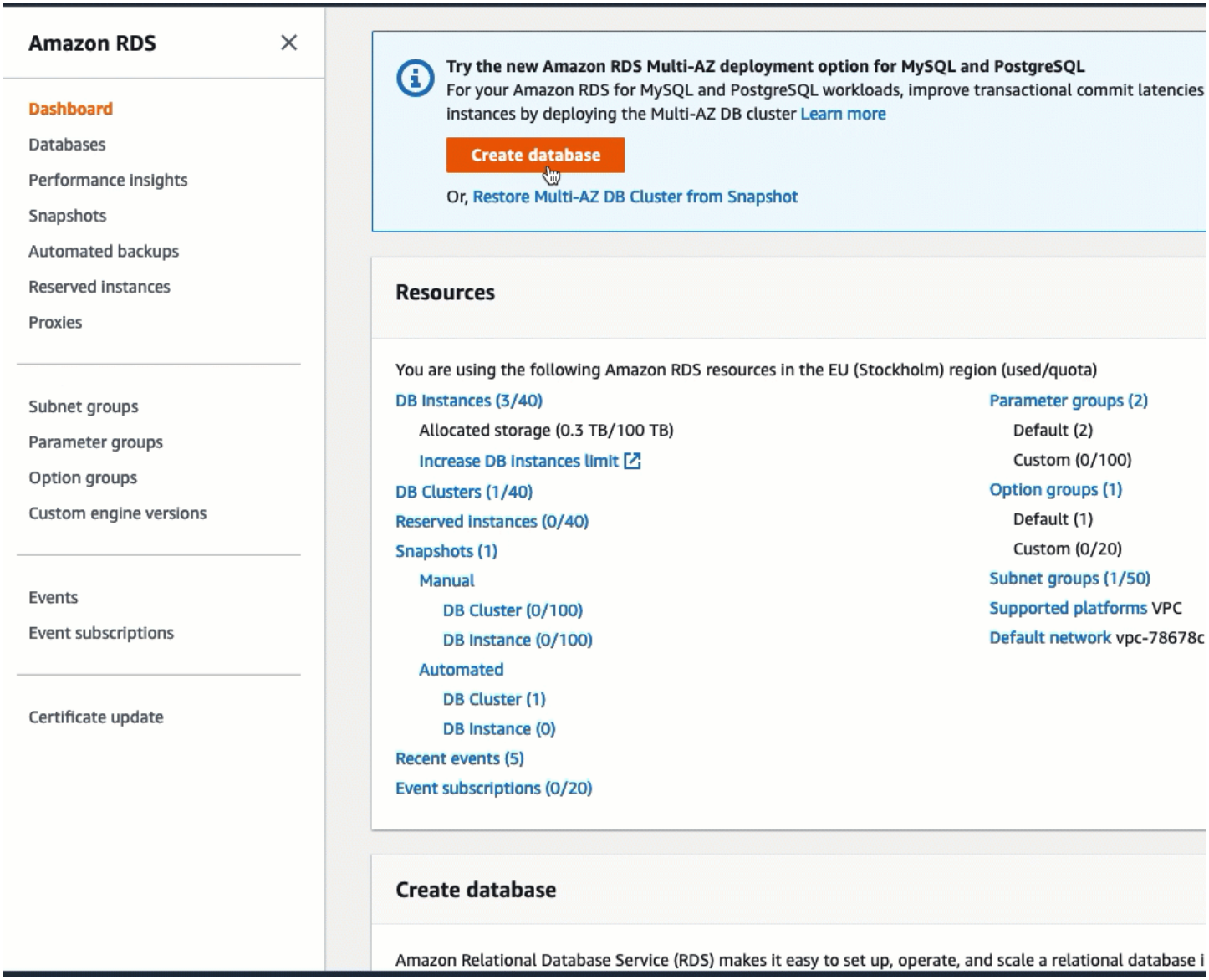
9. Sotto Connectivity (Connettività), per Compute resource (Risorsa di calcolo), scegli Don't connect to an EC2 compute resource (Non connetterti a una risorsa di calcolo EC2) perché connetterai l'istanza EC2 e il database RDS più avanti, nell'Attività 3.

   [Più avanti, nell'Opzione 2 di questo tutorial, proverai la funzione di connessione automatica nella console RDS scegliendo Connect to an EC2 compute resource (Connetti a una risorsa di calcolo EC2).]

10. Per Virtual private cloud (VPC) [Cloud privato virtuale (VPC)] seleziona un VPC. Il VPC deve avere un gruppo di sottorete database. Per utilizzare la funzione di connessione automatica, l'istanza EC2 e il database RDS devono trovarsi nello stesso VPC.
11. Per tutti gli altri campi di questa pagina mantieni i valori predefiniti.
12. Scegliere Crea database.

    Nella schermata Databases (Database) lo Status (Stato) del nuovo database è Creating fino a quando il database non è pronto per l'uso. Quando lo stato diventa Available (Disponibile), puoi connetterti al database. A seconda della classe del database e della quantità di storage, possono trascorrere fino a 20 minuti prima che il nuovo database sia disponibile.

Visualizzazione di un'animazione: creazione di un database RDS



A questo punto puoi eseguire Attività 2: avvio di un'istanza EC2 (opzionale).

Attività 2: avvio di un'istanza EC2 (opzionale)

> **Note**
>
> Il fulcro di questo tutorial non è l'avvio di un'istanza. Se già disponi di un'istanza Amazon EC2 e vorresti utilizzarla in questo tutorial, puoi ignorare questa attività.

Obiettivo dell'attività

L'obiettivo di questa attività è creare un'istanza EC2 in modo da poter completare l'Attività 3 che prevede la configurazione della connessione tra l'istanza EC2 e il database Amazon RDS. Se hai un'istanza EC2 e puoi utilizzarla, puoi saltare questa attività.

> **Important**
>
> Se utilizzi un'istanza EC2 esistente, assicurati che si trovi nello stesso VPC del database RDS in modo da poter utilizzare la funzione di connessione automatica.

Procedura di avvio di un'istanza EC2

Attieniti ai passaggi seguenti per avviare un'istanza EC2 per questo tutorial.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: avvio di un'istanza EC2.

Configurazione di un'istanza EC2

I passaggi di questa attività illustrano la configurazione dell'istanza EC2 come segue:

- nome dell'istanza: **`tutorial-instance-1`**
- AMI: Amazon Linux 2
- tipo di istanza: `t2.micro`
- assegnazione automatica dell'IP pubblico: abilitata
- gruppo di sicurezza con le tre regole seguenti:
  - Consenti SSH dal tuo indirizzo IP
  - Consenti il traffico HTTPS da qualsiasi luogo
  - Consenti il traffico HTTP da qualsiasi luogo

> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

Per avviare un'istanza EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal selettore di regione (in alto a destra), scegli un Regione AWS. Per poter utilizzare la funzione di connessione automatica nella console EC2, l'istanza e il database RDS devono trovarsi nella stessa regione.
3. Dal dashboard EC2, scegli Avvia istanza.
4. Sotto Name and tags (Nome e tag), per Name (Nome) inserisci un nome per identificare l'istanza. Per questo tutorial inserisci l'istanza **`tutorial-instance-1`**. Sebbene il nome dell'istanza non sia obbligatorio, quando selezioni l'istanza nella console EC2, questo ti aiuterà a identificarla facilmente.
5. Sotto Application and OS Images (Applicazioni e immagini del sistema operativo), scegli un'AMI che soddisfi le esigenze del tuo server web. Questo tutorial utilizza Amazon Linux 2.
6. Sotto Instance type(Tipo di istanza), per Instance type (Tipo di istanza), seleziona un tipo di istanza che soddisfi le esigenze del tuo server web. In questo tutorial si utilizza `t2.micro`.

   > **Note**
   >
   > Puoi utilizzare Amazon EC2 con il piano gratuito a condizione che il tuo AWS account abbia meno di 12 mesi e che tu scelga un tipo di `t2.micro` istanza (o nelle regioni `t3.micro` in cui non `t2.micro` è disponibile).

7. Sotto Key pair (login) [Coppia di chiavi (login)], per Key pair name (Nome della coppia di chiavi) scegli la tua coppia di chiavi.
8. Sotto Network settings (Impostazioni di rete) effettua le seguenti operazioni:

   a. Per Nework (Rete) e Subnet (Sottorete), se non hai apportato modifiche al VPC o alle sottoreti predefiniti, puoi mantenere le impostazioni predefinite.

      Se hai apportato modifiche al tuo VPC o alle sottoreti predefiniti, controlla quanto segue:

      i. Per utilizzare la funzione di connessione automatica, l'istanza deve trovarsi nello stesso VPC del database RDS. Per impostazione predefinita hai a disposizione un solo VPC.

      ii. Il VPC in cui stai avviando l'istanza deve avere un gateway Internet collegato ad esso in modo da poter accedere al tuo server web da Internet. Il tuo VPC predefinito viene configurato automaticamente con un gateway Internet.

iii. Per assicurarti che l'istanza riceva un indirizzo IP pubblico, in Auto-assign public IP (Assegnazione automatica IP pubblico) verifica che l'opzione Enable (Abilita) sia selezionata. Se è selezionato Disable (Disabilita), scegli Edit (Modifica) a destra di Network settings (Impostazioni di rete); quindi, per Auto-assign public IP (Assegnazione automatica IP pubblico), scegli Enable (Abilita).

b. Per connettersi all'istanza tramite SSH, è necessaria una regola del gruppo di sicurezza che autorizzi il traffico SSH (Linux) o RDP (Windows) dall'indirizzo IPv4 pubblico del computer. Per impostazione predefinita, quando si avvia un'istanza, viene creato un nuovo gruppo di sicurezza con una regola che consente il traffico SSH in entrata da qualsiasi luogo.

   Per assicurarti che solo il tuo indirizzo IP possa connettersi alla tua istanza, sotto Firewall (security groups) [Firewall (gruppi di sicurezza)], dall'elenco a discesa accanto al casella di controllo Allow SSH traffic from (Consenti traffico SSH da), scegli My IP (Il mio IP).

c. Per consentire il traffico da Internet alla tua istanza, seleziona le caselle di controllo seguenti:

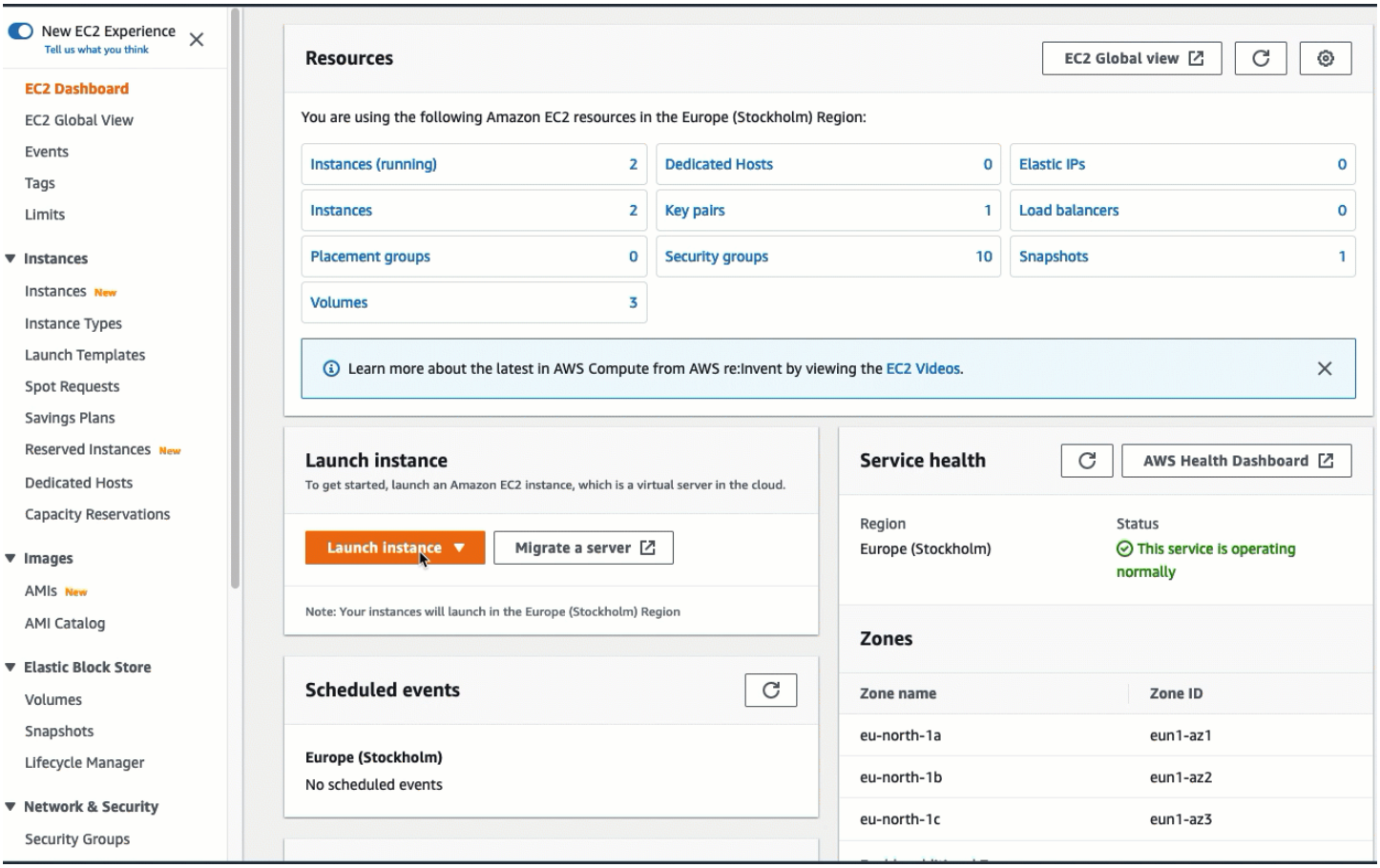
   - Allow HTTPs traffic from the internet (Autorizzare il traffico HTTPS da Internet)
   - Allow HTTP traffic from the internet (Autorizzare il traffico HTTP da Internet)

9. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).
10. Tieni aperta la pagina di conferma. Ne avrai bisogno per eseguire l'operazione successiva, quando connetti automaticamente l'istanza al database.

    Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

Per ulteriori informazioni sull'avvio di un'istanza, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Visualizzazione di un'animazione: avvio di un'istanza EC2



A questo punto puoi eseguire Attività 3: connessione automatica dell'istanza EC2 al database RDS.

Attività 3: connessione automatica dell'istanza EC2 al database RDS

Obiettivo dell'attività

L'obiettivo di questa attività è utilizzare la funzione di connessione automatica nella console EC2 per configurare automaticamente la connessione tra l'istanza EC2 e il database RDS.

Procedura per connettere l'istanza EC2 e il database RDS

Attieniti ai passaggi seguenti per connettere l'istanza EC2 e il database RDS utilizzando la funzionalità automatica nella console EC2.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: connessione automatica di un'istanza EC2 appena avviata a un database RDS.

Connessione automatica di un'istanza EC2 esistente a un database RDS utilizzando la console EC2

1. Nella pagina di conferma dell'avvenuto avvio dell'istanza (dovrebbe essere aperta dall'attività precedente), scegli Connect an RDS database (Connetti un database RDS).

   Se hai chiuso la pagina di conferma, segui questi passaggi:

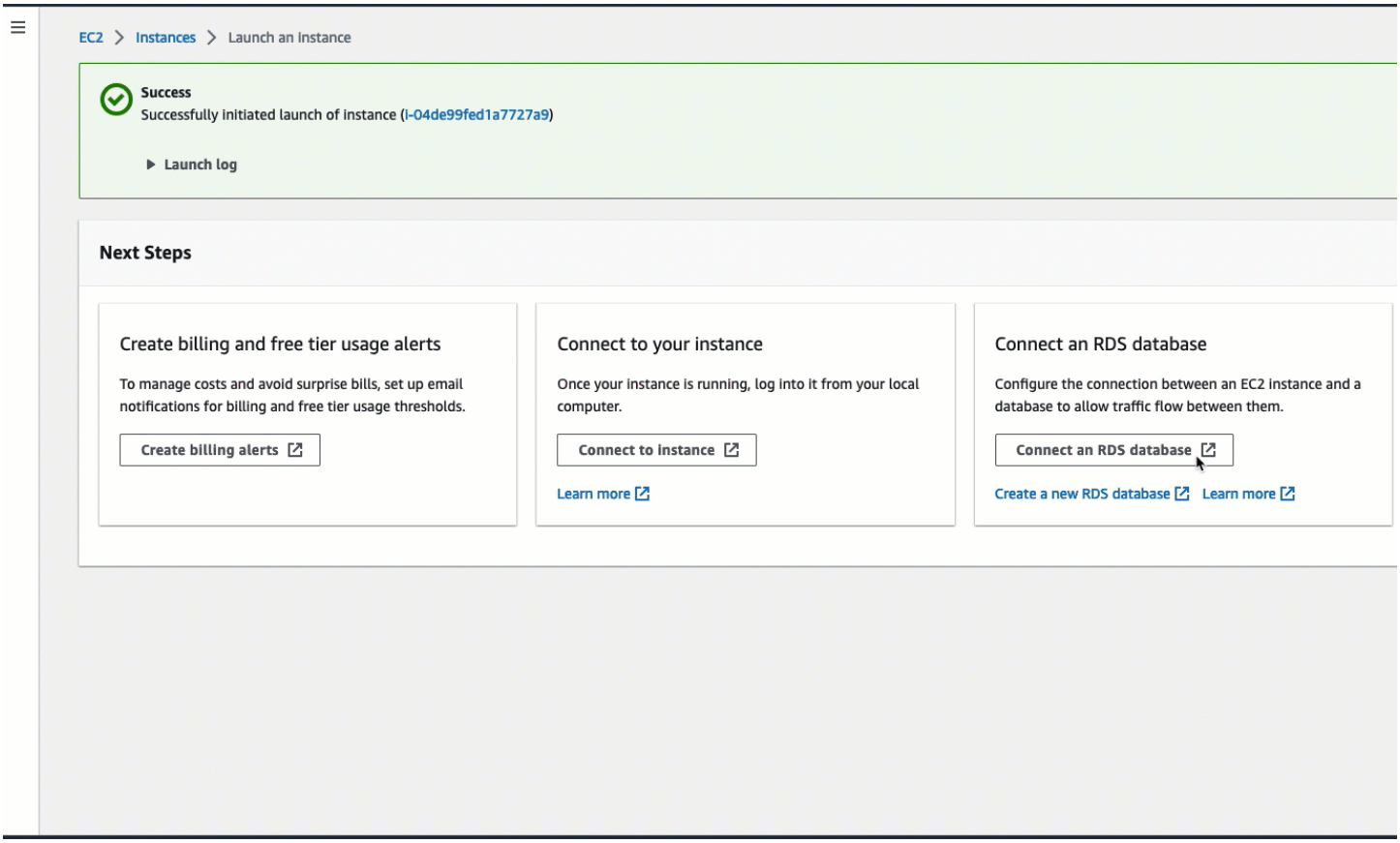
   a. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   b. Nel riquadro di navigazione, seleziona Istanze.
   c. Seleziona l'istanza EC2 che hai appena creato, quindi scegli Actions (Azioni), Networking (Rete), Connect RDS database (Connetti database RDS).

      Se Connect RDS database (Connetti database RDS) non è disponibile, controlla che l'istanza EC2 sia nello stato Running (In esecuzione).
2. Per il Database role (Ruolo del database), scegli Instance (Istanza). In questo caso Instance (Istanza) si riferisce all'istanza del database.
3. Per il RDS database (Database RDS), scegli il database RDS che hai creato nell'Attività 1.

   > **Note**
   >
   > L'istanza EC2 e il database RDS devono trovarsi nello stesso VPC per connettersi tra di loro.

4. Scegli Connetti.

Visualizzazione di un'animazione: connessione automatica di un'istanza EC2 appena avviata a un database RDS



A questo punto puoi eseguire Attività 4: verifica della configurazione della connessione.

Attività 4: verifica della configurazione della connessione

Obiettivo dell'attività

L'obiettivo di questa attività è verificare che i due gruppi di sicurezza siano stati creati e assegnati all'istanza e al database.

Quando utilizzi la funzione di connessione automatica nella console EC2 o nella console RDS per configurare la connettività, i gruppi di sicurezza vengono creati e assegnati automaticamente all'istanza e al database RDS, come segue:

- Il gruppo di sicurezza rds-ec2-***x*** viene creato e aggiunto all'istanza EC2. Una regola in uscita considera il gruppo di sicurezza ec2-rds-***x*** come origine. Ciò consente al traffico proveniente dall'istanza EC2 con il gruppo di sicurezza ec2-rds-***x*** di raggiungere il database RDS.

- Il gruppo di sicurezza ec2-rds-*x* viene creato e aggiunto all'istanza EC2. Una regola in uscita che considera il gruppo di sicurezza rds-ec2-*x* come destinazione. Ciò consente al traffico proveniente dall'istanza EC2 di raggiungere il database RDS con il gruppo di sicurezza ***rds-ec2-x***.

Passaggi per verificare la configurazione della connessione

Attieniti ai passaggi seguenti per verificare la configurazione della connessione.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: verifica della configurazione della connessione.

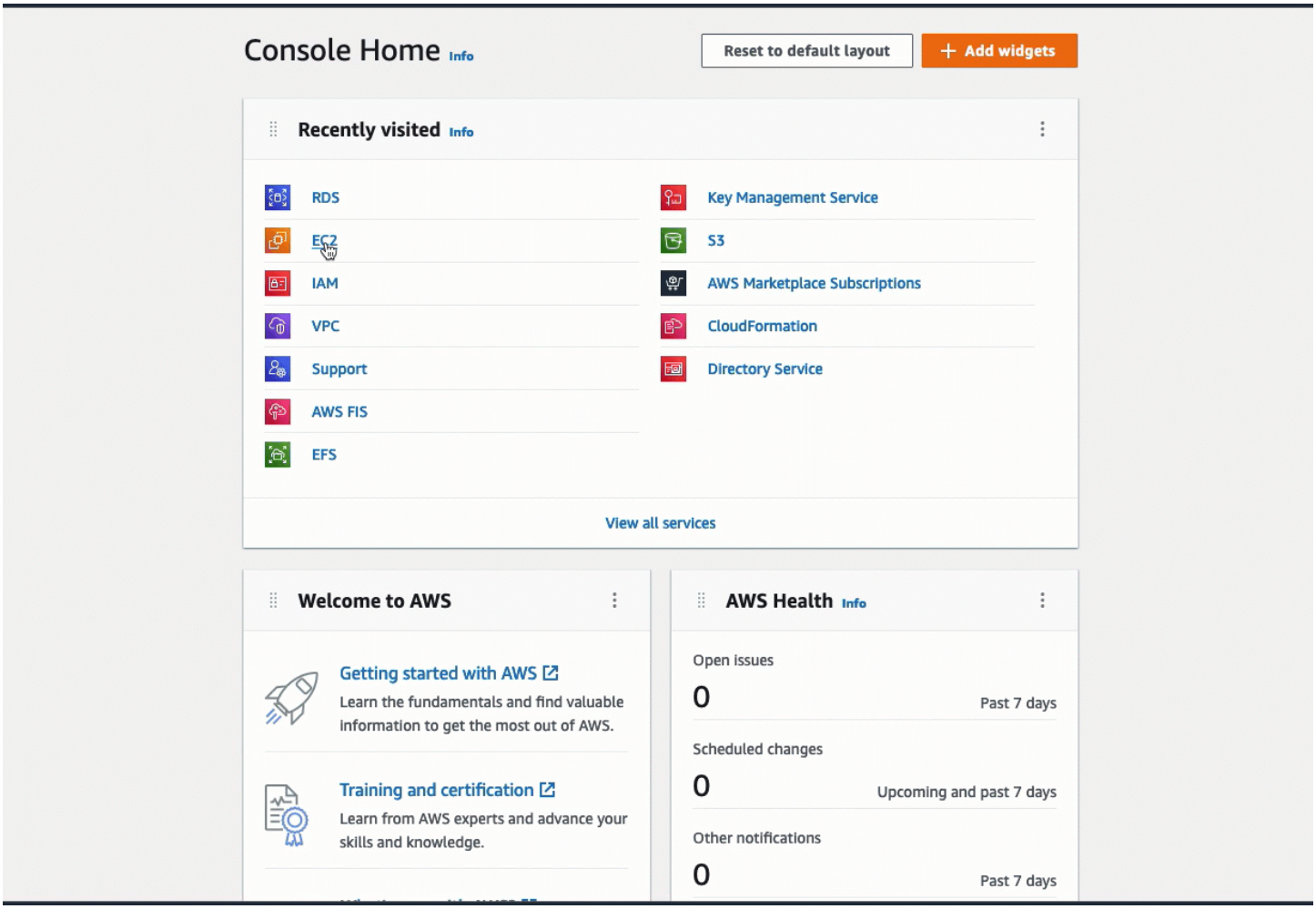
Verifica della configurazione della connessione tramite la console

1. Apri la console di Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Nel riquadro di navigazione scegli Databases (Database).
3. Scegli il database RDS creato per questo tutorial.
4. Nella scheda Connectivity & security (Connettività e sicurezza), sotto Security (Sicurezza), VPC security groups (Gruppi di sicurezza VPC), verifica che sia visualizzato un gruppo di sicurezza denominato rds-ec2-*x*.
5. Scegli il gruppo di sicurezza rds-ec2-*x*. Si apre la schermata Security Groups (Gruppi di sicurezza) nella console EC2.
6. Scegli il gruppo di sicurezza rds-ec2-*x* per aprirlo.
7. Selezionare la scheda Inbound Rules (Regole in entrata).
8. Verifica che esista la seguente regola del gruppo di sicurezza, come illustrato di seguito:
   - Tipo: MYSQL/Aurora
   - Intervallo porte: 3306
   - Fonte: ***sg-0987654321example*** / ec2-rds-*x* (questo è il gruppo di sicurezza assegnato all'istanza EC2 che hai verificato nei passaggi precedenti).
   - Descrizione: Regola per consentire le connessioni dalle istanze EC2 con ***sg-1234567890example*** collegato
9. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
10. Nel riquadro di navigazione, seleziona Istanze.
11. Scegli l'istanza EC2 che hai selezionato per connetterti al database RDS nell'operazione precedente e scegli la scheda Security (Sicurezza).

12. In Security details (Dettagli di sicurezza), Security groups (Gruppi di sicurezza), verifica che nell'elenco sia presente un gruppo di sicurezza denominato ec2-rds-*x*. *x* è un numero.
13. Scegli il gruppo di sicurezza ec2-rds-*x* per aprirlo.
14. Scegli la scheda Outbound rules (Regole in uscita).
15. Verifica che esista la seguente regola del gruppo di sicurezza, come illustrato di seguito:
    - Tipo: MYSQL/Aurora
    - Intervallo porte: 3306
    - Destinazione: *sg-1234567890example* / rds-ec2-*x*
    - Descrizione: Regola per consentire le connessioni a **database-tutorial** da qualsiasi istanza a cui è collegato questo gruppo di sicurezza

Verificando che questi gruppi di sicurezza e le regole dei gruppi di sicurezza esistano e che siano assegnati al database RDS e all'istanza EC2 come descritto in questa procedura, puoi verificare che la connessione sia stata configurata automaticamente utilizzando la funzione di connessione automatica.

Visualizzazione di un'animazione: verifica della configurazione della connessione



Hai completato l'Opzione 1 di questo tutorial. Ora puoi completare l'Opzione 2, che spiega come usare la console RDS per connettere automaticamente un'istanza EC2 a un database RDS, oppure puoi completare l'Opzione 3, che spiega come configurare manualmente i gruppi di sicurezza creati automaticamente nell'Opzione 1.

Opzione 2: connessione automatica dell'istanza EC2 al database RDS utilizzando la console RDS

Obiettivo

L'obiettivo dell'opzione 2 è comprendere la funzionalità di connessione automatica nella console RDS che prevede la configurazione automatica della connessione tra l'istanza EC2 e il database RDS in modo da consentire il traffico dall'istanza EC2 al database RDS. Nell'opzione 3 imparerai come configurare manualmente la connessione.

Prima di iniziare

Per completare questo tutorial, avrai bisogno di quanto segue:

- Un'istanza EC2 nello stesso VPC del database RDS. Puoi utilizzare un'istanza EC2 esistente o seguire i passaggi illustrati nell'Attività 1 per creare una nuova istanza.
- Autorizzazioni per effettuare le seguenti operazioni:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Attività per completare l'opzione 2

- Attività 1: avvio di un'istanza EC2 (opzionale)
- Attività 2: creazione di un database RDS e connessione automatica di questo all'istanza EC2
- Attività 3: verifica della configurazione di connessione

Attività 1: avvio di un'istanza EC2 (opzionale)

> **Note**
>
> Il fulcro di questo tutorial non è l'avvio di un'istanza. Se già disponi di un'istanza Amazon EC2 e vorresti utilizzarla in questo tutorial, puoi ignorare questa attività.

Obiettivo dell'attività

L'obiettivo di questa attività è avviare un'istanza EC2 in modo da poter completare l'Attività 2 che prevede la configurazione della connessione tra l'istanza EC2 e il database Amazon RDS. Se hai un'istanza EC2 e puoi utilizzarla, puoi saltare questa attività.

Procedura di avvio di un'istanza EC2

Attieniti ai passaggi seguenti per avviare un'istanza EC2 per questo tutorial.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: avvio di un'istanza EC2.

Configurazione di un'istanza EC2

I passaggi di questa attività illustrano la configurazione dell'istanza EC2 come segue:

- nome dell'istanza: **`tutorial-instance-2`**
- AMI: Amazon Linux 2
- tipo di istanza: `t2.micro`
- assegnazione automatica dell'IP pubblico: abilitata
- gruppo di sicurezza con le tre regole seguenti:
  - Consenti SSH dal tuo indirizzo IP
  - Consenti il traffico HTTPS da qualsiasi luogo
  - Consenti il traffico HTTP da qualsiasi luogo

> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

Per avviare un'istanza EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal dashboard EC2, scegli Avvia istanza.
3. Sotto Name and tags (Nome e tag), per Name (Nome) inserisci un nome per identificare l'istanza. Per questo tutorial inserisci l'istanza **`tutorial-instance-2`**. Sebbene il nome

dell'istanza non sia obbligatorio, quando selezioni l'istanza nella console RDS, questo ti aiuterà a identificarla facilmente.

4. Sotto Application and OS Images (Applicazioni e immagini del sistema operativo), scegli un'AMI che soddisfi le esigenze del tuo server web. Questo tutorial utilizza Amazon Linux.
5. Sotto Instance type(Tipo di istanza), per Instance type (Tipo di istanza), seleziona un tipo di istanza che soddisfi le esigenze del tuo server web. In questo tutorial si utilizza `t2.micro`.

   > **Note**
   >
   > Puoi utilizzare Amazon EC2 con il piano gratuito a condizione che il tuo AWS account abbia meno di 12 mesi e che tu scelga un tipo di `t2.micro` istanza (o nelle regioni `t3.micro` in cui non `t2.micro` è disponibile).

6. Sotto Key pair (login) [Coppia di chiavi (login)], per Key pair name (Nome della coppia di chiavi) scegli la tua coppia di chiavi.
7. Sotto Network settings (Impostazioni di rete) effettua le seguenti operazioni:

   a. Per Nework (Rete) e Subnet (Sottorete), se non hai apportato modifiche al VPC o alle sottoreti predefiniti, puoi mantenere le impostazioni predefinite.

      Se hai apportato modifiche al tuo VPC o alle sottoreti predefiniti, controlla quanto segue:

      i. Per utilizzare la configurazione di connessione automatica, l'istanza deve trovarsi nello stesso VPC del database RDS. Per impostazione predefinita hai a disposizione un solo VPC.

      ii. Il VPC in cui stai avviando l'istanza deve avere un gateway Internet collegato ad esso in modo da poter accedere al tuo server web da Internet. Il tuo VPC predefinito viene configurato automaticamente con un gateway Internet.

      iii. Per assicurarti che l'istanza riceva un indirizzo IP pubblico, in Auto-assign public IP (Assegnazione automatica IP pubblico) verifica che l'opzione Enable (Abilita) sia selezionata. Se è selezionato Disable (Disabilita), scegli Edit (Modifica) a destra di Network settings (Impostazioni di rete); quindi, per Auto-assign public IP (Assegnazione automatica IP pubblico), scegli Enable (Abilita).

   b. Per connettersi all'istanza tramite SSH, è necessaria una regola del gruppo di sicurezza che autorizzi il traffico SSH (Linux) o RDP (Windows) dall'indirizzo IPv4 pubblico del computer. Per impostazione predefinita, quando si avvia un'istanza, viene creato un nuovo gruppo di sicurezza con una regola che consente il traffico SSH in entrata da qualsiasi luogo.

Per assicurarti che solo il tuo indirizzo IP possa connettersi alla tua istanza, sotto Firewall (security groups) [Firewall (gruppi di sicurezza)], dall'elenco a discesa accanto al casella di controllo Allow SSH traffic from (Consenti traffico SSH da), scegli My IP (Il mio IP).

c. Per consentire il traffico da Internet alla tua istanza, seleziona le caselle di controllo seguenti:

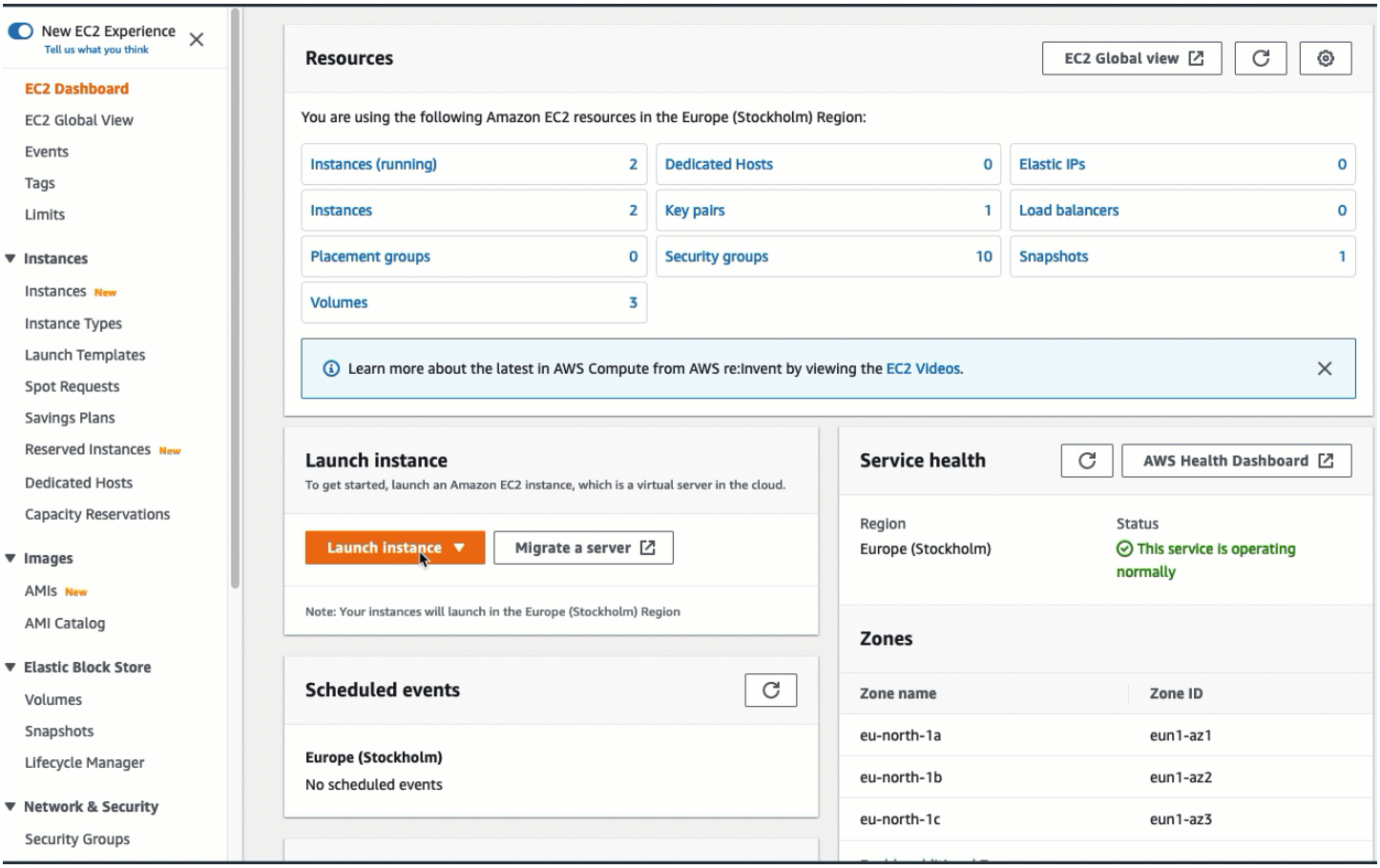
   - Allow HTTPs traffic from the internet (Autorizzare il traffico HTTPS da Internet)
   - Allow HTTP traffic from the internet (Autorizzare il traffico HTTP da Internet)

8. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).
9. Scegli View Instances (Visualizza istanze) per chiudere la pagina di conferma e tornare alla console. La tua istanza sarà prima in uno stato `pending` e poi passerà allo stato `running`.

   Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

Per ulteriori informazioni sull'avvio di un'istanza, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Visualizzazione di un'animazione: avvio di un'istanza EC2



A questo punto puoi eseguire Attività 2: creazione di un database RDS e connessione automatica di questo all'istanza EC2.

Attività 2: creazione di un database RDS e connessione automatica di questo all'istanza EC2

Obiettivo dell'attività

L'obiettivo di questa attività è creare un database RDS e usare la funzione di connessione automatica nella console RDS per configurare automaticamente la connessione tra l'istanza EC2 e il database RDS.

Procedura per creare un database RDS

Attieniti ai passaggi seguenti per creare un database RDS e connetterlo all'istanza EC2 utilizzando la funzionalità automatica nella console RDS.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: creazione un database RDS e connessione automatica di questo a un'istanza EC2.

Configurazione dell'istanza database

I passaggi di questa attività illustrano la configurazione dell'istanza database come segue:

- Tipo di motore: MySQL
- Modello: livello gratuito
- DB Instance Identifier (Identificatore istanze database): **`tutorial-database`**
- DB instance class (Classe istanza database): `db.t3.micro`

> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

Creare un database RDS e connetterlo automaticamente a un'istanza EC2

1. Apri la console di Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Dal selettore della regione (in alto a destra), scegli l'istanza EC2 Regione AWS in cui hai creato l'istanza EC2. L'istanza EC2 e il database RDS devono trovarsi nella stessa regione.
3. Sul pannello di controllo seleziona Create database (Crea database).
4. Sotto Choose a database creation method (Seleziona metodo di creazione del database), assicurati che Standard create (Creazione standard) sia selezionato. La funzione di connessione automatica non è disponibile, se scegli Easy create (Creazione facile).
5. Sotto Engine options (Opzioni del motore) per Engine type (Tipo di motore) scegli MySQL.
6. Sotto Templates (Modelli), scegli un modello di esempio che soddisfi le tue esigenze. Per questo tutorial scegli il Free tier (Livello gratuito) in modo da creare un database RDS gratuitamente. Tuttavia tieni presente che il piano gratuito è disponibile solo se il tuo account ha meno di 12 mesi. Si applicano altre restrizioni. Puoi saperne di più selezionando il link Info (Informazioni) nel campo Free tier (Livello gratuito).
7. In Settings (Impostazioni), procedere come segue:

    a. Per il DB instance identifier (Identificatore istanze database) inserire un nome per il database. Per questo tutorial, digita **`tutorial-database`**.

    b. Per il Master username (Nome utente principale), lascia il nome predefinito, che è **`admin`**.

c. Come Master password (Password principale) inserisci una password per questo tutorial che riesci a ricordare quindi per Confirm password (Conferma password) inserisci nuovamente la password.

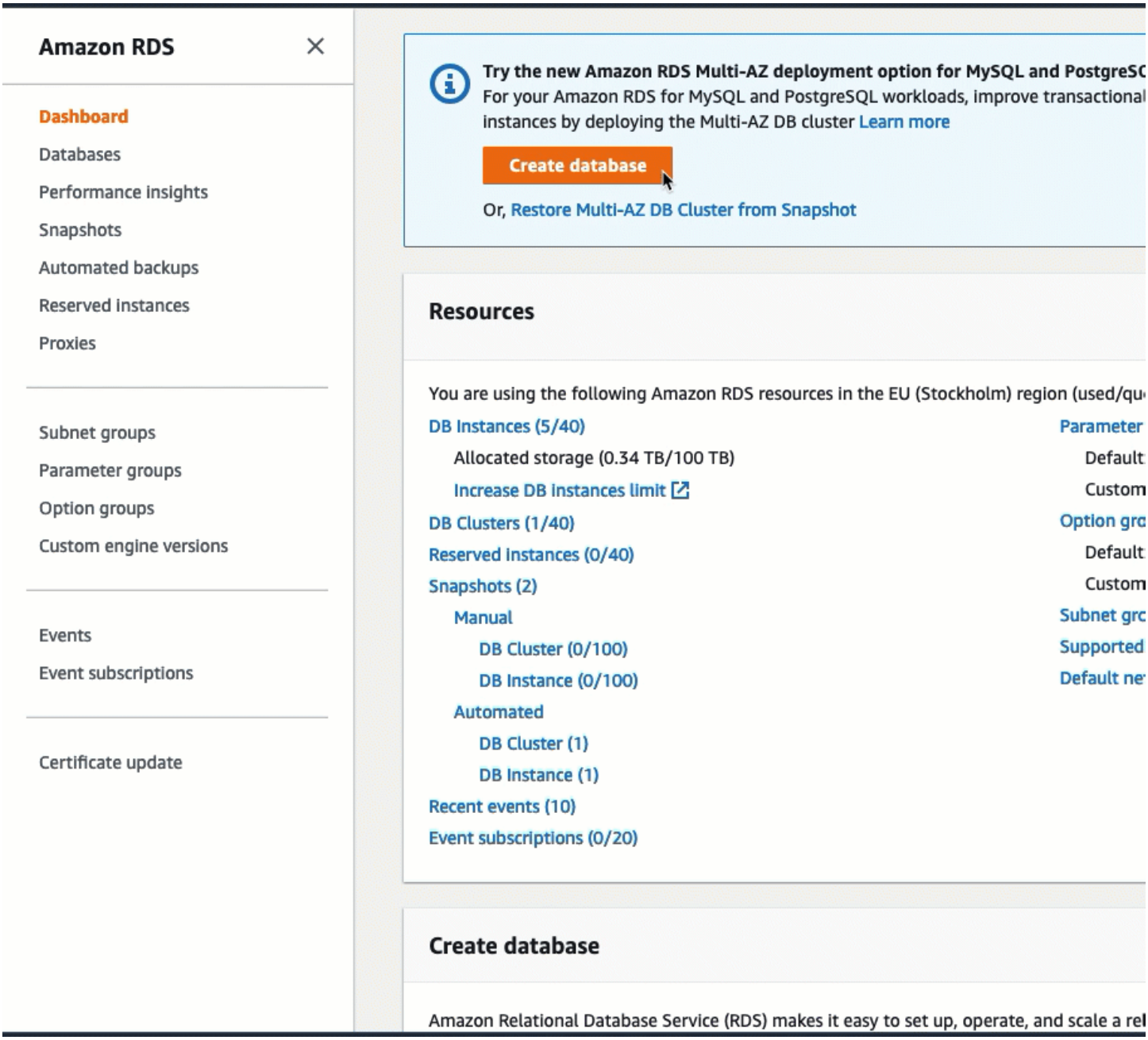
8. In Configurazione dell'istanza, per la classe di istanza DB, lascia il valore predefinito, che è db.t3.micro. Se il tuo account ha meno di 12 mesi, puoi utilizzare questa istanza gratuitamente. Si applicano altre restrizioni. Per ulteriori informazioni, consulta Piano gratuito di AWS.
9. Sotto Connectivity (Connettività), per Compute resource (Risorsa di calcolo), scegli Connect to an EC2 compute resource (Connetti a una risorsa di calcolo EC2). Questa è la funzione di connessione automatica della console RDS.
10. Per EC2 Instance (Istanza EC2) scegli il nome dell'istanza EC2 a cui vuoi connetterti. Ai fini di questo tutorial, puoi scegliere l'istanza che hai creato nell'attività precedente, che hai denominato **`tutorial-instance`**, oppure scegliere un'altra istanza esistente. Se l'istanza non è visualizzata nell'elenco, scegli l'icona di aggiornamento a destra di Connectivity (Connettività).

    Quando utilizzi la funzione di connessione automatica, un gruppo di sicurezza viene aggiunto a questa istanza EC2 e un altro gruppo di sicurezza viene aggiunto al database RDS. I gruppi di sicurezza sono configurati automaticamente per consentire il traffico tra l'istanza EC2 e il database RDS. Nella prossima attività, verificherai che i gruppi di sicurezza siano stati creati e assegnati all'istanza EC2 e al database RDS.
11. Scegliere Crea database.

    Nella schermata Databases (Database) lo Status (Stato) del nuovo database è Creating fino a quando il database non è pronto per l'uso. Quando lo stato diventa Available (Disponibile), puoi connetterti al database. A seconda della classe del database e della quantità di storage, possono trascorrere fino a 20 minuti prima che il nuovo database sia disponibile.

Per ulteriori informazioni, consulta Configurare la connettività di rete automatica con un'istanza EC2 nella Guida per l'utente di Amazon RDS.

Visualizzazione di un'animazione: creazione un database RDS e connessione automatica di questo a un'istanza EC2



A questo punto puoi eseguire Attività 3: verifica della configurazione di connessione.

Attività 3: verifica della configurazione di connessione

Obiettivo dell'attività

L'obiettivo di questa attività è verificare che i due gruppi di sicurezza siano stati creati e assegnati all'istanza e al database.

Quando utilizzi la funzione di connessione automatica nella console RDS per configurare la connettività, i gruppi di sicurezza vengono creati e assegnati automaticamente all'istanza e al database, come segue:

- Il gruppo di sicurezza rds-ec2-*x* viene creato e aggiunto all'istanza EC2. Una regola in uscita considera il gruppo di sicurezza ec2-rds-*x* come origine. Ciò consente al traffico proveniente dall'istanza EC2 con il gruppo di sicurezza ec2-rds-*x* di raggiungere il database RDS.
- Il gruppo di sicurezza ec2-rds-*x* viene creato e aggiunto all'istanza EC2. Una regola in uscita che considera il gruppo di sicurezza rds-ec2-*x* come destinazione. Ciò consente al traffico proveniente dall'istanza EC2 di raggiungere il database RDS con il gruppo di sicurezza ***rds-ec2-x***.

Passaggi per verificare la configurazione della connessione

Attieniti ai passaggi seguenti per verificare la configurazione della connessione.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: verifica della configurazione della connessione.

Verifica della configurazione della connessione tramite la console

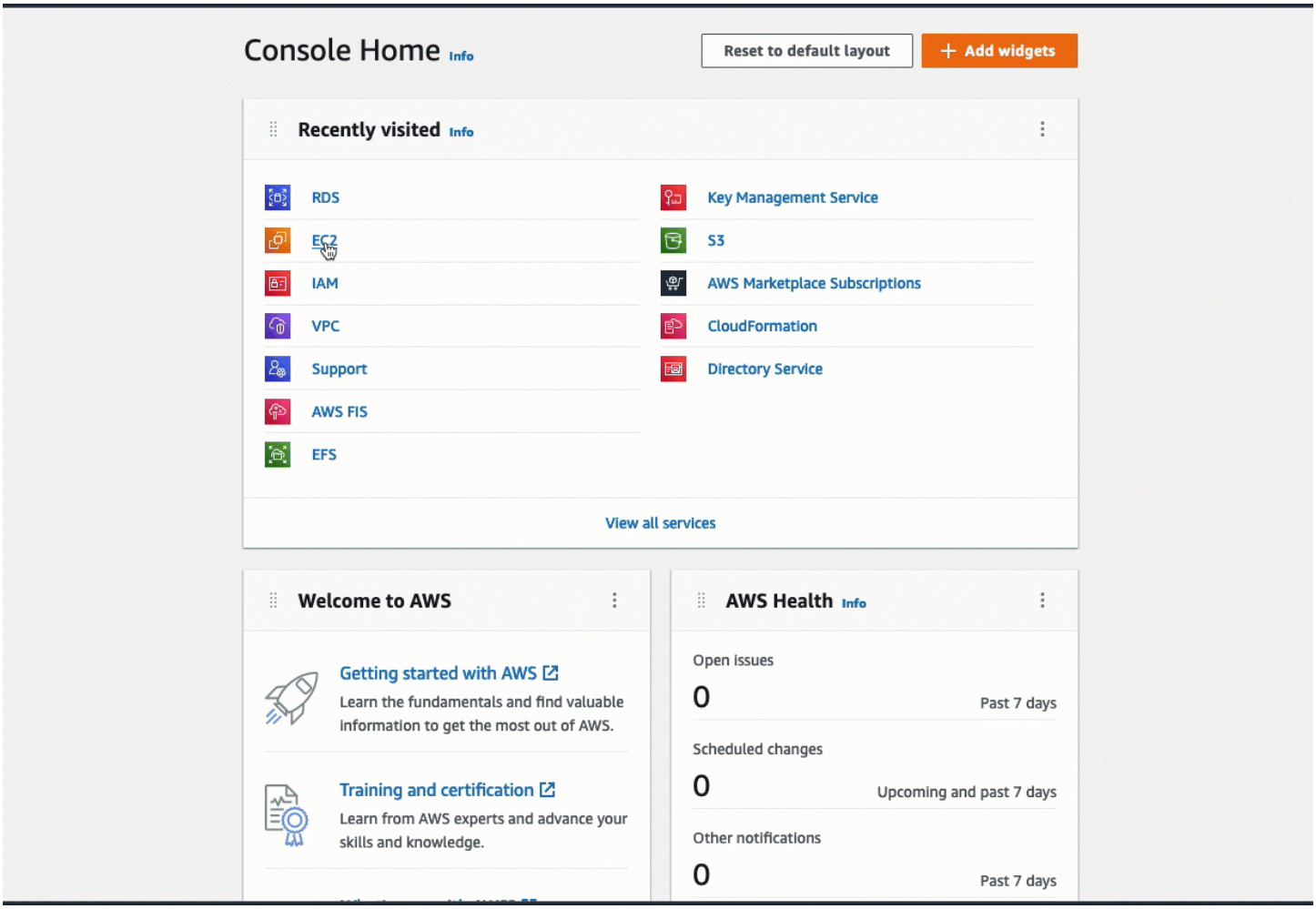
1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Scegli l'istanza EC2 che hai selezionato per connetterti al database RDS nell'operazione precedente e scegli la scheda Security (Sicurezza).
4. In Security details (Dettagli di sicurezza), Security groups (Gruppi di sicurezza), verifica che nell'elenco sia presente un gruppo di sicurezza denominato ec2-rds-*x*. *x* è un numero.
5. Scegli il gruppo di sicurezza ec2-rds-*x* per aprirlo.
6. Scegli la scheda Outbound rules (Regole in uscita).
7. Verifica che esista la seguente regola del gruppo di sicurezza, come illustrato di seguito:
   - Tipo: MYSQL/Aurora
   - Intervallo porte: 3306
   - Destinazione: ***sg-1234567890example*** / rds-ec2-*x*
   - Descrizione: Regola per consentire le connessioni a **`database-tutorial`** da qualsiasi istanza a cui è collegato questo gruppo di sicurezza
8. Apri la console di Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.

9. Nel riquadro di navigazione scegli Databases (Database).
10. Scegli il database RDS creato per questo tutorial.
11. Nella scheda Connectivity & security (Connettività e sicurezza), sotto Security (Sicurezza), VPC security groups (Gruppi di sicurezza VPC), verifica che sia visualizzato un gruppo di sicurezza denominato rds-ec2-***x***.
12. Scegli il gruppo di sicurezza rds-ec2-***x***. Si apre la schermata Security Groups (Gruppi di sicurezza) nella console EC2.
13. Scegli il gruppo di sicurezza rds-ec2-***x*** per aprirlo.
14. Selezionare la scheda Inbound Rules (Regole in entrata).
15. Verifica che esista la seguente regola del gruppo di sicurezza, come illustrato di seguito:

    - Tipo: MYSQL/Aurora
    - Intervallo porte: 3306
    - Fonte: ***sg-0987654321example*** / ec2-rds-***x*** (questo è il gruppo di sicurezza assegnato all'istanza EC2 che hai verificato nei passaggi precedenti).
    - Descrizione: Regola per consentire le connessioni dalle istanze EC2 con ***sg-1234567890example*** collegato

    Verificando che questi gruppi di sicurezza e le regole dei gruppi di sicurezza esistano e che siano assegnati all'istanza EC2 e al database RDS come descritto in questa procedura, puoi verificare che la connessione sia stata configurata automaticamente utilizzando la funzione di connessione automatica.

Visualizzazione di un'animazione: verifica della configurazione della connessione



Hai completato l'Opzione 2 di questo tutorial. Ora puoi completare l'Opzione 3, che ti spiega come configurare manualmente i gruppi di sicurezza creati automaticamente nell'Opzione 2.

Opzione 3: connessione manuale dell'istanza EC2 al database RDS imitando la funzione di connessione automatica

Obiettivo

L'obiettivo dell'Opzione 3 è imparare a configurare manualmente la connessione tra un'istanza EC2 e un database RDS riproducendo manualmente la configurazione della funzione di connessione automatica.

Prima di iniziare

Per completare questo tutorial, avrai bisogno di quanto segue:

- Un'istanza EC2 nello stesso VPC del database RDS. Puoi utilizzare un'istanza EC2 esistente o seguire i passaggi illustrati nell'Attività 1 per creare una nuova istanza.
- un database RDS nello stesso VPC dell'istanza EC2. Puoi utilizzare un database RDS esistente o seguire i passaggi illustrati nell'Attività 2 per creare un nuovo database.
- Autorizzazioni per effettuare le seguenti operazioni. Se hai completato l'Opzione 1 di questo tutorial, disponi già di queste autorizzazioni.
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Attività per completare l'opzione 3

- Attività 1: avvio di un'istanza EC2 (opzionale)
- Attività 2: creazione di un database RDS (opzionale)
- Attività 3: connessione manuale dell'istanza EC2 al database RDS creando gruppi di sicurezza e assegnandoli alle istanze

Attività 1: avvio di un'istanza EC2 (opzionale)

> **Note**
>
> Il fulcro di questo tutorial non è l'avvio di un'istanza. Se già disponi di un'istanza Amazon EC2 e vorresti utilizzarla in questo tutorial, puoi ignorare questa attività.

Obiettivo dell'attività

L'obiettivo di questa attività è creare un'istanza EC2 in modo da poter completare l'Attività 3 che prevede la configurazione della connessione tra l'istanza EC2 e il database Amazon RDS.

Procedura di avvio di un'istanza EC2

Attieniti ai passaggi seguenti per avviare un'istanza EC2 per questo tutorial.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: avvio di un'istanza EC2.

Configurazione di un'istanza EC2

I passaggi di questa attività illustrano la configurazione dell'istanza EC2 come segue:

- nome dell'istanza: **`tutorial-instance`**
- AMI: Amazon Linux 2
- tipo di istanza: `t2.micro`
- assegnazione automatica dell'IP pubblico: abilitata
- gruppo di sicurezza con le tre regole seguenti:
  - Consenti SSH dal tuo indirizzo IP
  - Consenti il traffico HTTPS da qualsiasi luogo
  - Consenti il traffico HTTP da qualsiasi luogo

> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

Per avviare un'istanza EC2

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal dashboard EC2, scegli Avvia istanza.

3. Sotto Name and tags (Nome e tag), per Name (Nome) inserisci un nome per identificare l'istanza. Per questo tutorial inserisci l'istanza **`tutorial-instance-manual-1`**. Sebbene il nome dell'istanza non sia obbligatorio, questo ti aiuterà a identificarla facilmente.
4. Sotto Application and OS Images (Applicazioni e immagini del sistema operativo), scegli un'AMI che soddisfi le esigenze del tuo server web. Questo tutorial utilizza Amazon Linux.
5. Sotto Instance type(Tipo di istanza), per Instance type (Tipo di istanza), seleziona un tipo di istanza che soddisfi le esigenze del tuo server web. In questo tutorial si utilizza `t2.micro`.

   > **Note**
   >
   > Puoi utilizzare Amazon EC2 con il piano gratuito a condizione che il tuo AWS account abbia meno di 12 mesi e che tu scelga un tipo di `t2.micro` istanza (o nelle regioni `t3.micro` in cui non `t2.micro` è disponibile).

6. Sotto Key pair (login) [Coppia di chiavi (login)], per Key pair name (Nome della coppia di chiavi) scegli la tua coppia di chiavi.
7. Sotto Network settings (Impostazioni di rete) effettua le seguenti operazioni:

   a. Per Nework (Rete) e Subnet (Sottorete), se non hai apportato modifiche al VPC o alle sottoreti predefiniti, puoi mantenere le impostazioni predefinite.

      Se hai apportato modifiche al tuo VPC o alle sottoreti predefiniti, controlla quanto segue:

      i. L'istanza deve trovarsi nella stessa VPC del database RDS. Per impostazione predefinita hai a disposizione un solo VPC.

      ii. Il VPC in cui stai avviando l'istanza deve avere un gateway Internet collegato ad esso in modo da poter accedere al tuo server web da Internet. Il tuo VPC predefinito viene configurato automaticamente con un gateway Internet.

      iii. Per assicurarti che l'istanza riceva un indirizzo IP pubblico, in Auto-assign public IP (Assegnazione automatica IP pubblico) verifica che l'opzione Enable (Abilita) sia selezionata. Se è selezionato Disable (Disabilita), scegli Edit (Modifica) a destra di Network settings (Impostazioni di rete); quindi, per Auto-assign public IP (Assegnazione automatica IP pubblico), scegli Enable (Abilita).

   b. Per connettersi all'istanza tramite SSH, è necessaria una regola del gruppo di sicurezza che autorizzi il traffico SSH (Linux) o RDP (Windows) dall'indirizzo IPv4 pubblico del computer. Per impostazione predefinita, quando si avvia un'istanza, viene creato un nuovo gruppo di sicurezza con una regola che consente il traffico SSH in entrata da qualsiasi luogo.

Per assicurarti che solo il tuo indirizzo IP possa connettersi alla tua istanza, sotto Firewall (security groups) [Firewall (gruppi di sicurezza)], dall'elenco a discesa accanto al casella di controllo Allow SSH traffic from (Consenti traffico SSH da), scegli My IP (Il mio IP).

c. Per consentire il traffico da Internet alla tua istanza, seleziona le caselle di controllo seguenti:

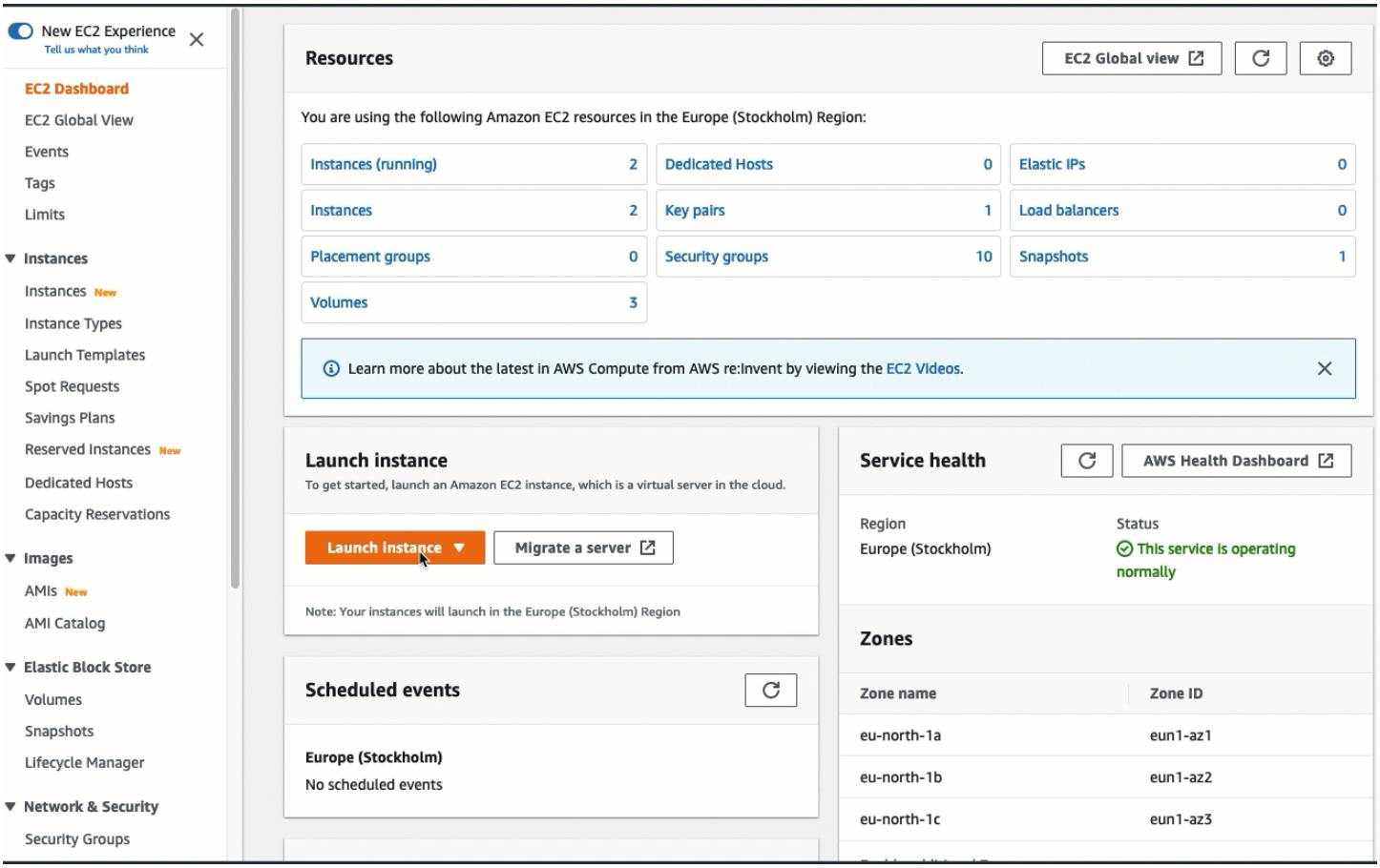
   - Allow HTTPs traffic from the internet (Autorizzare il traffico HTTPS da Internet)
   - Allow HTTP traffic from the internet (Autorizzare il traffico HTTP da Internet)

8. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).
9. Scegli View Instances (Visualizza istanze) per chiudere la pagina di conferma e tornare alla console. La tua istanza sarà prima in uno stato `pending` e poi passerà allo stato `running`.

   Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio delle istanze.

Per ulteriori informazioni sull'avvio di un'istanza, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Visualizzazione di un'animazione: avvio di un'istanza EC2



A questo punto puoi eseguire Attività 2: creazione di un database RDS (opzionale).

Attività 2: creazione di un database RDS (opzionale)

> **Note**
>
> Il fulcro di questa parte del tutorial non è la creazione di un database RDS. Se già disponi di un database RDS e vorresti utilizzarlo in questo tutorial, puoi ignorare questa attività.

Obiettivo dell'attività

L'obiettivo di questa attività è creare un database RDS. Potrai utilizzare questa istanza nel corso dell'Attività 3 quando la connetti all'istanza EC2.

Procedura per creare un database RDS

Attieniti ai passaggi seguenti per creare un database RDS per l'Opzione 3 di questo tutorial.

Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: creazione di un'istanza database.

Configurazione del database RDS

I passaggi di questa attività illustrano la configurazione del database RDS come segue:

- Tipo di motore: MySQL
- Modello: livello gratuito
- DB Instance Identifier (Identificatore istanze database): **`tutorial-database-manual`**
- DB instance class (Classe istanza database): `db.t3.micro`

> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

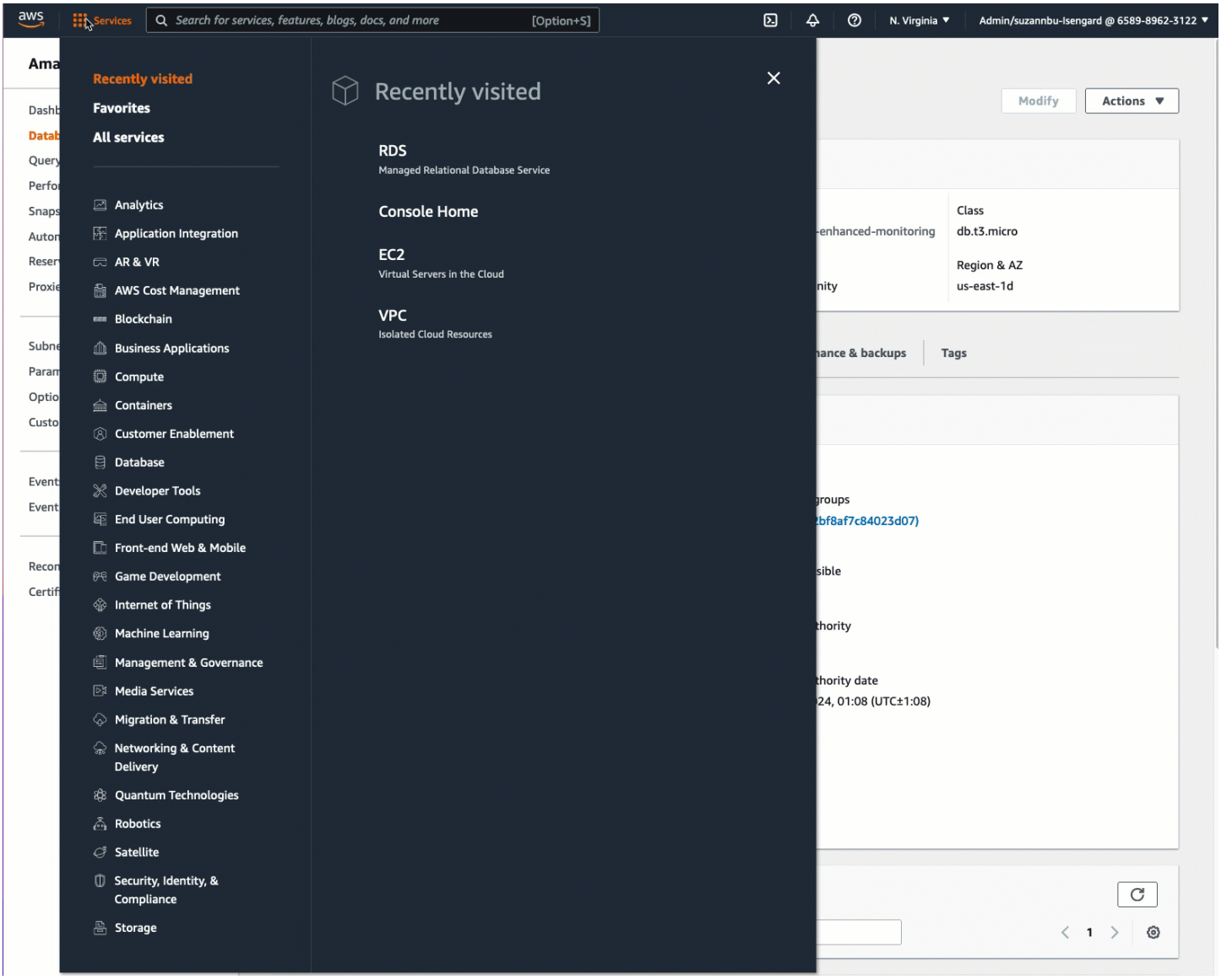
Per creare un'istanza database MySQL

1. Apri la console di Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Dal selettore della regione (in alto a destra), scegli l'istanza EC2 Regione AWS in cui hai creato l'istanza EC2. L'istanza EC2 e l'istanza database devono trovarsi nella stessa regione.
3. Sul pannello di controllo seleziona Create database (Crea database).
4. In Choose a database creation method (Seleziona metodo di creazione del database), scegli Standard create (Creazione standard). Quando scegli questa opzione, la funzione di connessione automatica per configurare automaticamente la connessione non è disponibile.
5. Sotto Engine options (Opzioni del motore) per Engine type (Tipo di motore) scegli MySQL.
6. Per DB instance size (Dimensione istanza database), seleziona Free tier (Piano gratuito).
7. Per il DB instance identifier (Identificatore istanze database) inserire un nome per il database RDS. Per questo tutorial, digita **`tutorial-database-manual`**.
8. Per il Master username (Nome utente principale), lascia il nome predefinito, che è **`admin`**.
9. Come Master password (Password principale) inserisci una password per questo tutorial che riesci a ricordare quindi per Confirm password (Conferma password) inserisci nuovamente la password.

10. Scegliere Crea database.

    Nella schermata Databases (Database) lo Status (Stato) dell'istanza database è Creating (Creazione in corso) fino a quando l'istanza database non è pronta per l'uso. Quando lo stato cambia in Available (Disponibile), puoi connettersi all'istanza database. A seconda della classe di istanza database e della quantità di storage, prima che la nuova istanza sia disponibile possono trascorrere fino a 20 minuti.

Visualizzazione di un'animazione: creazione di un'istanza database



A questo punto puoi eseguire Attività 3: connessione manuale dell'istanza EC2 al database RDS creando gruppi di sicurezza e assegnandoli alle istanze.

Attività 3: connessione manuale dell'istanza EC2 al database RDS creando gruppi di sicurezza e assegnandoli alle istanze

Obiettivo dell'attività

L'obiettivo di questa attività è riprodurre la configurazione della connessione della funzione di connessione automatica eseguendo manualmente quanto segue: crei due nuovi gruppi di sicurezza e quindi aggiungi un gruppo di sicurezza all'istanza EC2 e uno al database RDS.

Passaggi per creare nuovi gruppi di sicurezza e aggiungerli alle istanze

Attieniti ai passaggi seguenti per connettere un'istanza EC2 al tuo database RDS creando due nuovi gruppi di sicurezza. Quindi aggiungi un gruppo di sicurezza all'istanza EC2 e uno al database RDS.

Creare due nuovi gruppi di sicurezza e assegnare uno all'istanza EC2 e uno al database RDS

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Per prima cosa crea il gruppo di sicurezza per aggiungerlo all'istanza EC2, come indicato di seguito:
   a. Fare clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
   b. Scegliere Create Security Group (Crea gruppo di sicurezza).
   c. In Security group name (Nome di gruppo di sicurezza) inserisci un nome descrittivo per il gruppo di sicurezza. Per questo tutorial, digita **`ec2-rds-manual-configuration`**.
   d. In Description (Descrizione) inserisci una breve descrizione. Per questo tutorial, digita **`EC2 instance security group to allow EC2 instance to securely connect to RDS database`**.
   e. Scegliere Create Security Group (Crea gruppo di sicurezza). Dopo aver creato il gruppo di sicurezza del database RDS, tornerai a questo gruppo di sicurezza per aggiungere una regola in uscita.
3. Ora crea il gruppo di sicurezza da aggiungere al database RDS, come indicato di seguito:
   a. Fare clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
   b. Scegliere Create Security Group (Crea gruppo di sicurezza).
   c. In Security group name (Nome di gruppo di sicurezza) inserisci un nome descrittivo per il gruppo di sicurezza. Per questo tutorial, digita **`rds-ec2-manual-configuration`**.

d. In Description (Descrizione) inserisci una breve descrizione. Per questo tutorial, digita **`RDS database security group to allow EC2 instance to securely connect to RDS database`**.

e. In Inbound rules (Regole in entrata), scegli Add rule (Aggiungi regola) ed esegui le seguenti operazioni:

   i. Per Type (Tipo) scegli MySQL/Aurora.

   ii. Per Source, scegli il gruppo di sicurezza dell'istanza EC2 ec2- rds-manual-configuration che hai creato nel passaggio 2 di questa procedura.

f. Scegliere Create Security Group (Crea gruppo di sicurezza).

4. Per aggiungere una regola in uscita, modifica il gruppo di sicurezza dell'istanza EC2, come indicato di seguito:

   a. Fai clic su Gruppi di sicurezza nel riquadro di navigazione.

   b. Seleziona il gruppo di sicurezza dell'istanza EC2 (che hai denominato **`ec2-rds-manual-configuration`**) e scegli la scheda Outbound rules (Regole in uscita).

   c. Scegli Edit outbound rules (Modifica regole in uscita).

   d. Scegli Add rule (Aggiungi regola) ed esegui le seguenti operazioni:

      i. Per Type (Tipo) scegli MySQL/Aurora.

      ii. Per Source (Origine), scegli il gruppo di sicurezza del database RDS rds-ec2-manual-configuration creato nella Fase 3 di questa procedura.

      iii. Scegliere Salva regole.

5. Aggiungi il gruppo di sicurezza EC2 all'istanza EC2, come indicato di seguito:

   a. Nel riquadro di navigazione, seleziona Istanze.

   b. Seleziona l'istanza EC2, quindi scegli Actions (Azioni), Security (Sicurezza), Change security groups (Cambia gruppi di sicurezza).

   c. In Gruppi di sicurezza associati, scegli il campo Seleziona gruppi di sicurezza, scegli ec2-rds-manual-configuration che hai creato in precedenza, quindi scegli Aggiungi gruppo di sicurezza.

   d. Selezionare Salva.

6. Aggiungi il gruppo di sicurezza del database RDS al database RDS, come indicato di seguito:

   a. Apri la console di Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.

b. Nel riquadro di navigazione scegli Databases (Database) quindi seleziona il database.
c. Scegli Modifica.
d. Sotto Connectivity (Connettività), per il Security group (Gruppo di sicurezza), scegli rds-ec2-manual-configuration che hai creato in precedenza, quindi scegli Continue (Continua).
e. Sotto Scheduling of Modifications (Pianificazione delle modifiche) scegli Apply immediately (Applica immediatamente).
f. Scegliere Modify DB Instance (Modifica istanza database).

Ora hai completato i passaggi manuali che simulano i passaggi automatici che si verificano quando utilizzi la funzione di connessione automatica.

Hai completato l'Opzione 3 di questo tutorial. Se hai completato le opzioni 1, 2 e 3 e non hai più bisogno delle risorse create in questo tutorial, dovresti eliminarle per evitare di incorrere in costi inutili. Per ulteriori informazioni, consulta Eliminazione.

Eliminazione

Ora che hai completato il tutorial, è buona norma ripulire (eliminare) tutte le risorse che non desideri più utilizzare. La pulizia AWS delle risorse impedisce al tuo account di incorrere in ulteriori addebiti.

Argomenti

- Interruzione di un'istanza EC2
- Eliminazione di un database RDS

Interruzione di un'istanza EC2

Se hai avviato un'istanza EC2 appositamente per questo tutorial, puoi interromperla per non incorrere in alcun addebito correlato a questa.

Per interrompere un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza creata per questo tutorial, quindi scegli Instance state (Stato istanza), Terminate instance (Termina istanza).
4. Quando viene richiesta la conferma, seleziona Terminate (Interrompi).

Eliminazione di un database RDS

Se hai creato un database RDS appositamente per questo tutorial, puoi interromperlo per non incorrere in alcun addebito correlato a questo.

Eliminazione di un database RDS tramite la console

1. Apri la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Nel pannello di navigazione, scegliere Databases (Database).
3. Seleziona il database RDS che hai creato per questo tutorial e scegli Actions (Azioni), Delete (Elimina).
4. Inserisci **`delete me`** nella casella e scegli Delete (Elimina).

Identifica le tue istanze EC2

Potrebbe essere necessario determinare se l'applicazione è in esecuzione su un'istanza EC2, soprattutto se disponi di un ambiente di elaborazione misto. Ogni istanza ha un documento di identità firmato che puoi verificare crittograficamente. È possibile trovare questi documenti al seguente indirizzo locale non indirizzabile. `http://169.254.169.254/latest/dynamic/instance-identity/` Per ulteriori informazioni, consulta Documenti di identità dell'istanza.

Ispezionare l'UUID del sistema

È possibile ottenere l'UUID del sistema e cercarlo nell'ottetto iniziale dell'UUID `EC2` (in Linux, potrebbe essere in minuscolo). `ec2` Questo metodo è rapido, ma potenzialmente impreciso perché c'è una piccola possibilità che un sistema che non è un'istanza EC2 possa avere un UUID che inizia con questi caratteri. Inoltre, alcune versioni di SMBIOS utilizzano il formato little-endian, che non include l'UUID all'inizio. `EC2` Questo potrebbe essere il caso delle istanze EC2 che utilizzano SMBIOS 2.4 per Windows o delle distribuzioni Linux diverse da Amazon Linux 2 che dispongono di una propria implementazione di SMBIOS.

Esempio Linux: ottieni l'UUID da DMI (solo AMI HVM)

Utilizzare il comando seguente per ottenere l'UUID utilizzando la Desktop Management Interface (DMI):

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

Nell'esempio seguente di output, l'UUID inizia con "EC2", il che indica che il sistema è probabilmente un'istanza EC2.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

Nell'esempio seguente di output, l'UUID è rappresentato in formato little-endian.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

In alternativa, per le istanze create sul sistema Nitro, è possibile utilizzare il seguente comando:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Se l'output è un ID dell'istanza, come nell'esempio seguente, il sistema è un'istanza EC2:

```
i-0af01c0123456789a
```

Esempio Linux: ottieni l'UUID dall'hypervisor (solo AMI PV)

Utilizzare il seguente comando per ottenere l'UUID dall'hypervisor:

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

Nell'esempio seguente di output, l'UUID inizia con "ec2", il che indica che il sistema è probabilmente un'istanza EC2.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Esempio in Windows: ottieni l'UUID utilizzando WMI o Windows PowerShell

Utilizza la riga di comando Windows Management Instrumentation (WMIC) nel modo seguente:

```
wmic path win32_computersystemproduct get uuid
```

In alternativa, se si utilizza Windows PowerShell, utilizzare il Get-WmiObject cmdlet come segue:

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select
 UUID
```

Nell'esempio seguente di output, l'UUID inizia con "EC2", il che indica che il sistema è probabilmente un'istanza EC2.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Per istanze che utilizzano SMBIOS 2.4, l'UUID potrebbe essere rappresentato in formato little-endian, ad esempio:

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Ispezione dell'identificatore di generazione della macchina virtuale del sistema

Un identificatore di generazione della macchina virtuale è costituito da un buffer univoco di 128 bit interpretato come identificatore intero casuale crittografico. È possibile recuperare l'identificatore di generazione della macchina virtuale per identificare l'istanza di Amazon Elastic Compute Cloud. L'identificatore di generazione viene esposto all'interno del sistema operativo guest dell'istanza tramite una voce della tabella ACPI. Il valore cambierà se la macchina viene clonata, copiata o importata in AWS, come con VM Import/Export.

Esempio: recupera l'identificatore di generazione della macchina virtuale da Linux

Puoi utilizzare i seguenti comandi per recuperare l'identificatore di generazione della macchina virtuale dalle istanze che eseguono Linux.

Amazon Linux 2

1. Aggiorna i pacchetti software esistenti, se necessario, utilizzando il seguente comando:

   ```
   sudo yum update
   ```

2. Se necessario, utilizza il pacchetto busybox utilizzando il seguente comando:

   ```
   sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/
   b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
   ```

3. Se necessario, installa i pacchetti prerequisiti utilizzando il seguente comando:

   ```
   sudo yum install busybox.rpm iasl -y
   ```

4. Esegui il seguente comando `iasl` per produrre output dalla tabella ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

5. Esegui il comando seguente per esaminare l'output del comando `iasl`:

```
cat SSDT2.dsl
```

L'output deve restituire lo spazio degli indirizzi necessario per recuperare l'identificatore di generazione della macchina virtuale:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
```

```
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

6. (Opzionale) Aumenta le autorizzazioni del terminale per i passaggi rimanenti con il seguente comando:

```
sudo -s
```

7. Utilizza il comando seguente per archiviare lo spazio degli indirizzi precedentemente raccolto:

```
VMGN_ADDR=0xFED01000
```

8. Utilizza il comando seguente per scorrere lo spazio degli indirizzi e creare l'identificatore di generazione della macchina virtuale:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Recupera l'identificatore di generazione della macchina virtuale dal file di output con il seguente comando:

```
cat vmgenid ; echo
```

L'output visualizzato dovrebbe essere simile al seguente:

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Aggiorna i pacchetti software esistenti, se necessario, utilizzando il seguente comando:

```
sudo apt update
```

2. Se necessario, installa i pacchetti prerequisiti utilizzando il seguente comando:

```
sudo apt install busybox iasl -y
```

3. Esegui il seguente comando `iasl` per produrre output dalla tabella ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Esegui il comando seguente per esaminare l'output del comando `iasl`:

```
cat SSDT2.dsl
```

L'output deve restituire lo spazio degli indirizzi necessario per recuperare l'identificatore di generazione della macchina virtuale:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)
```

```
Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

5. (Opzionale) Aumenta le autorizzazioni del terminale per i passaggi rimanenti con il seguente comando:

```
sudo -s
```

6. Utilizza i comandi seguenti per archiviare lo spazio degli indirizzi precedentemente raccolto:

```
VMGN_ADDR=0xFED01000
```

7. Utilizza il comando seguente per scorrere lo spazio degli indirizzi e creare l'identificatore di generazione della macchina virtuale:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. Recupera l'identificatore di generazione della macchina virtuale dal file di output con il seguente comando:

```
cat vmgenid ; echo
```

L'output visualizzato dovrebbe essere simile al seguente:

```
EC2F335D979132C4165896753E72BD1C
```

Esempio: recupera l'identificatore di generazione della macchina virtuale da Windows

È possibile creare un'applicazione di esempio per recuperare l'identificatore di generazione della macchina virtuale dalle istanze che eseguono Windows. Per ulteriori informazioni, consulta Obtaining the virtual machine generation identifier (Ottenimento dell'identificatore di generazione della macchina virtuale) nella documentazione Microsoft.

Gestisci le impostazioni di sistema per la tua istanza Amazon EC2

Dopo aver avviato l'istanza, puoi accedere come amministratore per apportare modifiche. Questa sezione è incentrata sulla gestione delle impostazioni di sistema per l'istanza.

Indice

- Controllo dello stato del processore per l'istanza Amazon EC2 Linux
- Ottimizzazione delle opzioni della CPU
- AMD SEV-SNP su Amazon EC2
- Aggiungere componenti di sistema Windows utilizzando i supporti di installazione
- Gestisci gli utenti di sistema sulla tua istanza Linux
- Imposta la password dell'amministratore di Windows per la tua istanza

Sincronizzazione precisa dell'orologio e dell'ora sulla tua istanza EC2

Un riferimento temporale coerente e preciso sull'istanza Amazon EC2 è fondamentale per molte attività e processi del server. I timestamp nei log di sistema svolgono un ruolo essenziale nell'identificazione del momento in cui si sono verificati i problemi e dell'ordine cronologico degli eventi. Quando utilizzi l'SDK AWS CLI o un AWS SDK per effettuare richieste dalla tua istanza, questi strumenti firmano le richieste per tuo conto. Se le impostazioni di data e ora dell'istanza non sono accurate, può verificarsi una discrepanza tra la data riportata nella firma e la data della richiesta, con conseguente rifiuto delle richieste. AWS

Per risolvere questo importante aspetto, Amazon offre il servizio di sincronizzazione oraria di Amazon, accessibile da tutte le istanze EC2 e utilizzabile con vari Servizi AWS. Il servizio utilizza una serie di orologi di riferimento atomici e connessi via satellite ciascuno Regione AWS per fornire letture dell'ora accurate e aggiornate dello standard globale UTC (Coordinated Universal Time).

Per prestazioni ottimali, ti consigliamo di utilizzare il servizio Amazon Time Sync locale sulle tue istanze EC2. Per un backup sul servizio Amazon Time Sync locale sulle tue istanze o per connettere risorse esterne ad Amazon EC2 ad Amazon Time Sync Service, puoi utilizzare il servizio pubblico Amazon Time Sync disponibile all'indirizzo. `time.aws.com` Il servizio di sincronizzazione oraria di Amazon pubblico spalma in modo automatico i secondi intercalari aggiunti all'orario UTC. Il servizio pubblico Amazon Time Sync è supportato a livello globale dalla nostra flotta di orologi di riferimento atomici e connessi via satellite in ciascuno di essi. Regione AWS

Secondi intercalari

I secondi intercalari, introdotti nel 1972, sono regolazioni occasionali di un secondo dell'ora UTC per tenere conto delle irregolarità nella rotazione terrestre al fine di compensare le differenze tra l'ora atomica internazionale (TAI) e l'ora solare (Ut1). Per gestire i secondi intercalari per conto dei clienti, abbiamo progettato Leap Second Smearing all'interno del servizio di sincronizzazione oraria di Amazon. Per ulteriori informazioni, consulta Guarda prima di saltare: il secondo salto in arrivo e AWS.

I secondi intercalari stanno scomparendo e appoggiamo pienamente la decisione presa alla 27a conferenza generale sui pesi e le misure di abbandonare i secondi intercalari entro il 2035.

Per supportare questa transizione, prevediamo comunque di risparmiare tempo durante un secondo intercalare quando si accede al servizio di sincronizzazione oraria di Amazon tramite la connessione NTP locale o i nostri pool NTP pubblici (`time.aws.com`). Il clock hardware PTP, tuttavia, non offre l'opzione dei tempi spalmati. In caso di secondo intercalare, il clock hardware PTP aggiungerà il secondo intercalare secondo gli standard UTC. Le sorgenti temporali "spalmate" e "secondi intercalari" sono le stesse nella maggior parte dei casi. Tuttavia, poiché differiscono durante un evento di secondo intercalare, si sconsiglia di utilizzare contemporaneamente sorgenti temporali spalmate e non spalmate nella configurazione del client orario durante un evento di secondo intercalare.

Argomenti

- Imposta il riferimento temporale sulla tua istanza EC2 per utilizzare il servizio Amazon Time Sync locale
- Imposta il riferimento temporale sulla tua istanza EC2 o su qualsiasi dispositivo connesso a Internet per utilizzare il servizio pubblico Amazon Time Sync
- Confronta i timestamp delle tue istanze Linux
- Cambia il fuso orario della tua istanza

Risorse correlate

- AWS Blog di Compute: È ora: orologi accurati in microsecondi sulle istanze Amazon EC2
- AWS Blog sulle operazioni e le migrazioni sul cloud: Gestisci la precisione dell'orologio delle istanze Amazon EC2 utilizzando Amazon Time Sync Service e CloudWatch Amazon — Parte 1
- (Linux) https://chrony-project.org/

Imposta il riferimento temporale sulla tua istanza EC2 per utilizzare il servizio Amazon Time Sync locale

Il servizio Amazon Time Sync locale utilizza il Network Time Protocol (NTP) o fornisce un orologio hardware locale Precision Time Protocol (PTP) sulle istanze supportate. L'orologio hardware

PTP supporta una connessione NTP (istanze Linux e Windows) o una connessione PTP diretta (solo istanze Linux). Le connessioni NTP e PTP dirette utilizzano la stessa sorgente temporale estremamente precisa, ma la connessione PTP diretta è più accurata della connessione NTP. La connessione NTP al servizio di sincronizzazione oraria di Amazon supporta il leap smearing, mentre la connessione PTP al clock hardware PTP non spalma i tempi. Per ulteriori informazioni, consulta Secondi intercalari.

Le tue istanze possono accedere al servizio di sincronizzazione oraria di Amazon locale nel modo seguente:

- Tramite NTP nei seguenti endpoint di indirizzi IP:
  - IPv4: `169.254.169.123`
  - IPv6: `fd00:ec2::123` (Accessibile solo dalle istanze basate sul sistema Nitro). AWS
- (Solo Linux) Tramite una connessione PTP diretta per la connessione a un orologio hardware PTP locale:
  - `PHC0`

Le AMI Amazon Linux, le AMI Windows e la maggior parte delle AMI dei partner configurano l'istanza per utilizzare l'endpoint NTP IPv4 per impostazione predefinita. Questa è l'impostazione consigliata per la maggior parte dei carichi di lavoro dei clienti. Non sono necessarie ulteriori configurazioni per le istanze avviate da queste AMI, a meno che non si desideri utilizzare l'endpoint IPv6 o connettersi direttamente al clock hardware PTP.

Le connessioni NTP e PTP non richiedono alcuna modifica alla configurazione del VPC e l'istanza non richiede l'accesso a Internet.

> **Note**
>
> Solo le istanze Linux possono utilizzare una connessione PTP diretta per connettersi all'orologio hardware PTP locale. Le istanze Windows utilizzano NTP per connettersi all'orologio hardware PTP locale.

Argomenti

- Connect all'orologio hardware PTP

Connessione all'endpoint IPv4 del servizio di sincronizzazione oraria di Amazon

In questa sezione viene descritto come configurare l'istanza per l'utilizzo del servizio di sincronizzazione oraria di Amazon locale tramite l'endpoint IPv4.

Consulta le istruzioni relative al sistema operativo della tua istanza.

Linux

AL2023 e le ultime versioni delle AMI Amazon Linux 2 e Amazon Linux sono configurato per utilizzare per impostazione predefinita l'endpoint IPv4 del servizio di sincronizzazione oraria di Amazon. Non sono necessarie ulteriori configurazioni per le istanze avviate da queste AMI ed è possibile saltare la procedura seguente.

Se utilizzi un'AMI che non ha il servizio di sincronizzazione oraria di Amazon configurato per impostazione predefinita, utilizza una delle procedure seguenti per configurare il servizio di sincronizzazione oraria di Amazon sull'istanza con il client `chrony`. Richiede l'aggiunta di una voce del server per il servizio di sincronizzazione oraria di Amazon al file di configurazione di `chrony`.

Consulta le istruzioni relative al sistema operativo della tua istanza.

Amazon Linux

Connessione all'endpoint IPv4 del servizio di sincronizzazione oraria di Amazon su Amazon Linux tramite chrony

1. Connetti l'istanza e disinstalla il servizio NTP.

```
[ec2-user ~]$ sudo yum erase 'ntp*'
```

2. Installare il pacchetto `chrony`.

```
[ec2-user ~]$ sudo yum install chrony
```

3. Aprire il file `/etc/chrony.conf` tramite un editor di testo (ad esempio vim o nano). Verifica che il file includa la riga seguente:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

Se la riga è presente, allora il servizio di sincronizzazione oraria di Amazon è già configurato per l'uso dell'endpoint IPv4 del servizio ed è possibile passare alla fase successiva. In caso contrario, aggiungi la riga dopo qualsiasi altra istruzione `server` o `pool` già presente nel file, quindi salva le modifiche.

4. Avvia di nuovo il daemon `chrony` (`chronyd`).

```
[ec2-user ~]$ sudo service chronyd restart
```

```
Starting chronyd:                                          [  OK  ]
```

> **Note**
>
> In RHEL e CentOS (fino alla versione 6), il nome del servizio è `chrony` anziché `chronyd`.

5. Per configurare `chronyd` in modo da avviarlo a ogni avvio del sistema, utilizza il comando `chkconfig`.

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

6. Verifica che `chrony` utilizzi l'endpoint IPv4 `169.254.169.123` per sincronizzare l'orario.

```
[ec2-user ~]$ chronyc sources -v
```

```
210 Number of sources = 7

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
||                                                 .- xxxx [ yyyy ] +/-
zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted
offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured
offset,
```

```
       ||                                 \     |          |  zzzz = estimated
error.
       ||                                  |    |           \
       MS Name/IP address         Stratum Poll Reach LastRx Last sample


===============================================================================
       ^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-
 287us
       ^- ec2-12-34-231-12.eu-west>     2   6    17    43   -388us[ -388us] +/-
  11ms
       ^- tshirt.heanet.ie              1   6    17    44   +178us[  +25us] +/-
1959us
       ^? tbag.heanet.ie                0   6     0     -     +0ns[   +0ns] +/-
   0ns
       ^? bray.walcz.net                0   6     0     -     +0ns[   +0ns] +/-
   0ns
       ^? 2a05:d018:c43:e312:ce77:>     0   6     0     -     +0ns[   +0ns] +/-
   0ns
       ^? 2a05:d018:dab:2701:b70:b>     0   6     0     -     +0ns[   +0ns] +/-
   0ns
```

Nell'output restituito, ^* indica l'origine ora preferita.

7. Verifica i parametri di sincronizzazione dell'orario indicati da `chrony`.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
       Stratum         : 4
       Ref time (UTC)  : Wed Nov 22 13:18:34 2017
       System time     : 0.000000626 seconds slow of NTP time
       Last offset     : +0.002852759 seconds
       RMS offset      : 0.002852759 seconds
       Frequency       : 1.187 ppm fast
       Residual freq   : +0.020 ppm
       Skew            : 24.388 ppm
       Root delay      : 0.000504752 seconds
       Root dispersion : 0.001112565 seconds
       Update interval : 64.4 seconds
       Leap status     : Normal
```

Ubuntu

Connessione all'endpoint IPv4 del servizio di sincronizzazione oraria di Amazon su Ubuntu tramite chrony

1. Connettiti all'istanza e utilizza `apt` per installare il pacchetto `chrony`.

```
ubuntu:~$ sudo apt install chrony
```

> **Note**
>
> Se necessario, prima aggiorna l'istanza eseguendo `sudo apt update`.

2. Aprire il file `/etc/chrony/chrony.conf` tramite un editor di testo (ad esempio vim o nano). Aggiungi la riga seguente prima di qualsiasi altra istruzione `server` o `pool` già presente nel file, quindi salva le modifiche:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Riavvia il servizio `chrony`.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Verifica che `chrony` utilizzi l'endpoint IPv4 `169.254.169.123` per sincronizzare l'orario.

```
ubuntu:~$ chronyc sources -v
```

```
210 Number of sources = 7

              .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
            / .- Source state '*' = current synced, '+' = combined , '-' = not
 combined,
           | /   '?' = unreachable, 'x' = time may be in error, '~' = time too
 variable.
           ||                                                 .- xxxx [ yyyy ]
 +/- zzzz
```

```
           ||      Reachability register (octal) -.           |  xxxx =
adjusted offset,
           ||      Log2(Polling interval) --.      |          |  yyyy =
measured offset,
           ||                                \     |          |  zzzz =
estimated error.
           ||                                 |    |           \
           MS Name/IP address         Stratum Poll Reach LastRx Last sample

===============================================================================
           ^* 169.254.169.123               3   6    17    12    +15us[  +57us]
+/-  320us
           ^- tbag.heanet.ie                1   6    17    13  -3488us[-3446us]
+/- 1779us
           ^- ec2-12-34-231-12.eu-west-     2   6    17    13   +893us[ +935us]
+/- 7710us
           ^? 2a05:d018:c43:e312:ce77:6     0   6     0   10y     +0ns[   +0ns]
+/-    0ns
           ^? 2a05:d018:d34:9000:d8c6:5     0   6     0   10y     +0ns[   +0ns]
+/-    0ns
           ^? tshirt.heanet.ie              0   6     0   10y     +0ns[   +0ns]
+/-    0ns
           ^? bray.walcz.net                0   6     0   10y     +0ns[   +0ns]
+/-    0ns
```

Nell'output restituito, la riga che inizia con ^* indica l'origine di orario preferita.

5. Verifica i parametri di sincronizzazione dell'orario indicati da `chrony`.

```
ubuntu:~$ chronyc tracking
```

```
Reference ID    : 169.254.169.123 (169.254.169.123)
           Stratum         : 4
           Ref time (UTC)  : Wed Nov 29 07:41:57 2017
           System time     : 0.000000011 seconds slow of NTP time
           Last offset     : +0.000041659 seconds
           RMS offset      : 0.000041659 seconds
           Frequency       : 10.141 ppm slow
           Residual freq   : +7.557 ppm
           Skew            : 2.329 ppm
           Root delay      : 0.000544 seconds
           Root dispersion : 0.000631 seconds
           Update interval : 2.0 seconds
```

```
            Leap status     : Normal
```

SUSE Linux

A partire da SUSE Linux Enterprise Server 15, `chrony` è l'implementazione predefinita di NTP.

Connessione all'endpoint IPv4 del servizio di sincronizzazione oraria di Amazon su SUSE Linux tramite chrony

1. Aprire il file `/etc/chrony.conf` tramite un editor di testo (ad esempio vim o nano).
2. Verificare che il file contenga la riga seguente:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

   Aggiungere questa riga se non è presente.
3. Commentare le altre righe del server o del pool.
4. Apri yaST e abilita il servizio chrony.

Windows

A partire dal rilascio di agosto 2018, le AMI di Windows utilizzano Amazon Time Sync Service per impostazione predefinita. Non è richiesta alcuna ulteriore configurazione per le istanze avviate da queste AMI ed è possibile saltare le seguenti procedure.

Se utilizzi un'AMI che non ha il servizio Amazon Time Sync configurato di default, verifica innanzitutto la tua attuale configurazione NTP. Se la tua istanza utilizza già l'endpoint IPv4 del servizio di sincronizzazione oraria di Amazon, non è richiesta alcuna ulteriore configurazione. Se la tua istanza non utilizza il servizio di sincronizzazione oraria di Amazon, completa la procedura per modificare il server NTP in modo da utilizzare il servizio.

Per verificare la configurazione di NTP

1. Dall'istanza, aprire una finestra del prompt dei comandi.
2. Ottenere la configurazione attuale di NTP digitando il comando seguente:

   ```
   w32tm /query /configuration
   ```

Questo comando restituisce le impostazioni della configurazione corrente dell'istanza Windows e mostra se sei connesso al servizio di sincronizzazione oraria di Amazon.

3. (Opzionale) Ottenere lo stato della configurazione attuale digitando il comando seguente:

```
w32tm /query /status
```

Questo comando restituisce informazioni come l'ultima sincronizzazione dell'istanza con il server NTP e l'intervallo di polling.

Modifica del server NTP per l'utilizzo di Amazon Time Sync Service

1. Dalla finestra del prompt dei comandi, esegui il comando seguente:

```
w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
```

2. Verificare le nuove impostazioni tramite il comando seguente:

```
w32tm /query /configuration
```

Nell'output restituito, verifica che `NtpServer` visualizzi l'endpoint IPv4 `169.254.169.123`.

Impostazioni NTP (Network Time Protocol) predefinite per le AMI Windows Amazon

Le Amazon Machine Images (AMI) generalmente rispettano le out-of-the-box impostazioni predefinite, tranne nei casi in cui sono necessarie modifiche per funzionare sull'infrastruttura EC2. Le impostazioni seguenti sono state stabilite per il corretto funzionamento in un ambiente virtuale, nonché per mantenere qualsiasi scostamento dell'orologio entro un secondo di accuratezza:

- Intervallo di aggiornamento: regola la frequenza con cui il servizio aggiusterà l'ora del sistema in base alla precisione. AWS configura l'intervallo di aggiornamento in modo che si verifichi una volta ogni due minuti.
- Server NTP: a partire dalla versione di agosto 2018, le AMI utilizzeranno il servizio di sincronizzazione oraria di Amazon per impostazione predefinita. Questo servizio orario è accessibile da qualsiasi endpoint IPv4 Regione AWS 169.254.169.123. Inoltre, il flag 0x9 indica che il servizio ora funziona da client e indica di utilizzare `SpecialPollInterval` per stabilire la frequenza di check-in nel server di riferimento ora configurato.

- Type – "NTP" indica che il servizio funzionerà come client NTP standalone invece che come parte di un dominio.
- Abilitato e InputProvider: il servizio orario è abilitato e fornisce l'ora al sistema operativo.
- Intervallo di sondaggio speciale: esegue controlli sul server NTP configurato ogni 900 secondi (15 minuti).

Percorso Registro di sistema	Nome chiave	Dati
HKL M:\System\\ servicesC urrentControlSet\ w32time\ Config	UpdateInterval	120
HKL M:\System\\ services\ w32timeCurrentControlSet\ Parametri	NtpServer	169.254.169.123,0x9
HKL M:\System\\ services\ w32timeCurrentControlSet\ Parametri	Type	NTP
HKL M:\System\\ services\ CurrentControlSet w32time\\ TimeProviders NtpClient	Abilitato	1
HKL M:\System\\ services\ CurrentControlSet w32time\\ TimeProviders NtpClient	InputProvider	1
HKL M:\System\\ services\ CurrentControlSet w32time\\ TimeProviders NtpClient	SpecialPollInterval	900

Connessione all'endpoint IPv6 del servizio di sincronizzazione oraria di Amazon

In questa sezione viene descritto come differisce la procedura riportata in Connessione all'endpoint IPv4 del servizio di sincronizzazione oraria di Amazon nel caso della configurazione dell'istanza per

l'utilizzo del servizio di sincronizzazione oraria di Amazon locale tramite l'endpoint IPv6. Non viene illustrato l'intero processo di configurazione di Amazon Time Sync Service.

L'endpoint IPv6 è accessibile solo sulle istanze create sul sistema Nitro. AWS

> **Note**
>
> Non è consigliabile utilizzare contemporaneamente le voci dell'endpoint IPv4 e IPv6. I pacchetti NTP IPv4 e IPv6 provengono dallo stesso server locale per l'istanza. La configurazione degli endpoint IPv4 e IPv6 non è necessaria e non migliorerà la precisione dell'ora sull'istanza.

Consulta le istruzioni relative al sistema operativo della tua istanza.

Linux

A seconda della distribuzione Linux che stai utilizzando, quando raggiungi la fase di modifica del file chrony.conf, utilizzerai l'endpoint IPv6 di Amazon Time Sync Service (`fd00:ec2::123`) anziché l'endpoint IPv4 (): `169.254.169.123`

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Salva il file e verifica che `chrony` utilizzi l'endpoint IPv6 `fd00:ec2::123` per sincronizzare l'orario:

```
[ec2-user ~]$ chronyc sources -v
```

Nell'output, se compare l'endpoint IPv6 `fd00:ec2::123`, la configurazione è completa.

Windows

Quando raggiungi la fase di modifica del server NTP per utilizzare Amazon Time Sync Service, utilizzerai l'endpoint IPv6 di Amazon Time Sync Service (`fd00:ec2::123`) anziché l'endpoint IPv4 (): `169.254.169.123`

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Verifica che le nuove impostazioni utilizzino l'endpoint IPv6 per sincronizzare l'ora: `fd00:ec2::123`

```
w32tm /query /configuration
```

Nell'output, verifica che venga `NtpServer` visualizzato l'endpoint IPv6. `fd00:ec2::123`

Connect all'orologio hardware PTP

Il clock hardware PTP fa parte del AWS sistema Nitro, quindi è direttamente accessibile sulle istanze EC2 bare metal e virtualizzate supportate senza utilizzare le risorse del cliente.

Gli endpoint NTP per l'orologio hardware PTP sono gli stessi del normale Amazon Time Sync Service. Se la tua istanza ha un orologio hardware PTP e hai configurato la connessione NTP (verso l'endpoint IPv4 o IPv6), l'ora dell'istanza viene automaticamente ricavata dall'orologio hardware PTP tramite NTP.

Per le istanze Linux, puoi configurare una connessione PTP diretta, che ti fornirà un orario più preciso rispetto alla connessione NTP. Le istanze Windows supportano solo una connessione NTP all'orologio hardware PTP.

Requisiti

Il clock hardware PTP è disponibile su un'istanza quando vengono soddisfatti i seguenti requisiti:

- Supportato Regioni AWS: Stati Uniti orientali (Virginia settentrionale) e Asia Pacifico (Tokyo)
- Famiglie di istanza supportate:
  - Uso generale: M7a, M7g, M7gd, M7i
  - Calcolo ottimizzato: C7a, C7gd, C7i
  - Memoria ottimizzata: R7a, R7g, R7gd, R7i
- (Solo Linux) Driver ENA versione 2.10.0 o successiva installato su un sistema operativo supportato. Per ulteriori informazioni sui sistemi operativi supportati, consulta i prerequisiti del driver su. GitHub

(Solo Linux) Configurate una connessione PTP diretta all'orologio hardware PTP

Questa sezione descrive come configurare l'istanza Linux per utilizzare il servizio Amazon Time Sync locale tramite l'orologio hardware PTP utilizzando una connessione PTP diretta. Richiede l'aggiunta di una voce del server per l'orologio hardware PTP nel file di configurazione. `chrony`

Per configurare una connessione PTP diretta all'orologio hardware PTP (solo istanze Linux)

1. Connect alla propria istanza Linux ed effettuare le seguenti operazioni:

a. Installa il driver del kernel Linux per Elastic Network Adapter (ENA) versione 2.10.0 o successiva.

b. Abilita l'orologio hardware PTP.

Per le istruzioni di installazione, consultate il driver del kernel Linux per la famiglia Elastic Network Adapter (ENA) su. GitHub

2. Verifica che il dispositivo `/dev/ptp0` sia presente sulla tua istanza.

```
[ec2-user ~]$ ls /dev/ptp0
```

L'output previsto è il seguente: Se `/dev/ptp0` non è presente nell'output, significa che il driver ENA non è stato installato correttamente. Rivedi il passaggio 1 di questa procedura per l'installazione del driver.

```
/dev/ptp0
```

3. Modifica `/etc/chrony.conf` con un editor di testo e aggiungi la seguente riga in qualsiasi punto del file.

```
refclock PHC /dev/ptp0 poll 0 delay 0.000010 prefer
```

4. Riavvia chrony.

```
[ec2-user ~]$ sudo systemctl restart chronyd
```

5. Verifica che chrony stia utilizzando il clock hardware PTP per sincronizzare l'ora su questa istanza.

```
[ec2-user ~]$ chronyc sources
```

Output previsto

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
#* PHC0                          0   0    377    1   +2ns[ +1ns] +/-   5031ns
```

Nell'output restituito, * indica la fonte dell'ora preferita. PHC0 corrisponde al clock hardware PTP. Potrebbe essere necessario attendere qualche secondo dopo il riavvio di chrony per la visualizzazione dell'asterisco.

Imposta il riferimento temporale sulla tua istanza EC2 o su qualsiasi dispositivo connesso a Internet per utilizzare il servizio pubblico Amazon Time Sync

Puoi configurare la tua istanza, o qualsiasi dispositivo connesso a Internet, come il computer locale o un server on-premise, per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico, accessibile via Internet all'indirizzo `time.aws.com`. Puoi utilizzare il servizio pubblico Amazon Time Sync come backup per il servizio Amazon Time Sync locale e per connettere risorse esterne al servizio Amazon Time Sync. AWS

> **Note**
>
> Per prestazioni ottimali, ti consigliamo di utilizzare il servizio Amazon Time Sync locale sulle tue istanze e di utilizzare solo il servizio pubblico Amazon Time Sync come backup.

Utilizza le istruzioni relative al sistema operativo dell'istanza o del dispositivo.

Linux

Configurazione dell'istanza o del dispositivo Linux per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico tramite chrony o ntpd

1. Utilizzando un editor di testo, modifica `/etc/chrony.conf` (se usi chrony) o `/etc/ntp.conf` (se usi ntpd) come segue:

   a. Per evitare che l'istanza o il dispositivo tenti di mischiare server "spalmati" e server non "spalmati", rimuovi o commenta le righe che iniziano con `server`, ad eccezione di qualsiasi connessione esistente al servizio di sincronizzazione oraria di Amazon locale.

   > **Important**
   >
   > Se stai configurando la tua istanza EC2 per connettersi al servizio di sincronizzazione oraria di Amazon pubblico, non rimuovere la seguente riga che imposta l'istanza per connettersi al servizio di sincronizzazione oraria di Amazon

locale. Il servizio di sincronizzazione oraria di Amazon locale è una connessione più diretta e fornirà una migliore precisione di clock. Il servizio di sincronizzazione oraria di Amazon pubblico deve essere usato solo come backup.

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

b. Aggiungi la seguente riga per connetterti al servizio di sincronizzazione oraria di Amazon pubblico.

```
pool time.aws.com iburst
```

2. Riavvia il daemon utilizzando uno dei seguenti comandi.

   - chrony

   ```
   sudo service chronyd force-reload
   ```

   - ntpd

   ```
   sudo service ntp reload
   ```

macOS

Configurazione dell'istanza o del dispositivo macOS per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico

1. Apri Preferenze di Sistema.
2. Scegli Date & Time (Data e ora), quindi scegli la scheda Date & Time (Data e ora).
3. Per apportare modifiche, scegli l'icona del lucchetto e inserisci la password quando richiesto.
4. In Set date and time automatically (Imposta data e ora automaticamente), inserisci **`time.aws.com`**.

Windows

Configurazione dell'istanza o del dispositivo Windows per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico

1. Apri il Pannello di controllo.
2. Scegli l'icona Date and Time (Data e ora).
3. Scegli la scheda Internet Time (Ora Internet). Questa scheda non sarà disponibile se il PC fa parte di un dominio. In tal caso, sincronizzerà l'ora con il controller di dominio. Puoi configurare il controller per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico.
4. Scegli Change settings (Cambia impostazioni).
5. Seleziona la casella di controllo Synchronize with an Internet time server (Sincronizza con un server orario Internet).
6. Accanto a Server, inserisci **`time.aws.com`**.

Configurazione dell'istanza o del dispositivo Windows Server per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico

- Segui le istruzioni di Microsoft per aggiornare il registro.

Confronta i timestamp delle tue istanze Linux

Se utilizzi il servizio Amazon Time Sync, puoi confrontare i timestamp delle tue istanze Amazon EC2 Linux ClockBound con per determinare l'ora reale di un evento. ClockBound misura la precisione dell'orologio della tua istanza EC2 e ti consente di verificare se un determinato timestamp è passato o futuro rispetto all'orologio corrente dell'istanza. Queste informazioni sono utili per determinare l'ordine e la coerenza degli eventi e delle transazioni tra le istanze EC2, indipendentemente dalla posizione geografica di ciascuna istanza.

ClockBound è un demone e una libreria open source. Per ulteriori informazioni ClockBound, comprese le istruzioni di installazione, vedere ClockBoundsu. GitHub

ClockBound è supportato solo per le istanze Linux.

Se utilizzi la connessione PTP diretta al clock hardware PTP, il tuo daemon orario, ad esempio chrony, sottovaluterà il limite di errore del clock. Questo perché un clock hardware PTP non trasmette le informazioni corrette relative all'errore a chrony come invece fa NTP. Di conseguenza, il daemon

di sincronizzazione del clock presuppone che il clock sia preciso rispetto all'UTC e quindi abbia un limite di errore pari a `0`. Per misurare l'intero limite di errore, Nitro System calcola il limite di errore dell'orologio hardware PTP e lo rende disponibile all'istanza EC2 tramite il file system del driver ENA. `sysfs` Puoi leggerlo direttamente come valore, in nanosecondi.

Per recuperare il limite di errore dell'orologio hardware PTP

1. Per prima cosa ottenete la posizione corretta del dispositivo di orologio hardware PTP utilizzando uno dei seguenti comandi. Il percorso del comando è diverso a seconda dell'AMI utilizzata per avviare l'istanza.

   - Per Amazon Linux 2:

     ```
     cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
     ```

   - Per Amazon Linux 2023:

     ```
     cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
     ```

   L'output è il nome dello slot PCI, che è la posizione del dispositivo di clock hardware PTP. In questo esempio, la posizione è. `0000:00:03.0`

   ```
   PCI_SLOT_NAME=0000:00:03.0
   ```

2. Per recuperare l'errore dell'orologio hardware PTP associato, esegui il comando seguente. Includi il nome dello slot PCI del passaggio precedente.

   ```
   cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
   ```

   L'output è il limite di errore del clock hardware PTP, espresso in nanosecondi.

Per calcolare l'errore di clock corretto associato a un determinato momento quando si utilizza la connessione PTP diretta all'orologio hardware PTP, è necessario aggiungere l'errore di clock associato ClockBound a chrony o all'ora in cui viene eseguito il chrony polling dell'orologio hardware PTP. Per ulteriori informazioni sulla misurazione e il monitoraggio della precisione dell'orologio, consulta Gestire la precisione dell'orologio delle istanze Amazon EC2 utilizzando Amazon Time Sync Service e Amazon CloudWatch — Parte 1.

Cambia il fuso orario della tua istanza

Per impostazione predefinita, le istanze Amazon EC2 sono impostate sul fuso orario UTC (Coordinated Universal Time). È possibile modificare l'ora di un'istanza all'ora locale o a un altro fuso orario della rete.

Consulta le istruzioni relative al sistema operativo della tua istanza.

Linux

> **Important**
>
> Queste informazioni si applicano ad Amazon Linux. Per informazioni su altre distribuzioni, consulta la documentazione specifica.

Per modificare il fuso orario su un'istanza Amazon Linux 2 o AL2023

1. Visualizzare l'impostazione del fuso orario corrente del sistema.

   ```
   [ec2-user ~]$ timedatectl
   ```

2. Elencare i fusi orari disponibili.

   ```
   [ec2-user ~]$ timedatectl list-timezones
   ```

3. Impostare il fuso orario scelto.

   ```
   [ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
   ```

4. (Facoltativo) Verificare che il fuso orario corrente venga aggiornato al nuovo fuso orario eseguendo di nuovo il comando timedatectl.

   ```
   [ec2-user ~]$ timedatectl
   ```

Windows

Modifica del fuso orario su un'istanza Windows

1. Dall'istanza, aprire una finestra del prompt dei comandi.

2. Identificare il fuso orario da utilizzare sull'istanza. Per ottenere un elenco dei fusi orari, utilizzare il comando seguente:

   ```
   tzutil /l
   ```

   Questo comando restituisce un elenco di tutti i fusi orari disponibili nel seguente formato:

   ```
   display name
   time zone ID
   ```

3. Individuare l'ID del fuso orario da assegnare all'istanza.
4. Assegna a un altro fuso orario tramite il comando seguente:

   ```
   tzutil /s "Pacific Standard Time"
   ```

   Il nuovo fuso orario sarà applicato immediatamente.

> **Note**
>
> È possibile assegnare il fuso orario UTC utilizzando il comando seguente:
>
> ```
> tzutil /s "UTC"
> ```

Per evitare che il fuso orario cambi dopo averlo impostato per Windows Server

Quando modifichi il fuso orario su un'istanza Windows, è necessario assicurarsi che il fuso orario venga mantenuto a seguito dei riavvii del sistema. In caso contrario, al riavvio dell'istanza, viene ripristinato l'orario in formato UTC. È possibile mantenere l'impostazione del fuso orario aggiungendo una chiave di RealTimeIsUniversal registro. Questa chiave è impostata per impostazione predefinita su tutte le istanze della generazione attuale. Per verificare se la chiave RealTimeIsUniversal del Registro di sistema è impostata, vedi la fase 4 nella procedura seguente. Se la chiave non è impostata attieniti alla seguente procedura dall'inizio.

Per impostare la chiave di RealTimeIsUniversal registro

1. Dall'istanza, aprire una finestra del prompt dei comandi.

2. Utilizzare il comando seguente per aggiungere la chiave di registro:

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /
v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. Se si utilizza un'AMI Windows Server 2008 (non Windows Server 2008 R2) creata prima del 22 febbraio 2013, è consigliabile eseguire l'aggiornamento all'AMI AWS Windows più recente. Se utilizzi un'AMI che esegue Windows Server 2008 R2 (non Windows Server 2008), è necessario verificare che sia installato l'aggiornamento rapido di Microsoft KB2922223. Se questo hotfix non è installato, si consiglia di eseguire l'aggiornamento all'AMI AWS Windows più recente.
4. (Opzionale) Verificare che il salvataggio della chiave da parte dell'istanza sia riuscito tramite il comando seguente:

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
\TimeZoneInformation" /s
```

Questo comando restituisce le sottochiavi per la chiave di registro TimeZoneInformation. Alla fine dell'elenco dovrebbe essere visualizzata una chiave RealTimeIsUniversal simile alla seguente:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                            REG_DWORD     0x1e0
    DaylightBias                    REG_DWORD     0xffffffc4
    DaylightName                    REG_SZ        @tzres.dll,-211
    DaylightStart                   REG_BINARY    00000300020002000000000000000000
    StandardBias                    REG_DWORD     0x0
    StandardName                    REG_SZ        @tzres.dll,-212
    StandardStart                   REG_BINARY    00000B0001000200000000000000000
    TimeZoneKeyName                 REG_SZ        Pacific Standard Time
    DynamicDaylightTimeDisabled     REG_DWORD     0x0
    ActiveTimeBias                  REG_DWORD     0x1a4
    RealTimeIsUniversal             REG_DWORD     0x1
```

Controllo dello stato del processore per l'istanza Amazon EC2 Linux

Gli stati C-state controllano i livelli di sospensione in cui può entrare un core quando è inattivo. Gli stati C-state sono numerati a partire da C0 (lo stato più superficiale in cui il core è completamente attivo ed esegue le istruzioni) fino a C6 (lo stato inattivo più profondo in cui un core è spento).

Gli stati P-state controllano le prestazioni desiderate (in frequenza CPU) da un core. Gli stati P-state sono numerati a partire da P0 (l'impostazione sulle prestazioni più elevate in cui è permesso al core di utilizzare la tecnologia Intel Turbo Boost per aumentare la frequenza, se possibile) e vanno da P1 (lo stato P-state che richiede la frequenza di base massima) a P15 (la frequenza più bassa possibile).

Stati C e stati P

I tipi di istanza seguenti consentono a un sistema operativo di controllare gli stati C-state e P-state del processore:

- Scopo generale: `m4.10xlarge` `m4.16xlarge` | `m5.metal` | | `m5d.metal` | `m5n.metal` | `m5zn.metal` | `m6i.metal` | `m6id.metal` | `m7a.metal-48xl` | `m7i.metal-24xl` `m7i.metal-48xl`
- Calcolo ottimizzato: `c4.8xlarge` | `c5.metal` | `c5an.metal` | `c5adn.metal` | `c5n.metal` | `c6i.metal` | `c6id.metal` | `c7a.metal-48xl` | `c7i.metal-24xl` | `c7i.metal-48xl`
- Memoria ottimizzata: `r4.8xlarge` `r4.16xlarge` `r5.metal` `r5b.metal` | `r5d.metal` | `r6i.metal` | `r7a.metal-48xl` | `r7i.metal-24xl` | `r7i.metal-48xl` | `r7iz.metal-16xl` | `r7iz.metal-32xl` | `u-6tb1.metal` | `u-9tb1.metal` | `u-12tb1.metal` `u-18tb1.metal` | `u-24tb1.metal` | `x1.16xlarge` | `x1.32xlarge` | `x1e.8xlarge` | `x1e.16xlarge` | `x1e.32xlarge` | `z1d.metal`
- Archiviazione ottimizzato: `d2.8xlarge` | `d3.metal` | `d3en.metal` | `i3.8xlarge` | `i3.16xlarge` | `i3.metal` | `i3en.metal` | `h1.8xlarge` | `h1.16xlarge`
- Elaborazione accelerata: `f1.16xlarge` | `g3.16xlarge` | `g4dn.metal` | `p2.16xlarge` | `p3.16xlarge`

Solo stati C

I tipi di istanza seguenti consentono a un sistema operativo di controllare gli stati C-state del processore:

- Uso generale: `m5.12xlarge` `m5.24xlarge` | `m5d.12xlarge` | `m5d.24xlarge` | `m5n.12xlarge` | `m5n.24xlarge` | `m5dn.12xlarge` | `m5dn.24xlarge` | `m6a.24xlarge` | `m6a.48xlarge` `m6ad.metal` | `m6i.16xlarge` | `m6i.32xlarge` | `m7a.medium` | `m7a.large` | `m7a.xlarge` | `m7a.2xlarge` | `m7a.4xlarge` `m7a.8xlarge` | `m7a.12xlarge` | `m7a.16xlarge` | `m7a.24xlarge` | `m7a.32xlarge` | `m7a.48xlarge` | `m7i.large` | `m7i.xlarge` | `m7i.2xlarge` `m7i.4xlarge` | `m7i.8xlarge` | `m7i.12xlarge` | `m7i.16xlarge` | `m7i.24xlarge` | `m7i.48xlarge`

- Ottimizzato per il calcolo: c5.9xlarge c5.12xlarge c5.18xlarge | c5.24xlarge | c5a.24xlarge | c5ad.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5n.9xlarge | c5n.18xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge | c6i.16xlarge | | c6i.32xlarge | c7a.medium | c7a.large | c7a.xlarge | c7a.2xlarge | c7a.4xlarge | c7a.8xlarge | c7a.12xlarge | c7a.16xlarge | c7a.24xlarge | c7a.32xlarge | c7a.48xlarge | c7i.large | c7i.xlarge | c7i.2xlarge | c7i.4xlarge | c7i.8xlarge | c7i.12xlarge | c7i.16xlarge | c7i.24xlarge c7i.48xlarge
- Memoria ottimizzata: r5.12xlarge r5.24xlarge r5d.12xlarge | r5d.24xlarge | r5n.12xlarge | r5n.24xlarge r5dn.12xlarge | r5dn.24xlarge | r6a.24xlarge | r6a.48xlarge | r6i.16xlarge | r6i.32xlarge | r6id.32xlarge | r6in.32xlarge | r7a.medium | r7a.large | r7a.xlarge | r7a.2xlarge | r7a.4xlarge | r7a.8xlarge | r7a.12xlarge | r7a.16xlarge | r7a.24xlarge | r7a.32xlarge | r7a.48xlarge | r7i.large r7i.xlarge | r7i.2xlarge | r7i.4xlarge | r7i.8xlarge | r7i.12xlarge | r7i.16xlarge | r7i.24xlarge | r7i.48xlarge | r7iz.large | r7iz.xlarge | r7iz.2xlarge r7iz.4xlarge| r7iz.8xlarge | r7iz.12xlarge | r7iz.16xlarge | r7iz.32xlarge | u-6tb1.56xlarge | u-6tb1.112xlarge | u-9tb1.112xlarge | u-12tb1.112xlarge | u-18tb1.112xlarge | u-24tb1.112xlarge | u7i-12tb.224xlarge | u7in-16tb.224xlarge | u7in-24tb.224xlarge | u7in-32tb.224xlarge | z1d.6xlarge | z1d.12xlarge
- Ottimizzate per l'archiviazione: d3en.12xlarge | dl1.24xlarge | i3en.12xlarge | i3en.24xlarge | i4i.metal | r5b.12xlarge | r5b.24xlarge | i4i.16xlarge
- Calcolo accelerato: dl1.24xlarge | g5.24xlarge | | g5.48xlarge | g6.24xlarge | g6.48xlarge | inf1.24xlarge | | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge vt1.24xlarge

AWS I processori Graviton dispongono di modalità di risparmio energetico integrate e funzionano a frequenza fissa. Pertanto, non offrono al sistema operativo la possibilità di controllare gli stati C e gli stati P.

Potresti modificare le impostazioni degli stati C-state o P-state per aumentare la consistenza delle prestazioni del processore, ridurre la latenza oppure ottimizzare l'istanza per un carico di lavoro specifico. Le impostazioni predefinite degli stati C-state e P-state forniscono le prestazioni massime, ottimali per la maggior parte dei carichi di lavoro. Tuttavia, se l'applicazione traesse vantaggio dalla latenza ridotta al costo di frequenze single-core o dual-core più elevate o da prestazioni coerenti

a frequenze più basse anziché frequenze Turbo Boost intermittenti, consigliamo di prendere in considerazione le impostazioni degli stati C-state o P-state disponibili per queste istanze.

Per informazioni sulle diverse configurazioni dei processori e su come monitorare gli effetti della configurazione per Amazon Linux, consulta Processor state control for Amazon EC2 Amazon Linux instance nella Amazon Linux 2 User Guide. Queste procedure sono state scritte e si applicano ad Amazon Linux; tuttavia, potrebbero funzionare anche per altre distribuzioni Linux con un kernel Linux 3.9 o successivo. Per ulteriori informazioni su altre distribuzioni Linux e sul controllo degli stati del processore, consultare la documentazione specifica del sistema.

Ottimizzazione delle opzioni della CPU

Molte istanze Amazon EC2 supportano il multithreading simultaneo, che consente l'esecuzione simultanea di più thread su un singolo core CPU. Ciascun thread è rappresentato come una CPU virtuale (vCPU) sull'istanza. Un'istanza ha un numero predefinito di core CPU, variabile in base al tipo di istanza. Ad esempio, un tipo di istanza `m5.xlarge` ha due core CPU e due thread per core per impostazione predefinita, per un totale— di quattro vCPU.

> **Note**
>
> Ogni vCPU è un thread di un core CPU, ad eccezione delle istanze T2, M7a, Mac processore Apple e delle piattaforme ARM a 64 bit, come le istanze alimentate da processori AWS Graviton.

Nella maggior parte dei casi, è presente un tipo di istanza Amazon EC2 con una combinazione di memoria e numero di vCPU adatta ai tuoi carichi di lavoro. Tuttavia, puoi specificare le seguenti opzioni CPU per ottimizzare la tua istanza per carichi di lavoro specifici o determinate esigenze aziendali:

- Numero di core CPU: è possibile personalizzare il numero di core CPU per l'istanza. Questo ti offre la possibilità di ottimizzare i costi di licenza del software con un'istanza dotata di una quantità sufficiente di RAM per carichi di lavoro a memoria elevata ma di un numero minore di core CPU.
- Thread per core: è possibile disabilitare la tecnologia multithreading specificando un singolo thread per core CPU. Potresti scegliere questa opzione per determinati carichi di lavoro, come quelli high performance computing (HPC).

È possibile specificare queste opzioni CPU durante l'avvio dell'istanza. Questa operazione non comporta costi supplementari. Ti vengono addebitati gli stessi costi delle istanze avviate con opzioni CPU predefinite.

Indice

Regole per specificare le opzioni CPU

Per specificare le opzioni CPU per l'istanza, tieni conto delle seguenti regole:

- Non è possibile specificare le opzioni della CPU per le istanze bare metal.
- Le opzioni CPU possono essere specificate solo durante l'avvio dell'istanza e non possono essere modificate in seguito.
- Quando avvii un'istanza, è necessario specificare sia il numero di core CPU sia i thread per core nella richiesta. Per esempi di richieste, vedi Specifica delle opzioni CPU per l'istanza.
- Il numero di vCPU per l'istanza corrisponde al numero di core CPU moltiplicato per thread per core. Per specificare un numero di vCPU personalizzato, è necessario specificare un numero di core CPU valido e i thread per core per il tipo di istanza. Non puoi superare il numero di vCPU predefinito per l'istanza. Per ulteriori informazioni, consulta Core CPU e thread per core CPU per tipo di istanza.
- Per disabilitare il multithreading, specifica un solo thread per core.
- Se modifichi il tipo di istanza di un'istanza esistente, le opzioni CPU passano automaticamente alle opzioni CPU predefinite per il nuovo tipo di istanza.
- Le opzioni CPU specificate restano invariate dopo l'arresto, l'avvio o il riavvio di un'istanza.

Core CPU e thread per core CPU per tipo di istanza

Nelle seguenti tabelle vengono descritti i tipi di istanze che supportano la specifica di opzioni CPU.

Indice

- Istanze a calcolo ottimizzato
- Istanze con memoria ottimizzata
- Istanze con storage ottimizzato
- Istanze di calcolo accelerate
- Istanze di High Performance Computing

Istanze per uso generale

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m2.xlarge	2	2	1	1, 2	1
m2.2xlarge	4	4	1	1, 2, 3, 4	1
m2.4xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m3.large	2	1	2	1	1, 2
m3.xlarge	4	2	2	1, 2	1, 2
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2	1	2	1	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6a.large	2	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6id.large	2	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7i-flex.large	2	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
t3.nano	2	1	2	1	1, 2
t3.micro	2	1	2	1	1, 2
t3.small	2	1	2	1	1, 2
t3.medium	2	1	2	1	1, 2
t3.large	2	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2	1	2	1	1, 2
t3a.micro	2	1	2	1	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Istanze a calcolo ottimizzato

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c3.large	2	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c4.large	2	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c6a.large	2	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1, 2, 3, 4	1
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6id.large	2	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7i-flex.large	2	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Istanze con memoria ottimizzata

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r3.large	2	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5dn.xlarge	4	2	2	1, 2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6idn.large	2	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2	1	2	1	1, 2
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7iz.large	2	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8g.large	2	2	1	1, 2	1
r8g.xlarge	4	4	1	1, 2, 3, 4	1
r8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 98,, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				168, 170, 172, 174, 176, 178, 182, 184, 186, 188, 190, 192	
u-3tb1.56xlarge	224	112	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2
u-6tb1.56xlarge	224	224	1	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u-6tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-9tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u-12tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-18tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u-24tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7i-12tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 248, 256, 264, 272, 280, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7in-16tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 248, 256, 264, 272, 280, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7in-24tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 248, 256, 264, 272, 280, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7in-32tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 248, 256, 264, 272, 280, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
z1d.large	2	1	2	1	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
z1d.xlarge	4	2	2	1, 2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Istanze con storage ottimizzato

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
i3.large	2	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i3en.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
i4g.large	2	2	1	1, 2	1
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Istanze di calcolo accelerate

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28,	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
f1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
f1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
p2.xlarge	4	2	2	1, 2	1, 2
p2.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p2.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
p3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
trn1.2xlarge	8	4	2	2, 4	1, 2
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

Istanze di High Performance Computing

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
hpc6id.32xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				48, 50, 52, 54, 56, 58, 60, 62, 64	

Specifica delle opzioni CPU per l'istanza

Puoi specificare le opzioni CPU durante l'avvio dell'istanza.

Gli esempi seguenti descrivono come specificare le opzioni della CPU quando si utilizza la procedura guidata di avvio dell'istanza nella console EC2 e il AWS CLI comando run-instances, nonché la pagina di creazione del modello di avvio nella console EC2 e il create-launch-template AWS CLI comando. Per il parco istanze o la serie di istanze spot EC2, devi specificare le opzioni della CPU in un modello di avvio.

Gli esempi seguenti riguardano un tipo di istanza `r5.4xlarge`, caratterizzato dai valori predefiniti riportati di seguito:

- Core CPU predefiniti: 8
- Thread per core predefiniti: 2
- vCPU predefinite: 16 (8 * 2)
- Numero valido di core CPU: 2, 4, 6, 8
- Numero valido di thread per core: 1, 2

Disabilitazione del multithreading

Per disabilitare il multithreading, specifica un solo thread per core.

New console

Per disabilitare il multithreading durante l'avvio dell'istanza

1. Segui la procedura Avvio rapido di un'istanza e configura l'istanza in base alle esigenze.
2. Espandi Dettagli avanzati e seleziona la casella di controllo Specifica le opzioni della CPU.

3. Per Core count (Numero di core), selezionare il numero di core CPU richiesti. In questo esempio, per specificare il numero di core CPU predefinito per un'istanza `r5.4xlarge`, scegliere 8.
4. Per disabilitare il multithreading per Threads per core (Thread per core), selezionare 1.
5. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Old console

Per disabilitare il multithreading durante l'avvio dell'istanza

1. Seguire la procedura Avvio di un'istanza tramite la vecchia procedura guidata di avvio.
2. Nella pagina Configure Instance Details (Configura dettagli istanza), per CPU options (Opzioni CPU), scegliere Specify CPU options (Specifica opzioni CPU).
3. Per Core count (Numero di core), selezionare il numero di core CPU richiesti. In questo esempio, per specificare il numero di core CPU predefinito per un'istanza `r5.4xlarge`, scegliere 8.
4. Per disabilitare il multithreading per Threads per core (Thread per core), selezionare 1.
5. Continuare come richiesto dalla procedura guidata. Dopo avere esaminato le opzioni nella pagina Rivedere l'avvio dell'istanza, scegliere Launch (Avvia). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la vecchia procedura guidata di avvio.

AWS CLI

Per disabilitare il multithreading durante l'avvio dell'istanza

Utilizzare il comando della AWS CLI run-instances e specificare il valore 1 per `ThreadsPerCore` per il parametro `--cpu-options`. Per `CoreCount`, specificare il numero di core CPU. In questo esempio, per specificare il numero di core CPU predefinito per un'istanza `r5.4xlarge`, specificare un valore di 8.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Specifica di un numero personalizzato di vCPU all'avvio

È possibile personalizzare il numero di core CPU e di thread per core per l'istanza.

L'esempio seguente avvia un'`r5.4xlarge`istanza con 4 vCPU.

New console

Per specificare un numero personalizzato di vCPU durante l'avvio dell'istanza

1. Segui la procedura Avvio rapido di un'istanza e configura l'istanza in base alle esigenze.
2. Espandi Dettagli avanzati e seleziona la casella di controllo Specifica le opzioni della CPU.
3. Per ottenere 4 vCPU, specificare 2 core CPU e 2 thread per core, come segue:
   - Per Core count, scegli 2.
   - In Threads per core (Thread per core), scegliere 2.
4. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Old console

Per specificare un numero personalizzato di vCPU durante l'avvio dell'istanza

1. Seguire la procedura Avvio di un'istanza tramite la vecchia procedura guidata di avvio.
2. Nella pagina Configure Instance Details (Configura dettagli istanza), per CPU options (Opzioni CPU), scegliere Specify CPU options (Specifica opzioni CPU).
3. Per ottenere 4 vCPU, specificare 2 core CPU e 2 thread per core, come segue:
   - Per Core count, scegli 2.
   - In Threads per core (Thread per core), scegliere 2.
4. Continuare come richiesto dalla procedura guidata. Dopo avere esaminato le opzioni nella pagina Rivedere l'avvio dell'istanza, scegliere Launch (Avvia). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la vecchia procedura guidata di avvio.

AWS CLI

Per specificare un numero personalizzato di vCPU durante l'avvio dell'istanza

Utilizzate il AWS CLI comando run-instances e specificate il numero di core della CPU e il numero di thread nel parametro. `--cpu-options` È possibile specificare 2 core CPU e 2 thread per core per ottenere 4 vCPU.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=2,ThreadsPerCore=2" \
    --key-name MyKeyPair
```

In alternativa, specifica 4 core CPU e 1 thread per core (disabilita il multithreading) per ottenere 4 vCPU:

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=4,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Specifica di un numero personalizzato di vCPU in un modello di avvio

Puoi personalizzare il numero di core CPU e di thread per core per l'istanza in un modello di avvio.

L'esempio seguente crea un modello di avvio che specifica la configurazione per un'`r5.4xlarge`istanza con 4 vCPU.

Console

Per specificare un numero personalizzato di vCPU in un modello di avvio

1. Segui la procedura Crea un modello di lancio dai parametri e configura il modello di avvio in base alle esigenze.
2. Espandi Dettagli avanzati e seleziona la casella di controllo Specifica le opzioni della CPU.
3. Per ottenere 4 vCPU, specificare 2 core CPU e 2 thread per core, come segue:
   - Per Core count, scegli 2.
   - In Threads per core (Thread per core), scegliere 2.
4. Nel pannello Riepilogo, verifica la configurazione dell'istanza, quindi scegli Crea modello di avvio. Per ulteriori informazioni, consulta Avvio di un'istanza da un modello di avvio.

AWS CLI

Per specificare un numero personalizzato di vCPU in un modello di avvio

Utilizzate il create-launch-template AWS CLI comando e specificate il numero di core della CPU e il numero di thread nel `CpuOptions` parametro. È possibile specificare 2 core CPU e 2 thread per core per ottenere 4 vCPU.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForCPUOptions \
    --version-description CPUOptionsVersion1 \
    --launch-template-data file://template-data.json
```

Di seguito è riportato un file JSON di esempio che contiene i dati del modello di avvio, che includono le opzioni della CPU, per la configurazione dell'istanza per questo esempio.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":2,
        "ThreadsPerCore":2
    }
}
```

In alternativa, specifica 4 core CPU e 1 thread per core (disabilita il multithreading) per ottenere 4 vCPU:

```
{
```

```
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":1
    }
}
```

Visualizzazione delle opzioni CPU per l'istanza

Puoi visualizzare le opzioni CPU per un'istanza esistente nella console Amazon EC2 o descrivendo l'istanza utilizzando AWS CLI.

Console

Per visualizzare le opzioni CPU di un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra scegliere Instances (Istanze) e selezionare l'istanza.
3. Nella scheda Details (Dettagli) in Host and placement group (Host e gruppo di collocamento), trovare Number of vCPUs (Numero di vCPU).

AWS CLI

Per visualizzare le opzioni CPU per un'istanza (AWS CLI)

Utilizzare il comando describe-instances.

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

```
...
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": "ec2-198-51-100-5.eu-central-1.compute.amazonaws.com",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "EbsOptimized": false,
            "LaunchTime": "2018-05-08T13:40:33.000Z",
            "PublicIpAddress": "198.51.100.5",
            "PrivateIpAddress": "172.31.2.206",
            "ProductCodes": [],
            "VpcId": "vpc-1a2b3c4d",
            "CpuOptions": {
                "CoreCount": 34,
                "ThreadsPerCore": 1
            },
            "StateTransitionReason": "",
            ...
        }
    ]
...
```

Nell'output restituito, il campo `CoreCount` indica il numero di core per l'istanza. Il campo `ThreadsPerCore` indica il numero di thread per core.

In alternativa, per visualizzare le informazioni sulla CPU, puoi connetterti all'istanza e utilizzare uno dei seguenti strumenti di sistema:

- Windows `Task Manager` sulla tua istanza di Windows
- Il lscpu comando sulla tua istanza Linux

È possibile AWS Config utilizzarlo per registrare, valutare, controllare e valutare le modifiche alla configurazione delle istanze, incluse le istanze terminate. Per ulteriori informazioni, consulta Nozioni di base su AWS Config nella AWS Config Guida per gli sviluppatori.

AMD SEV-SNP su Amazon EC2

AMD Secure Encrypted Virtualization-Secure Nested Paging (AMD SEV-SNP) è una funzionalità della CPU che fornisce le seguenti proprietà:

- Attestazione: AMD SEV-SNP consente di recuperare un rapporto di attestazione firmato che contiene una misura crittografica che può essere utilizzata per convalidare lo stato e l'identità dell'istanza e che è in esecuzione su hardware AMD originale. Per ulteriori informazioni, consulta Attestazione con AMD SEV-SNP.
- Crittografia della memoria: a partire dai processori AMD EPYC (Milano), AWS Graviton2 e Intel Xeon Scalable (Ice Lake), la memoria delle istanze è sempre crittografata. Le istanze abilitate per AMD SEV-SNP utilizzano una chiave specifica dell'istanza per la crittografia della memoria.

Concetti e terminologia

Prima di iniziare a utilizzare AMD SEV-SNP, assicurati di conoscere i concetti e la terminologia seguenti.

Rapporto di attestazione AMD SEV-SNP

Il rapporto di attestazione AMD SEV-SNP è un documento che un'istanza può richiedere alla CPU. Il rapporto di attestazione AMD SEV-SNP può essere utilizzato per convalidare lo stato e l'identità di un'istanza e per verificare che sia in esecuzione in un ambiente AMD autorizzato. Il rapporto include una misurazione di avvio, che è un hash crittografico dello stato di avvio iniziale di un'istanza, incluso il contenuto della memoria dell'istanza iniziale e lo stato iniziale delle vCPU. Il rapporto di attestazione AMD SEV-SNP è firmato con una firma VLEK che si ricollega a una root di fiducia AMD.

VLEK

La Versioned Loaded Endorsement Key (VLEK) è una chiave di firma con versioni certificata da AMD e utilizzata dalla CPU AMD per firmare i rapporti di attestazione AMD SEV-SNP. Le firme VLEK possono essere convalidate utilizzando i certificati forniti da AMD.

Binario OVMF

L'Open Virtual Machine Firmware (OVMF) è il codice di avvio anticipato utilizzato per fornire un ambiente UEFI per l'istanza. Il codice di avvio anticipato viene eseguito prima dell'avvio del codice nell'AMI. L'OVMF trova ed esegue anche il boot loader fornito nell'AMI. Per ulteriori informazioni, consulta il repository OVMF.

Requisiti

Per utilizzare AMD SEV-SNP, assicurati di:

- Utilizzare uno dei seguenti tipi di istanza supportati:
  - Uso generico: `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Ottimizzate per il calcolo: `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Ottimizzate per la memoria: `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Avvia l'istanza in un formato supportato. Regione AWS Attualmente sono supportate solo le Regioni Stati Uniti orientali (Ohio) ed Europa (Irlanda).
- Utilizzare un'AMI con modalità di avvio `uefi` oppure `uefi-preferred` e un sistema operativo che supporti AMD SEV-SNP. Per ulteriori informazioni sul supporto AMD SEV-SNP sul tuo sistema operativo, consulta la documentazione del rispettivo sistema operativo. Infatti AWS, AMD SEV-SNP è supportato su AL2023, RHEL 9.3, SLES 15 SP4 e Ubuntu 23.04 e versioni successive.

Considerazioni

È possibile attivare AMD SEV-SNP solo quando si avvia un'istanza. Quando AMD SEV-SNP è attivato per il lancio dell'istanza, si applicano le seguenti regole.

- AMD SEV-SNP non può essere disattivato. Rimane attivo per tutto il ciclo di vita dell'istanza.
- È possibile modificare il tipo di istanza solo con un altro tipo di istanza che supporti AMD SEV-SNP.
- Hibernation e Nitro Enclaves non sono supportati.
- Gli host dedicati non sono supportati.
- Se l'host sottostante della tua istanza è programmato per la manutenzione, riceverai una notifica sull'evento pianificato 14 giorni prima dell'evento. È necessario interrompere o riavviare manualmente l'istanza per spostarla su un nuovo host.

Prezzi

Quando avvii un'istanza Amazon EC2 con AMD SEV-SNP attivato, ti viene addebitata una tariffa di utilizzo oraria aggiuntiva equivalente al 10 percento della tariffa oraria on demand del tipo di istanza selezionato.

Questa tariffa per l'utilizzo di AMD SEV-SNP è un costo applicato separatamente dall'utilizzo dell'istanza Amazon EC2. Le istanze riservate, Savings Plans e l'utilizzo del sistema operativo non influiscono su questa tariffa.

Se si configura un'istanza spot per l'avvio con AMD SEV-SNP attivato, viene addebitata una tariffa di utilizzo oraria aggiuntiva equivalente al 10% della tariffa oraria on demand del tipo di istanza selezionato. Se la strategia di allocazione utilizza il prezzo come input, il parco istanze spot non include questa tariffa aggiuntiva; viene utilizzato solo il prezzo spot.

Lavora con AMD SEV-SNP su Amazon EC2

Completa le seguenti attività per lavorare con AMD SEV-SNP su Amazon EC2.

Attività

- Individuazione dei tipi di istanza supportati
- Attivazione di AMD SEV-SNP all'avvio
- Verifica dello stato di AMD SEV-SNP

Individuazione dei tipi di istanza supportati

Puoi utilizzarlo AWS CLI per trovare tipi di istanze che supportano AMD SEV-SNP.

Per trovare i tipi di istanza che supportano AMD SEV-SNP utilizzando il, usa il AWS CLI seguente comando. describe-instance-types

```
$ C:\> aws ec2 describe-instance-types \
--filters Name=processor-info.supported-features,Values=amd-sev-snp \
--query 'InstanceTypes[*].InstanceType'
```

Output di esempio:

```
[
 "r6a.2xlarge",
 "m6a.large",
```

```
 "m6a.2xlarge",
 "r6a.xlarge",
 "c6a.16xlarge",
 "c6a.8xlarge",
 "m6a.4xlarge",
 "c6a.12xlarge",
 "r6a.4xlarge",
 "c6a.xlarge",
 "c6a.4xlarge",
 "c6a.2xlarge",
 "m6a.xlarge",
 "c6a.large",
 "r6a.large",
 "m6a.8xlarge"
]
```

Attivazione di AMD SEV-SNP all'avvio

È possibile utilizzare il AWS CLI per avviare un'istanza con AMD SEV-SNP attivato.

Per avviare un'istanza con AMD SEV-SNP attivato utilizzando il AWS CLI, usa il comando e includi l'run-instancesopzione. `--cpu-options AmdSevSnp=enabled` Per `--image-id`, specifica un'AMI con modalità di avvio `uefi` oppure `uefi-prefered` e un sistema operativo che supporti AMD SEV-SNP. Per `--instance-type`, specifica un tipo di istanza supportato.

```
$ C:\> aws ec2 run-instances \
--image-id supported_ami_id \
--instance-type supported_instance_type \
--key-name key_pair_name \
--subnet-id subnet_id \
--cpu-options AmdSevSnp=enabled
```

Verifica dello stato di AMD SEV-SNP

È possibile utilizzare uno dei seguenti metodi per verificare lo stato di AMD SEV-SNP.

AWS CLI

Per verificare se AMD SEV-SNP è attivato per un'istanza che utilizza il, usa il comando. AWS CLIdescribe-instances Per `--instance-ids`, specifica l'ID dell'istanza da controllare.

```
$ C:\> aws ec2 describe-instances --instance-ids instance_id
```

Nell'output del comando, il valore per `AmdSevSnp` in `CpuOptions` indica se AMD SEV-SNP è attivato o disattivato.

AWS CloudTrail

Nel AWS CloudTrail caso della richiesta di avvio dell'istanza, il valore di `"cpuOptions": {"AmdSevSnp": enabled}` indica che AMD SEV-SNP è attivato per l'istanza.

Attestazione con AMD SEV-SNP

L'attestazione è un processo che consente all'istanza di dimostrare il suo stato e la sua identità. Quando attivi AMD SEV-SNP per un'istanza, puoi richiedere un rapporto di attestazione AMD SEV-SNP al processore sottostante. Il rapporto di attestazione AMD SEV-SNP contiene un hash crittografico, chiamato misurazione dell'avvio, del contenuto iniziale della memoria guest e dello stato iniziale della vCPU. Il rapporto di attestazione è firmato con una firma VLEK che si ricollega a una root di fiducia AMD. È possibile utilizzare la misurazione di avvio inclusa nel rapporto di attestazione per verificare che l'istanza sia in esecuzione in un ambiente AMD originale e per convalidare il codice di avvio iniziale utilizzato per avviare l'istanza.

Per eseguire l'attestazione con AMD SEV-SNP, esegui la procedura descritta di seguito.

Fase 1: ottenimento del rapporto di attestazione

In questo passaggio, si installa e si crea l'`snpguest`utilità, quindi la si utilizza per richiedere il rapporto di attestazione e i certificati AMD SEV-SNP.

1. Esegui i seguenti comandi per creare l'`snpguest`utilità da. snpguest repository

```
$ C:\> git clone https://github.com/virtee/snpguest.git
$ C:\> cd snpguest
$ C:\> cargo build -r
$ C:\> cd target/release
```

2. Genera una richiesta per il rapporto di attestazione. L'utilità richiede il rapporto di attestazione dall'host e lo scrive in un file binario con i dati di richiesta forniti.

   L'esempio seguente crea una stringa di richiesta casuale e la utilizza come file di richiesta (`request-file.txt`). Quando il comando restituisce il rapporto di attestazione, viene memorizzato nel percorso del file specificato (`report.bin`). In questo caso, l'utilità memorizza il report nella directory corrente.

```
$ C:\> ./snpguest report report.bin request-file.txt --random
```

3. Richiedete i certificati dalla memoria host e archiviateli come file PEM. L'esempio seguente memorizza i file nella stessa directory dell'`snpguest`utilità. Se i certificati esistono già nella directory specificata, tali certificati vengono sovrascritti.

```
$ C:\> ./snpguest certificates PEM ./
```

Fase 2: Convalida della firma del rapporto di attestazione

Il rapporto di attestazione è firmato con un certificato, denominato Versioned Loaded Endorsement Key (VLEK), rilasciato da AMD per. AWS In questo passaggio, puoi verificare che il certificato VLEK sia emesso da AMD e che il rapporto di attestazione sia firmato da quel certificato VLEK.

1. Scarica la radice dei certificati di fiducia VLEK dal sito Web ufficiale di AMD nella directory corrente.

```
$ C:\> sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/
Milan/cert_chain -o ./cert_chain.pem
```

2. Utilizza `openssl` per convalidare che il certificato VLEK sia firmato dai certificati root di fiducia di AMD.

```
$ C:\> sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
```

Output previsto:

```
certs/vcek.pem: OK
```

3. Utilizza l'utilità `snpguest` per convalidare che il rapporto di attestazione sia firmato dal certificato VLEK.

```
$ C:\> ./snpguest verify attestation ./ report.bin
```

Output previsto.

```
Reported TCB Boot Loader from certificate matches the attestation report.
Reported TCB TEE from certificate matches the attestation report.
```

```
Reported TCB SNP from certificate matches the attestation report.
Reported TCB Microcode from certificate matches the attestation report.
VEK signed the Attestation Report!
```

Aggiungere componenti di sistema Windows utilizzando i supporti di installazione

I sistemi operativi Windows Server includono molti componenti opzionali. L'installazione di tutti i componenti opzionali in ciascuna AMI Amazon EC2 Windows Server non è una soluzione pratica. Ti forniamo invece snapshot EBS dei supporti di installazione contenenti i file necessari per configurare o installare i componenti sulle istanze Windows.

Per accedere ai componenti opzionali e installarli, devi individuare lo snapshot EBS corretto per la versione in uso di Windows Server, creare un volume dallo snapshot e collegare il volume all'istanza specifica.

Prima di iniziare

Utilizza AWS Management Console o uno strumento da riga di comando per ottenere l'ID dell'istanza e la zona di disponibilità dell'istanza. Devi creare il volume EBS nella stessa zona di disponibilità dell'istanza.

Aggiunta di componenti di Windows mediante la console

Utilizza la procedura seguente per AWS Management Console aggiungere componenti Windows all'istanza.

Per aggiungere i componenti di Windows all'istanza mediante la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Snapshots (Snapshot).
3. Nella barra Filter (Filtro), scegliere Public Snapshots (Snapshot pubbliche).
4. Aggiungere il filtro Owner (Proprietario) e scegliere Amazon images (Immagini Amazon).
5. Aggiungere il filtro Description (Descrizione) e digitare **`Windows`**.
6. Premere Invio.

7. Selezionare lo snapshot corrispondente all'architettura del sistema e alla preferenza di lingua. Ad esempio, selezionare Windows 2019 English Installation Media (Supporto di installazione Windows 2019 in lingua inglese) se l'istanza in uso esegue Windows Server 2019.
8. Scegliere Actions (Operazioni),Create volume from snapshot (Crea volume da snapshot).
9. In Availability Zone (Zona di disponibilità), selezionare la zona di disponibilità corrispondente all'istanza di Windows. Scegliere Add tag (Aggiungi tag) e specificare **`Name`** per la chiave tag e un nome descrittivo per il valore del tag. Selezionare Create volume (Crea volume).
10. Nel messaggio Successfully created volume (Volume creato correttamente), scegliere il volume appena creato.
11. Scegliere Actions (Operazioni), Attach Volume (Collega volume).
12. Da Instance (Istanza), selezionare l'ID dell'istanza.
13. Per Device name (Nome dispositivo), inserire il nome del dispositivo per l'allegato. In caso di dubbi con il nome del dispositivo, consultare Nomi dei dispositivi sulle istanze Amazon EC2.
14. Scegli Attach volume (Collega volume).
15. Connettersi all'istanza e rendere disponibile il volume. Per ulteriori informazioni, consulta Rendere disponibile un volume Amazon EBS per l'uso nella Amazon EBS User Guide.

    > **Important**
    >
    > Non inizializzare il volume.

16. Aprire Control Panel (Pannello di controllo), Programs and Features (Programmi e funzionalità). Scegliere Turn Windows features on or off (Attiva o disattiva funzionalità di Windows). Se viene richiesto il supporto di installazione, specificare il volume EBS contenente il supporto di installazione.
17. (Facoltativo) Dopo aver terminato con il supporto di installazione, è possibile scollegare il volume. Dopo aver scollegato il volume, è possibile eliminarlo.

Aggiungi componenti Windows utilizzando gli strumenti per Windows PowerShell

Utilizza la procedura seguente per utilizzare gli Strumenti per Windows PowerShell per aggiungere componenti di Windows all'istanza.

Aggiungi componenti Windows all'istanza utilizzando gli Strumenti per Windows PowerShell

1. Utilizza il Get-EC2Snapshotcmdlet con i `description` filtri `Owner` and per ottenere un elenco delle istantanee dei supporti di installazione disponibili.

```
PS C:\> Get-EC2Snapshot -Owner amazon -Filter @{ Name="description";
 Values="Windows*" }
```

2. Facendo riferimento all'output annotare l'ID dello snapshot corrispondente all'architettura del sistema e alla preferenza di lingua. Per esempio:

```
...
DataEncryptionKeyId :
Description         : Windows 2019 English Installation Media
Encrypted           : False
KmsKeyId            :
OwnerAlias          : amazon
OwnerId             : 123456789012
Progress            : 100%
SnapshotId          : snap-22da283e
StartTime           : 10/25/2019 8:00:47 PM
State               : completed
StateMessage        :
Tags                : {}
VolumeId            : vol-be5eafcb
VolumeSize          : 6
...
```

3. Utilizzare il New-EC2Volumecmdlet per creare un volume dall'istantanea. Specificare la stessa zona di disponibilità dell'istanza.

```
PS C:\> New-EC2Volume -AvailabilityZone us-east-1a -VolumeType gp2 -
SnapshotId snap-22da283e
```

4. Facendo riferimento all'output, annotare l'ID del volume.

```
Attachments      : {}
AvailabilityZone : us-east-1a
CreateTime       : 4/18/2017 10:50:25 AM
Encrypted        : False
Iops             : 100
KmsKeyId         :
```

```
Size             : 6
SnapshotId       : snap-22da283e
State            : creating
Tags             : {}
VolumeId         : vol-06aa9e1fbf8b82ed1
VolumeType       : gp2
```

5. Utilizzare il Add-EC2Volumecmdlet per collegare il volume all'istanza.

```
PS C:\> Add-EC2Volume -InstanceId i-087711ddaf98f9489 -
VolumeId vol-06aa9e1fbf8b82ed1 -Device xvdh
```

6. Connettersi all'istanza e rendere disponibile il volume. Per ulteriori informazioni, consulta Rendere disponibile un volume Amazon EBS per l'uso nella Amazon EBS User Guide.

> **Important**
>
> Non inizializzare il volume.

7. Aprire Control Panel (Pannello di controllo), Programs and Features (Programmi e funzionalità). Scegliere Turn Windows features on or off (Attiva o disattiva funzionalità di Windows). Se viene richiesto il supporto di installazione, specificare il volume EBS contenente il supporto di installazione.
8. (Facoltativo) Quando hai finito con il supporto di installazione, utilizza il Dismount-EC2Volumecmdlet per scollegare il volume dall'istanza. Dopo aver scollegato il volume, è possibile utilizzare il Remove-EC2Volumecmdlet per eliminare il volume.

Aggiungere i componenti di Windows utilizzando il AWS CLI

Utilizza la procedura seguente per AWS CLI aggiungere componenti Windows all'istanza.

Per aggiungere componenti Windows all'istanza utilizzando il AWS CLI

1. Utilizzare il comando describe-snapshots con il parametro `owner-ids` e il filtro `description` per recuperare l'elenco degli snapshot dei supporti di installazione disponibili.

```
aws ec2 describe-snapshots --owner-ids amazon --filters
 Name=description,Values=Windows*
```

2. Facendo riferimento all'output annotare l'ID dello snapshot corrispondente all'architettura del sistema e alla preferenza di lingua. Ad esempio:

```
{
    "Snapshots": [
    ...
        {
            "OwnerAlias": "amazon",
            "Description": "Windows 2019 English Installation Media",
            "Encrypted": false,
            "VolumeId": "vol-be5eafcb",
            "State": "completed",
            "VolumeSize": 6,
            "Progress": "100%",
            "StartTime": "2019-10-25T20:00:47.000Z",
            "SnapshotId": "snap-22da283e",
            "OwnerId": "123456789012"
        },
    ...
   ]
}
```

3. Utilizzare il comando create-volume per creare un volume dallo snapshot. Specificare la stessa zona di disponibilità dell'istanza.

```
aws ec2 create-volume --snapshot-id snap-22da283e --volume-type gp2 --availability-
zone us-east-1a
```

4. Facendo riferimento all'output, annotare l'ID del volume.

```
{
    "AvailabilityZone": "us-east-1a",
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-0c98b37f30bcbc290",
    "State": "creating",
    "Iops": 100,
    "SnapshotId": "snap-22da283e",
    "CreateTime": "2017-04-18T10:33:10.940Z",
    "Size": 6
}
```

5. Utilizzare il comando attach-volume per collegare il volume all'istanza.

```
aws ec2 attach-volume --volume-id vol-0c98b37f30bcbc290 --instance-
id i-01474ef662b89480 --device xvdg
```

6. Connettersi all'istanza e rendere disponibile il volume. Per ulteriori informazioni, consulta Rendere disponibile un volume Amazon EBS per l'uso nella Amazon EBS User Guide.

> **Important**
>
> Non inizializzare il volume.

7. Aprire Control Panel (Pannello di controllo), Programs and Features (Programmi e funzionalità). Scegliere Turn Windows features on or off (Attiva o disattiva funzionalità di Windows). Se viene richiesto il supporto di installazione, specificare il volume EBS contenente il supporto di installazione.
8. (Facoltativo) Al termine del supporto di installazione, utilizzare il comando detach-volume per scollegare il volume dall'istanza. Dopo aver scollegato il volume, è possibile utilizzare il comando delete-volume per eliminare il volume.

Gestisci gli utenti di sistema sulla tua istanza Linux

Ogni istanza Linux viene avviata con un utente predefinito del sistema Linux. Puoi aggiungere utenti alla tua istanza ed eliminare utenti.

Per l'utente predefinito, il nome utente predefinito viene determinato dall'AMI specificata quando hai avviato l'istanza.

> **Note**
>
> Per impostazione predefinita, l'autenticazione tramite password e l'accesso root sono disabilitati e sudo è abilitato. Per accedere alla tua istanza, devi usare una coppia di chiavi. Per ulteriori informazioni sull'accesso, consulta Connessione all'istanza di Linux.
> Puoi consentire l'autenticazione tramite password e l'accesso root per la tua istanza. Per ulteriori informazioni, consulta la documentazione relativa al sistema operativo in uso.

> **Note**
>
> Gli utenti del sistema Linux non devono essere confusi con gli utenti IAM. Per ulteriori informazioni, consulta Utenti IAM nella Guida per l'utente di IAM.

Indice

Nomi utente predefiniti

Il nome utente predefinito per un'istanza EC2 viene determinato dall'AMI specificata quando hai avviato l'istanza.

I nomi utente predefiniti sono:

- Per AL2023, Amazon Linux 2 o Amazon Linux AMI, il nome utente è `ec2-user`.
- Per un'AMI CentOS, il nome utente è `centos` o `ec2-user`.
- Per un'AMI Debian, il nome utente è `admin`.
- Per un'AMI Fedora, il nome utente è `fedora` o `ec2-user`.
- Per un'AMI RHEL, il nome utente è `ec2-user` o `root`.
- Per un'AMI SUSE, il nome utente è `ec2-user` o `root`.
- Per un'AMI Ubuntu, il nome utente è `ubuntu`.
- Per un'AMI Oracle, il nome utente è `ec2-user`.
- Per un'AMI Bitnami, il nome utente è `bitnami`.

> **Note**
>
> Per trovare il nome utente predefinito per altre distribuzioni Linux, rivolgiti al provider AMI.

Considerazioni

L'utilizzo dell'utente di default è adeguato per numerose applicazioni, ma puoi aggiungere altri utenti in modo tale che possano disporre di propri file e WorkSpace. Inoltre, la creazione di utenti per i nuovi utenti è una procedura più sicura rispetto alla concessione a più utenti (spesso inesperti) dell'accesso all'utente predefinito, dal momento che tale utente può causare seri problemi al sistema se viene utilizzato in modo inappropriato. Per ulteriori informazioni, consulta Suggerimenti per la sicurezza delle istanze EC2.

Per abilitare l'accesso SSH agli utenti per l'istanza EC2 utilizzando un utente del sistema Linux, devi condividere la chiave SSH con l'utente. In alternativa, puoi utilizzare EC2 Instance Connect per fornire accesso agli utenti senza necessità di condividere e gestire le chiavi SSH. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite EC2 Instance Connect.

Creazione di un utente

Prima crea l'utente e in seguito aggiungi la chiave pubblica SSH che permette all'utente di connettersi e accedere all'istanza.

Creazione di un utente

1. Creazione di una nuova coppia di chiavi. È necessario fornire il file `.pem` all'utente per il quale si sta creando l'utente. Gli utenti devono utilizzare questo file per connettersi all'istanza.
2. Recuperare la chiave pubblica dalla coppia di chiavi creata nella fase precedente.

   ```
   $ C:\>  ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
   ```

   Il comando restituisce la chiave pubblica, come illustrato nell'esempio seguente.

   ```
   ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
   +PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
   d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
   i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
   +CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
   +z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
   ```

3. Collegati all'istanza.

4. Utilizzare il comando adduser per creare l'utente e aggiungerlo al sistema (con una voce nel file `/etc/passwd`). Il comando crea anche un gruppo e una home directory per l'utente. In questo esempio, l'utente viene chiamato *`newuser`*.

   - Amazon Linux e Amazon Linux 2

     Con Amazon Linux e Amazon Linux 2, l'utente viene creato con l'autenticazione tramite password disabilitata per impostazione predefinita.

     ```
     [ec2-user ~]$ sudo adduser newuser
     ```

   - Ubuntu

     Includi il parametro `--disabled-password` per creare l'utente con l'autenticazione tramite password disabilitata.

     ```
     [ubuntu ~]$ sudo adduser newuser --disabled-password
     ```

5. Passare al nuovo utente in modo che la directory e il file che verranno creati siano associati a una proprietà idonea.

   ```
   [ec2-user ~]$ sudo su - newuser
   ```

   Il prompt cambia da `ec2-user` in *`newuser`* per indicare che si è passati dalla sessione di shell (interprete dei comandi) al nuovo utente.

6. Aggiungi la chiave pubblica SSH all'utente. Creare prima una directory nella home directory dell'utente per il file della chiave SSH, in seguito creare il file della chiave e infine incollare la chiave pubblica nel file della chiave, come descritto nelle seguenti fasi secondarie.

   a. Creare una directory `.ssh` nella home directory *`newuser`* e modificare le relative autorizzazioni file in `700` (solo il proprietario può leggere, scrivere o aprire la directory).

      ```
      [newuser ~]$ mkdir .ssh
      ```

      ```
      [newuser ~]$ chmod 700 .ssh
      ```

> **Important**
>
> Senza queste precise autorizzazioni file l'utente non sarà in grado di eseguire l'accesso.

b. Creare un file denominato `authorized_keys` nella home directory `.ssh` e modificare le relative autorizzazioni file in `600` (solo il proprietario può leggere o scrivere nel file).

```
[newuser ~]$ touch .ssh/authorized_keys
```

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

> **Important**
>
> Senza queste precise autorizzazioni file l'utente non sarà in grado di eseguire l'accesso.

c. Aprire il file `authorized_keys` con l'editor di testo preferito (ad esempio vim o nano).

```
[newuser ~]$ nano .ssh/authorized_keys
```

Incollare la chiave pubblica recuperata nella fase 2 nel file e salvare le modifiche.

> **Important**
>
> Assicurarsi di incollare la chiave pubblica in una riga continua. La chiave pubblica non deve essere divisa su più righe.

L'utente ora dovrebbe essere in grado di eseguire l'accesso all'istanza tramite l'utente *`newuser`* utilizzando la chiave privata corrispondente alla chiave pubblica aggiunta al file `authorized_keys`. Per ulteriori informazioni sui diversi metodi di connessione a un'istanza Linux, vedere Connessione all'istanza di Linux.

Rimuovere un utente

Se un utente non è più necessario, puoi rimuoverlo in modo che non possa più essere utilizzato.

Utilizza il comando userdel per rimuovere l'utente dal sistema. Quando si specifica il parametro `-r`, la home directory e lo spool di posta dell'utente vengono eliminati. Per conservare la home directory e lo spool di posta dell'utente, omettere il parametro `-r`.

```
[ec2-user ~]$ sudo userdel -r olduser
```

Imposta la password dell'amministratore di Windows per la tua istanza

Quando ti connetti a un'istanza Windows, è necessario specificare un account utente e una password che disponga dell'autorizzazione per accedere all'istanza. La prima volta che ti connetti a un'istanza, ti viene richiesto di specificare l'account dell'amministratore e la password predefinita.

Con le AMI AWS Windows per Windows Server 2012 R2 e versioni precedenti, Configurare un'istanza di Windows utilizzando il servizio EC2Config (legacy) genera la password predefinita. Con le AMI AWS Windows per Windows Server 2016 e 2019, Configurazione dell'istanza Windows tramite EC2Launch genera la password predefinita. Con le AMI AWS Windows per Windows Server 2022 e versioni successive, Configurare un'istanza Windows tramite EC2Launch v2 genera la password predefinita.

> **Note**
>
> Con Windows Server 2016 e versioni successive, l'opzione `Password never expires` è disattivata per l'amministratore locale. Con Windows Server 2012 R2 e versione precedente, l'opzione `Password never expires` è abilitata per l'amministratore locale.

Modifica della password dell'amministratore dopo la connessione

Quando ti connetti a un'istanza per la prima volta, ti consigliamo di modificare il valore predefinito della password dell'amministratore. La procedura seguente ti permette di modificare la password dell'amministratore per un'istanza Windows.

> **Important**
>
> Conserva la nuova password in un luogo sicuro. Non sarà possibile recuperarla tramite la console Amazon EC2. La console può solo recuperare la password predefinita. Se tenti di connetterti all'istanza utilizzando la password predefinita dopo averla modificata, riceverai un messaggio di errore "Your credentials did not work" (Le credenziali specificate non funzionano).

Per modificare la password dell'amministratore locale

1. Collegati all'istanza e apri il prompt dei comandi.
2. Esegui il comando riportato qui di seguito. Se la tua nuova password contiene caratteri speciali, racchiudila tra virgolette.

```
net user Administrator "new_password"
```

3. Conserva la nuova password in un luogo sicuro.

Modifica di una password persa o scaduta

Se perdi la password o questa scade, puoi generare una nuova password. Per le procedure di reimpostazione della password, consulta Reimpostazione di una password amministratore Windows persa o scaduta.

Gestisci i driver di dispositivo per la tua istanza Amazon EC2

Alcuni driver non sono preinstallati sull'AMI EC2 da cui si avvia. Altri potrebbero aver bisogno di aggiornamenti per sfruttare le funzionalità estese. I seguenti argomenti riguardano l'installazione, gli aggiornamenti e la configurazione di alcuni driver di dispositivo collegati alle istanze EC2.

Indice

Installa i driver NVIDIA sulla tua istanza Amazon EC2

Un'istanza con una GPU NVIDIA collegata, ad esempio un'istanza P3 o G4dn, deve avere installato il driver NVIDIA appropriato. A seconda del tipo di istanza, puoi scaricare un driver NVIDIA pubblico, scaricare un driver da Amazon S3 disponibile solo per i clienti AWS oppure utilizzare un'AMI con driver preinstallato.

Per installare i driver AMD su un'istanza con una GPU AMD collegata, ad esempio un'istanza G4ad, consulta. Installare i driver AMD Per installare i driver NVIDIA, consulta. Installare i driver NVIDIA

Indice

Tipi di driver NVIDIA

Di seguito sono riportati i principali tipi di driver NVIDIA che possono essere utilizzati con le istanze basate su GPU.

Driver Tesla

Questi driver sono destinati principalmente ai carichi di lavoro di calcolo che utilizzano le GPU per attività come calcoli in virgola mobile parallelizzati per il machine learning e le trasformazioni veloci di Fourier per applicazioni di calcolo ad alte prestazioni.

Driver GRID

Questi driver sono certificati per fornire prestazioni ottimali per le applicazioni di visualizzazione professionali che eseguono il rendering di contenuti come modelli 3D o video ad alta risoluzione. Puoi configurare i driver GRID per supportare due modalità. Le Quadro Virtual Workstation forniscono l'accesso a quattro display 4K per GPU. Le vApps GRID forniscono funzionalità di hosting di app RDSH.

Driver di gioco

Questi driver contengono ottimizzazioni per il gioco e vengono aggiornati frequentemente per migliorare le prestazioni. Supportano un singolo display 4K per GPU.

Modalità configurata

In Windows, i driver Tesla sono configurati per l'esecuzione in modalità Tesla Compute Cluster (TCC). I driver GRID e di gioco sono configurati per l'esecuzione in modalità WDDM (Windows Display Driver Model). In modalità TCC, la scheda è dedicata ai carichi di lavoro di calcolo. In modalità WDDM, la scheda supporta sia i carichi di lavoro di calcolo che quelli grafici.

Pannello di controllo NVIDIA

Il pannello di controllo NVIDIA è supportato con i driver GRID e Gaming. Non è supportato con i driver Tesla.

API supportate per Tesla, GRID e driver di gioco

- OpenCL, OpenGL e Vulkan
- NVIDIA CUDA e librerie correlate (ad esempio, cuDNN, TensorRT, nvJPEG e cuBLAS)
- NVENC per la codifica video e NVDEC per la decodifica video
- API solo per Windows: DirectX, Direct2D, accelerazione video DirectX, DirectX Raytracing

Driver disponibili per tipo di istanza

Nella tabella seguente vengono riepilogati i driver NVIDIA supportati per ogni tipo di istanza GPU.

Tipo di istanza	Driver Tesla	Driver GRID	Driver di gioco
G3	Sì	Sì	No
G4dn	Sì	Sì	Sì
G5	Sì	Sì	Sì
G5g	Sì [1]	No	No
G6	Sì	Sì	No

Tipo di istanza	Driver Tesla	Driver GRID	Driver di gioco
Gr 6	Sì	Sì	No
P2	Sì	No	No
P3	Sì	No	No
P4d	Sì	No	No
P4de	Sì	No	No

[1] Questo driver Tesla supporta anche applicazioni grafiche ottimizzate specifiche per la piattaforma ARM64

[2] Uso esclusivo delle AMI del Marketplace

Opzioni di installazione

Utilizza una delle seguenti opzioni per ottenere i driver NVIDIA necessari per l'istanza GPU.

Opzioni

- Opzione 1: AMI con i driver NVIDIA installati
- Opzione 2: driver NVIDIA pubblici
- Opzione 3: driver GRID (istanze G6, Gr6, G5, G4dn e G3)
- Opzione 4: driver di gioco NVIDIA (istanze G4dn e G5)

Opzione 1: AMI con i driver NVIDIA installati

AWS e NVIDIA offrono diverse Amazon Machine Images (AMI) fornite con i driver NVIDIA installati.

- Offerte di Marketplace con il driver Tesla
- Offerte di Marketplace con il driver GRID
- Offerte di Marketplace con il driver di gioco

Per esaminare le considerazioni che dipendono dalla piattaforma del sistema operativo (OS), scegli la scheda relativa alla tua AMI.

Linux

Per aggiornare la versione del driver installata utilizzando una di queste AMI, è necessario disinstallare i pacchetti NVIDIA dall'istanza per evitare conflitti di versione. Utilizza questo comando per disinstallare i pacchetti NVIDIA:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

Il pacchetto di kit di strumenti CUDA presenta dipendenze sui driver NVIDIA. Disinstallando i pacchetti NVIDIA, il kit di strumenti CUDA viene cancellato. Devi reinstallare questo kit di strumenti dopo avere installato il driver NVIDIA.

Windows

Se si crea un'AMI Windows personalizzata utilizzando una delle Marketplace AWS offerte, l'AMI deve essere un'immagine standardizzata creata con Windows Sysprep per garantire il funzionamento del driver GRID. Per ulteriori informazioni, consulta Creare un'AMI con Windows Sysprep.

Opzione 2: driver NVIDIA pubblici

Le opzioni offerte da AWS includono la licenza necessaria per il conducente. In alternativa, puoi installare i driver pubblici e usare la tua licenza. Per installare un driver pubblico, scaricalo dal sito NVIDIA come descritto qui.

In alternativa, puoi utilizzare le opzioni offerte da AWS anziché i conducenti pubblici. Per utilizzare un driver GRID su un'istanza P3, usa le Marketplace AWS AMI come descritto nell'Opzione 1. Per utilizzare un driver GRID su un'istanza G6, Gr6, G5, G4dn o G3, usa le Marketplace AWS AMI come descritto nell'Opzione 1 o installa i driver NVIDIA forniti da come descritto in. AWS Opzione 3: driver GRID (istanze G6, Gr6, G5, G4dn e G3)

Per scaricare un driver NVIDIA pubblico

Accedi alla tua istanza e scarica il driver NVIDIA a 64 bit appropriato per il tipo di istanza da http://www.nvidia.com/Download/Find.aspx. Per Tipo di prodotto, Serie di prodotti e Prodotto, utilizza le opzioni riportate nella seguente tabella.

Istanza	Tipo di prodotto	Serie di prodotti	Prodotto
G3	Tesla	M-Class	M60

Istanza	Tipo di prodotto	Serie di prodotti	Prodotto
G4dn	Tesla	T-Series	T4
G5 [1]	Tesla	Serie A	A10
G5g [2]	Tesla	T-Series	NVIDIA T4G
G6[3]	Tesla	Serie L	L4
Gr6 [3]	Tesla	Serie L	L4
P2	Tesla	Serie K	K80
P3	Tesla	Serie V	V100
P4d	Tesla	Serie A	A100
P4de	Tesla	Serie A	A100
P5 [4]	Tesla	Serie H	H100

[1] Le istanze G5 richiedono una versione del driver 470.00 o successiva.

[2] Le istanze G5 richiedono una versione del driver 470.82.01 o successiva. Il sistema operativo è Linux aarch64.

[3] Le istanze G6 e Gr6 richiedono la versione del driver 525.0 o successiva.

[4] istanze P5 richiedono la versione del driver 530 o successiva.

Per installare il driver NVIDIA sui sistemi operativi Linux, consulta la Guida rapida all'installazione dei driver NVIDIA.

Per installare il driver NVIDIA su Windows, segui questi passaggi:

1. Aprire la cartella in cui è stato scaricato il driver e avviare il file di installazione. Seguire le istruzioni per installare il driver e riavviare l'istanza come necessario.
2. Disabilita la scheda video denominata Scheda video di base Microsoft contrassegnata da un'icona di avviso utilizzando Gestione dispositivi. Installare le funzionalità Windows Media Foundation e Quality Windows Audio Video Experience.

> **Important**
>
> Non disattivare la scheda video denominata Scheda video remota di Microsoft. Se la Scheda video remota di Microsoft è disabilitata, la connessione potrebbe essere interrotta e i tentativi di connessione all'istanza dopo il riavvio potrebbero fallire.

3. Aprire Gestione dispositivi per verificare che la GPU funzioni correttamente.
4. Per ottenere prestazioni ottimali dalla GPU, completare le fasi di ottimizzazione in Ottimizza le impostazioni della GPU sulle istanze Amazon EC2.

Opzione 3: driver GRID (istanze G6, Gr6, G5, G4dn e G3)

Questi download sono disponibili solo per i clienti. AWS Effettuando il download, al fine di rispettare i requisiti della AWS soluzione di cui al Contratto di licenza per l'utente finale (EULA) di NVIDIA GRID Cloud, l'utente accetta di utilizzare il software scaricato solo per sviluppare AMI da utilizzare con l'hardware NVIDIA L4, NVIDIA A10G, NVIDIA Tesla T4 o NVIDIA Tesla M60. Installando il software, sarai vincolato dai termini del contratto di licenza con l'utente finale NVIDIA GRID Cloud End User License Agreement. Per informazioni sulla versione del driver NVIDIA GRID per il sistema operativo in uso, consulta NVIDIA® Virtual GPU (vGPU) Software Documentation sul sito Web di NVIDIA.

Considerazioni

- Le istanze G6 e Gr6 richiedono GRID 17 o versione successiva.
- Le istanze G5 richiedono GRID 13.1 o successivo (o GRID 12.4 o successivo).
- Le istanze G3 richiedono una risoluzione DNS AWS fornita per il funzionamento delle licenze GRID.
- IMDSv2 è supportato solo con il driver NVIDIA versione 14.0 o superiore.
- Per le istanze Windows, se si avvia l'istanza da un'AMI Windows personalizzata, l'AMI deve essere un'immagine standardizzata creata con Windows Sysprep per garantire il funzionamento del driver GRID. Per ulteriori informazioni, consulta Creare un'AMI con Windows Sysprep.
- GRID 17.0 e versioni successive non supportano Windows Server 2019.
- GRID 14.2 e versioni successive non supportano Windows Server 2016.
- GRID 17.0 e versioni successive non sono supportati con le istanze G3.

Amazon Linux e Amazon Linux 2

Come installare il driver NVIDIA GRID sull'istanza

1. Connessione a un'istanza Linux.
2. Installalo AWS CLI sulla tua istanza Linux e configura le credenziali predefinite. Per ulteriori informazioni, consulta Installazione dell' AWS CLI nella Guida per l'utente dell'AWS Command Line Interface .

   > **Important**
   >
   > Il tuo utente o ruolo deve disporre delle autorizzazioni concesse che contengono la politica ReadOnlyAccessAmazonS3. Per ulteriori informazioni, consulta la policy AWS gestita: AmazonS3 ReadOnlyAccess nella Guida per l'utente di Amazon Simple Storage Service.

3. Installare gcc e make, se non sono già installati.

   ```
   [ec2-user ~]$ sudo yum install gcc make
   ```

4. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

5. Riavviare l'istanza per caricare la versione più recente del kernel.

   ```
   [ec2-user ~]$ sudo reboot
   ```

6. Riconnettersi all'istanza dopo averla riavviata.
7. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

   ```
   [ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
   ```

8. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

   ```
   [ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
   ```

In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Se si utilizza Amazon Linux 2 con kernel versione 5.10, utilizzare il comando seguente per installare il driver GRID.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

11. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

12. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

14. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni NICE DCV.

    b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze basate su GPU Amazon EC2.

CentOS 7 e Red Hat Enterprise Linux 7

Come installare il driver NVIDIA GRID sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.
2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

6. Disattivare il driver open source `nouveau` per le schede grafiche NVIDIA.

a. Aggiungere nouveau al file di blacklist /etc/modprobe.d/blacklist.conf. Copiare il seguente blocco di codice e incollarlo in un terminale.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

b. Modificare il file /etc/default/grub e aggiungere la seguente riga:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Ricompilare il file di configurazione di Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

10. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

12. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

13. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni NICE DCV.

    b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze basate su GPU Amazon EC2.

    c. Installare il pacchetto desktop/workstation della GUI.

```
[ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
```

Per CentOS Stream 8 e Red Hat Enterprise Linux 8

Come installare il driver NVIDIA GRID sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.
2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

   ```
   [ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel
    kernel-devel-$(uname -r)
   ```

6. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

   ```
   [ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
   ```

   In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

   ```
   [ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
   ```

7. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

   ```
   [ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
   ```

8. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

   ```
   [ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
   ```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

9. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

12. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni NICE DCV.

    b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze basate su GPU Amazon EC2.

    c. Installare il pacchetto workstation della GUI.

```
[ec2-user ~]$ sudo dnf groupinstall -y workstation
```

Rocky Linux 8

Per installare il driver NVIDIA GRID sull'istanza Linux

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.
2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

   ```
   [ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel
    kernel-devel-$(uname -r)
   ```

6. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

   ```
   [ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
   ```

   In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

   ```
   [ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
   ```

7. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

   ```
   [ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
   ```

8. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

   ```
   [ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
   ```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

9. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

12. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni NICE DCV.

    b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze basate su GPU Amazon EC2.

Ubuntu e Debian

Come installare il driver NVIDIA GRID sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.
2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
$ sudo apt-get update -y
```

3. (Ubuntu) Aggiornare il pacchetto `linux-aws` per ricevere la versione più recente.

```
$ sudo apt-get upgrade -y linux-aws
```

(Debian) Aggiornare il pacchetto per ricevere la versione più recente.

```
$ sudo apt-get upgrade -y
```

4. Riavviare l'istanza per caricare la versione più recente del kernel.

```
$ sudo reboot
```

5. Riconnettersi all'istanza dopo averla riavviata.
6. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

7. Disattivare il driver open source `nouveau` per le schede grafiche NVIDIA.

   a. Aggiungere `nouveau` al file di blacklist `/etc/modprobe.d/blacklist.conf`. Copiare il seguente blocco di codice e incollarlo in un terminale.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Modificare il file `/etc/default/grub` e aggiungere la seguente riga:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Ricompilare il file di configurazione di Grub.

```
$ sudo update-grub
```

8. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

   ```
   $ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
   ```

   In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

   ```
   $ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
   ```

9. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

   ```
   $ chmod +x NVIDIA-Linux-x86_64*.run
   ```

10. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

    ```
    $ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
    ```

    Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

11. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

    ```
    $ nvidia-smi -q | head
    ```

12. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

    ```
    $ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    $ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
    modprobe.d/nvidia.conf
    ```

13. Riavviare l'istanza.

```
$ sudo reboot
```

14. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni NICE DCV.

    b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze basate su GPU Amazon EC2.

    c. Installare il pacchetto desktop/workstation della GUI.

    ```
    $ sudo apt-get install -y lightdm ubuntu-desktop
    ```

Sistemi operativi Windows

Per installare il driver NVIDIA GRID sull'istanza di Windows

1. Connect all'istanza di Windows e apri una PowerShell finestra.
2. Configura le credenziali predefinite per l' AWS Tools for Windows PowerShell istanza di Windows. Per ulteriori informazioni, consulta Nozioni di base su AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Tools for Windows PowerShell .

   > **Important**
   >
   > Il tuo utente o ruolo deve disporre delle autorizzazioni concesse che contengono la politica ReadOnlyAccessAmazonS3. Per ulteriori informazioni, consulta la policy AWS gestita: AmazonS3 ReadOnlyAccess nella Guida per l'utente di Amazon Simple Storage Service.

3. Scarica i driver e il contratto di licenza per l'utente finale di NVIDIA GRID Cloud da Amazon S3 sul desktop utilizzando i PowerShell seguenti comandi.

   ```
   $Bucket = "ec2-windows-nvidia-drivers"
   $KeyPrefix = "latest"
   $LocalPath = "$home\Desktop\NVIDIA"
   ```

```
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

In questo bucket, vengono archiviate più versioni di un driver NVIDIA GRID. È possibile scaricare tutte le versioni di Windows disponibili nel bucket rimuovendo l'opzione `-KeyPrefix $KeyPrefix`. Per informazioni sulla versione del driver NVIDIA GRID per il sistema operativo in uso, consulta NVIDIA® Virtual GPU (vGPU) Software Documentation sul sito Web di NVIDIA.

A partire da GRID versione 11.0 puoi utilizzare i driver in `latest` per le istanze G3 e G4dn. Non verranno aggiunte versioni successive alla 11.0 a `g4/latest`, ma la versione 11.0 e le versioni precedenti specifiche di G4dn continueranno a stare in `g4/latest`.

Le istanze G5 richiedono GRID 13.1 o successivo (o GRID 12.4 o successivo).

4. Accedere al desktop e fare doppio clic sul file di installazione per avviarlo (scegliere la versione del driver che corrisponde alla versione SO dell'istanza in uso). Seguire le istruzioni per installare il driver e riavviare l'istanza come necessario. Per verificare che la GPU funzioni correttamente, controllare in Gestione dispositivi.
5. (Opzionale) Utilizzare il seguente comando per disabilitare la pagina di licenza nel pannello di controllo per evitare che gli utenti modifichino accidentalmente il tipo di prodotto (NVIDIA GRID Virtual Workstation è abilitata per impostazione predefinita). Per ulteriori informazioni, consulta il documento GRID Licensing User Guide.

   PowerShell

   Esegui i seguenti PowerShell comandi per creare il valore di registro per disabilitare la pagina delle licenze nel pannello di controllo. L' AWS Tools for PowerShell impostazione predefinita delle AMI di AWS Windows è la versione a 32 bit e questo comando ha esito negativo. Utilizza invece la versione a 64 bit PowerShell inclusa nel sistema operativo.

   ```
   New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing
   New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -
   Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
   ```

Prompt dei comandi

Esegui il seguente comando di registro per creare il valore di registro al fine di disabilitare la pagina delle licenze nel pannello di controllo. È possibile eseguirlo utilizzando la finestra del prompt dei comandi o una versione a 64 bit diPowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v
 NvCplDisableManageLicensePage /t REG_DWORD /d 1
```

6. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

   a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni NICE DCV.

   b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze basate su GPU Amazon EC2.

Opzione 4: driver di gioco NVIDIA (istanze G4dn e G5)

Questi driver sono disponibili solo per AWS i clienti. Scaricandoli, l'utente accetta di utilizzare il software scaricato solo per sviluppare AMI da utilizzare con l'hardware NVIDIA A10G e NVIDIA Tesla T4. Installando il software, sarai vincolato dai termini del contratto di licenza con l'utente finale NVIDIA GRID Cloud End User License Agreement.

Considerazioni

- Le istanze G3 richiedono AWS la risoluzione DNS fornita per il funzionamento delle licenze GRID.
- IMDSv2 è supportato solo con il driver NVIDIA versione 495.x o superiore.

Prerequisito

Prima di installare i driver di gioco NVIDIA, verifica di averli AWS CLI installati sull'istanza e di aver configurato le credenziali predefinite. Per ulteriori informazioni, consulta Installazione dell' AWS CLI nella Guida per l'utente dell'AWS Command Line Interface .

> **Important**
>
> L'utente o il ruolo devono disporre delle autorizzazioni concesse che contengono la politica di AmazonS3. ReadOnlyAccess Per ulteriori informazioni, consulta la policy AWS gestita: AmazonS3 ReadOnlyAccess nella Guida per l'utente di Amazon Simple Storage Service.

Amazon Linux e Amazon Linux 2

Come installare il driver di gioco NVIDIA sull'istanza

1. Connessione a un'istanza Linux.
2. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo yum install gcc make
```

3. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

4. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

5. Riconnettersi all'istanza dopo averla riavviata.
6. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

7. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

9. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

10. Eseguire il programma di installazione utilizzando l'URL seguente:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Se si utilizza Amazon Linux 2 con kernel versione 5.10, utilizzare il comando seguente per installare i driver di gioco NVIDIA.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

11. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Utilizza il comando seguente per scaricare e rinominare il file certificato.
    - Per la versione 460.39 o successiva:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Per le versioni da 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Per le versioni precedenti:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

14. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

15. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni NICE DCV.

CentOS 7 e Red Hat Enterprise Linux 7

Come installare il driver di gioco NVIDIA sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.
2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.

5. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. Disattivare il driver open source `nouveau` per le schede grafiche NVIDIA.

   a. Aggiungere `nouveau` al file di blacklist `/etc/modprobe.d/blacklist.conf`. Copiare il seguente blocco di codice e incollarlo in un terminale.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Modificare il file `/etc/default/grub` e aggiungere la seguente riga:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Ricompilare il file di configurazione di Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

10. Eseguire il programma di installazione utilizzando l'URL seguente:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

11. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Utilizza il comando seguente per scaricare e rinominare il file certificato.
    - Per la versione 460.39 o successiva:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Per le versioni da 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Per le versioni precedenti:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

14. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

15. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni NICE DCV. Se non è necessaria questa funzionalità, non completare questa fase.

Per CentOS Stream 8 e Red Hat Enterprise Linux 8

Come installare il driver di gioco NVIDIA sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.
2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Eseguire il programma di installazione utilizzando l'URL seguente:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

   Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

10. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilizza il comando seguente per scaricare e rinominare il file certificato.

    - Per la versione 460.39 o successiva:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Per le versioni da 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Per le versioni precedenti:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

14. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni NICE DCV.

Rocky Linux 8

Come installare il driver di gioco NVIDIA sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.
2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
[ec2-user ~]$ sudo dnf install -y unzip gcc make elfutils-libelf-devel libglvnd-
devel kernel-devel-$(uname -r)
```

6. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Eseguire il programma di installazione utilizzando l'URL seguente:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

   Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

10. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilizza il comando seguente per scaricare e rinominare il file certificato.

    - Per la versione 460.39 o successiva:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Per le versioni da 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Per le versioni precedenti:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

14. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni NICE DCV.

Ubuntu e Debian

Come installare il driver di gioco NVIDIA sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.
2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
$ sudo apt-get update -y
```

3. Aggiornare il pacchetto `linux-aws` per ricevere la versione più recente.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Riavviare l'istanza per caricare la versione più recente del kernel.

```
$ sudo reboot
```

5. Riconnettersi all'istanza dopo averla riavviata.
6. Installare il compilatore gcc e il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
$ sudo apt-get install -y unzip gcc make linux-headers-$(uname -r)
```

7. Disattivare il driver open source `nouveau` per le schede grafiche NVIDIA.

   a. Aggiungere `nouveau` al file di blacklist `/etc/modprobe.d/blacklist.conf`. Copiare il seguente blocco di codice e incollarlo in un terminale.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

b. Modificare il file `/etc/default/grub` e aggiungere la seguente riga:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Ricompilare il file di configurazione di Grub.

```
$ sudo update-grub
```

8. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

11. Eseguire il programma di installazione utilizzando l'URL seguente:

```
$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

12. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Utilizza il comando seguente per scaricare e rinominare il file certificato.

    - Per la versione 460.39 o successiva:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Per le versioni da 440.68 a 445.48:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Per le versioni precedenti:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consultare la documentazione di NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

15. Riavviare l'istanza.

```
$ sudo reboot
```

16. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni NICE DCV. Se non è necessaria questa funzionalità, non completare questa fase.

Sistemi operativi Windows

Prima di installare un driver di gioco NVIDIA sulla tua istanza, devi assicurarti che siano soddisfatti i seguenti prerequisiti oltre alle considerazioni menzionate per tutti i driver di gioco.

- Se si avvia l'istanza di Windows utilizzando un'AMI Windows personalizzata, l'AMI deve essere un'immagine standardizzata creata con Windows Sysprep per garantire il funzionamento del driver di gioco. Per ulteriori informazioni, consulta Creare un'AMI con Windows Sysprep.
- Configura le credenziali predefinite per l'istanza AWS Tools for Windows PowerShell Windows. Per ulteriori informazioni, consulta Nozioni di base su AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Tools for Windows PowerShell .

Per installare il driver di gioco NVIDIA sull'istanza di Windows

1. Connect all'istanza di Windows e apri una PowerShell finestra.
2. Scarica e installa il driver di gioco utilizzando i seguenti PowerShell comandi.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

In questo bucket S3 vengono archiviate più versioni di un driver NVIDIA GRID. Per scaricare tutte le versioni disponibili nel bucket, modifica il valore della variabile `$KeyPrefix` da "windows/più recente" a "windows".

3. Accedere al desktop e fare doppio clic sul file di installazione per avviarlo (scegliere la versione del driver che corrisponde alla versione SO dell'istanza in uso). Seguire le istruzioni per installare il driver e riavviare l'istanza come necessario. Per verificare che la GPU funzioni correttamente, controlla in Gestione dispositivi.
4. Per registrare il driver, utilizza uno dei seguenti metodi.

   Version 527.27 or above

   Crea la seguente chiave di registro con la versione a 64 bit di PowerShell o la finestra del prompt dei comandi.

   chiave: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global`

   nome: vGamingMarketplace

   tipo: DWord

   valore: 2

   PowerShell

   Esegui il PowerShell comando seguente per creare questo valore di registro. L' AWS Tools for PowerShell impostazione predefinita delle AMI di AWS Windows è la versione a 32 bit e questo comando ha esito negativo. Utilizza invece la versione a 64 bit PowerShell inclusa nel sistema operativo.

   ```
   New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
    -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
   ```

   Prompt dei comandi

   Esegui il seguente comando di registro per creare questo valore di registro. È possibile eseguirlo utilizzando la finestra del prompt dei comandi o una versione a 64 bit di PowerShell.

   ```
   reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
    vGamingMarketplace /t REG_DWORD /d 2
   ```

Earlier versions

Crea la seguente chiave di registro con la versione a 64 bit di o PowerShell la finestra del prompt dei comandi.

chiave: `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global`

nome: vGamingMarketplace

tipo: DWord

valore: 2

PowerShell

Esegui il PowerShell comando seguente per creare questo valore di registro. L' AWS Tools for PowerShell impostazione predefinita delle AMI di AWS Windows è la versione a 32 bit e questo comando ha esito negativo. Utilizza invece la versione a 64 bit PowerShell inclusa nel sistema operativo.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name
 "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Prompt dei comandi

Esegui il seguente comando di registro per creare questa chiave di registro con la finestra del prompt dei comandi. È possibile utilizzare questo comando anche nella versione a 64 bit diPowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t
 REG_DWORD /d 2
```

5. Esegui il comando seguente in PowerShell. In tal modo, viene scaricato il file del certificato, viene rinominato il file `GridSwCert.txt` e viene spostato il file nella cartella Documenti pubblici dell'unità di sistema. In genere, il percorso della cartella è `C:\Users\Public\Documents`.
   - Per la versione 461.40 o successiva:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCertWindows_2023_9_22.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

- Per la versione 445.87:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

- Per le versioni precedenti:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

> **Note**
>
> Se ricevi un errore durante il download del file e utilizzi Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo PowerShell terminale. Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il seguente comando e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

6. Riavviare l'istanza.
7. Verificare la licenza NVIDIA Gaming utilizzando il seguente comando:

```
C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\nvidia-smi.exe -q
```

L'output visualizzato dovrebbe essere simile al seguente.

```
vGPU Software Licensed Product
Product Name              : NVIDIA Cloud Gaming
License Status            : Licensed (Expiry: N/A)
```

8. (Facoltativo) Per utilizzare i quattro display con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni NICE DCV. Se non è necessaria questa funzionalità, non completare questa fase.

Installare una versione aggiuntiva di CUDA

Dopo aver installato un driver grafico NVIDIA nell'istanza, è possibile installare una versione di CUDA diversa da quella fornita con il driver grafico. Nella procedura seguente viene illustrato come configurare più versioni di CUDA nell'istanza.

Installa il toolkit CUDA su Linux

Segui questi passaggi per installare il toolkit CUDA su Linux:

1. Connessione a un'istanza Linux.
2. Aprire il sito Web NVIDIA e selezionare la versione di CUDA necessaria.
3. Selezionare l'architettura, la distribuzione e la versione per il sistema operativo nell'istanza. Per Installer Type (Tipo di installazione), selezionare runfile (local).
4. Seguire le istruzioni per scaricare lo script di installazione.
5. Aggiungere le autorizzazioni di esecuzione allo script di installazione scaricato utilizzando il comando seguente.

```
[ec2-user ~]$ chmod +x downloaded_installer_file
```

6. Eseguire lo script di installazione come segue per installare il toolkit CUDA e aggiungere il numero di versione CUDA al percorso del toolkit.

```
[ec2-user ~]$ sudo sh downloaded_installer_file --silent --override --toolkit --
samples --toolkitpath=/usr/local/cuda-version --samplespath=/usr/local/cuda --no-
opengl-libs
```

7. (Facoltativo) Impostare la versione CUDA predefinita nel modo seguente.

```
[ec2-user ~]$ sudo ln -s /usr/local/cuda-version /usr/local/cuda
```

Installa il toolkit CUDA su Windows

Segui questi passaggi per installare il toolkit CUDA su Windows:

Per installare il toolkit CUDA

1. Connettersi all'istanza Windows.
2. Aprire il sito Web NVIDIA e selezionare la versione di CUDA necessaria.
3. Per Installer Type (Tipo di installazione), selezionare exe (local) quindi scegliere Download (Scarica).
4. Utilizzando il browser, eseguire il file di installazione scaricato. Seguire le istruzioni per installare il toolkit CUDA. Potrebbe essere necessario riavviare l'istanza.

Installa i driver AMD sulla tua istanza Amazon EC2

Un'istanza con una GPU AMD collegata, ad esempio un'istanza G4ad, deve avere installato il driver AMD appropriato. A seconda delle esigenze, è possibile utilizzare una AMI con il driver preinstallato o scaricare un driver da Amazon S3.

Per installare i driver NVIDIA su un'istanza con una GPU NVIDIA collegata, ad esempio un'istanza G4dn, consulta Installare i driver NVIDIA.

Indice

Driver AMD Radeon Pro Software for Enterprise

Il driver AMD Radeon Pro Software for Enterprise è progettato per fornire supporto nei casi d'uso di grafica a livello professionale. Utilizzando il driver, è possibile configurare le istanze con due display 4K per GPU.

API supportate

- OpenGL, OpenCL
- Vulkan
- AMD Advanced Media Framework
- API di accelerazione video

- DirectX 9 e versioni successive
- Microsoft Media Foundation Transform hardware

AMI con driver AMD installato

AWS offre diverse Amazon Machine Images (AMI) fornite con i driver AMD installati. Apri leofferte nel Marketplace con driver AMD.

Download del driver AMD

Se non si utilizza una AMI con driver AMD installato, è possibile scaricare il driver AMD e installarlo sull'istanza. Solo le seguenti versioni del sistema operativo supportano i driver AMD:

- Amazon Linux 2 con versione del kernel 4.14

> **Note**
>
> La versione del driver AMD amdgpu-pro-20.20-1184451 e le versioni più recenti richiedono la versione del kernel 5.15 o superiore.

- Windows Server 2016
- Windows Server 2019

Questi download sono disponibili solo per AWS i clienti. Eseguendo il download, accetti di utilizzare il software scaricato solo per sviluppare AMIs da utilizzare con l'hardware AMD Radeon Pro V520. Installando il software, sarai vincolato dai termini del contratto di licenza con l'utente finale AMD Software End User License Agreement.

Installa il driver AMD sulla tua istanza Linux

1. Connessione a un'istanza Linux.
2. Installalo AWS CLI sulla tua istanza Linux e configura le credenziali predefinite. Per ulteriori informazioni, consulta Installazione dell' AWS CLI nella Guida per l'utente dell'AWS Command Line Interface .

> **Important**
>
> Il tuo utente o ruolo deve disporre delle autorizzazioni concesse che contengono la politica ReadOnlyAccessAmazonS3. Per ulteriori informazioni, consulta la policy AWS gestita: AmazonS3 ReadOnlyAccess nella Guida per l'utente di Amazon Simple Storage Service.

3. Installare gcc e make, se non sono già installati.

```
$ sudo yum install gcc make
```

4. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

   - Per Amazon Linux 2:

```
$ sudo amazon-linux-extras install epel -y
$ sudo yum update -y
```

   - Per Ubuntu 22.04:

```
$ wget https://repo.radeon.com/.preview/a0e4ef1dffbc95b4abb54e891f265e61/amdgpu-install/5.5.02.05.2/ubuntu/jammy/amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo apt install ./amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo sed -i 's#repo.radeon.com#&/.preview/a0e4ef1dffbc95b4abb54e891f265e61#' /etc/apt/sources.list.d/{amdgpu.list,rocm.list,amdgpu-proprietary.list}
```

   - Per altre versioni di Ubuntu:

```
$ sudo dpkg --add-architecture i386
$ sudo apt-get update -y && sudo apt upgrade -y
```

   - Per CentOS:

```
$ sudo yum install epel-release -y
$ sudo yum update -y
```

5. Riavviare l'istanza.

```
$ sudo reboot
```

6. Riconnettersi all'istanza dopo il riavvio.
7. Scaricare il driver AMD più recente.

> **Note**
>
> Salta questo passaggio per Ubuntu 22.04.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

8. Estrarre il file.
   - Per Amazon Linux 2 e CentOS:

     ```
     $ tar -xf amdgpu-pro-*rhel*.tar.xz
     ```

   - Per Ubuntu:

     > **Note**
     >
     > Salta questo passaggio per Ubuntu 22.04.

     ```
     $ tar -xf amdgpu-pro*ubuntu*.xz
     ```

9. Passare alla cartella del driver estratto.
10. Aggiungi i moduli mancanti per l'installazione del driver.
    - Per Amazon Linux 2 e CentOS:

      Salta questo passaggio.

    - Per Ubuntu:

      > **Note**
      >
      > Salta questo passaggio per Ubuntu 22.04.

```
$ sudo apt install linux-modules-extra-$(uname -r) -y
```

11. Eseguire lo script di installazione automatica per installare lo stack grafico completo.

    - Per Ubuntu 22.04:

      ```
      $ sudo amdgpu-install --usecase=workstation --vulkan=pro --opencl=rocr,legacy -y
      ```

    - Per Amazon Linux 2 e CentOS e altre versioni di Ubuntu:

      ```
      $ ./amdgpu-pro-install -y --opencl=pal,legacy
      ```

12. Riavviare l'istanza.

    ```
    $ sudo reboot
    ```

13. Verificare che il driver funzioni.

    ```
    $ dmesg | grep amdgpu
    ```

    La risposta dovrebbe essere simile alla seguente:

    ```
    Initialized amdgpu
    ```

Installa il driver AMD sulla tua istanza di Windows

1. Connect all'istanza di Windows e apri una PowerShell finestra.
2. Configura le credenziali predefinite per l' AWS Tools for Windows PowerShell istanza di Windows. Per ulteriori informazioni, consulta Nozioni di base su AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Tools for Windows PowerShell .

   > **Important**
   >
   > Il tuo utente o ruolo deve disporre delle autorizzazioni concesse che contengono la politica ReadOnlyAccessAmazonS3. Per ulteriori informazioni, consulta la policy AWS

gestita: AmazonS3 ReadOnlyAccess nella Guida per l'utente di Amazon Simple Storage Service.

3. Scarica i driver da Amazon S3 sul desktop utilizzando i seguenti PowerShell comandi.

```
$Bucket = "ec2-amd-windows-drivers"
$KeyPrefix = "latest" # use "archives" for Windows Server 2016
$LocalPath = "$home\Desktop\AMD"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

4. Decomprimi il file del driver scaricato ed esegui il programma di installazione utilizzando i seguenti comandi. PowerShell

```
Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose
```

Ora, controlla il nome della nuova directory. Il nome della directory può essere recuperato utilizzando il comando. `Get-ChildItem` PowerShell

```
Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"
```

L'output visualizzato dovrebbe essere simile al seguente:

```
Directory: C:\Users\Administrator\Desktop\AMD\latest

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       10/13/2021  12:52 AM                210414a-365562C-Retail_End_User.2
```

Installa i driver AMD:

```
pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs
```

5. Seguire le istruzioni per installare il driver e riavviare l'istanza come necessario.
6. Per verificare che la GPU funzioni correttamente, controllare in Gestione dispositivi. "AMD Radeon Pro V520 MxGPU" dovrebbe elencata come scheda video.
7. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni NICE DCV.

Configura un desktop interattivo per Linux

Dopo aver verificato che sull'istanza Linux sia installato il driver AMD GPU e che amdgpu sia in uso, puoi installare un desktop manager interattivo. Si consiglia l'ambiente desktop MATE per la massima garanzia in termini di compatibilità e prestazioni.

Prerequisito

Aprire un editor di testo e salvare quanto segue come file denominato `xorg.conf`. Questo file sarà necessario sull'istanza.

```
Section "ServerLayout"
Identifier     "Layout0"
Screen          0 "Screen0"
InputDevice     "Keyboard0" "CoreKeyboard"
InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath "/opt/amdgpu/lib/xorg/modules"
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Mouse0"
Driver         "mouse"
Option         "Protocol" "auto"
Option         "Device" "/dev/psaux"
Option         "Emulate3Buttons" "no"
```

```
Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Keyboard0"
Driver         "kbd"
EndSection
Section "Monitor"
Identifier     "Monitor0"
VendorName     "Unknown"
ModelName      "Unknown"
EndSection
Section "Device"
Identifier     "Device0"
Driver         "amdgpu"
VendorName     "AMD"
BoardName      "Radeon MxGPU V520"
BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
Option         "DPMS" "Disable"
EndSection
Section "Screen"
Identifier     "Screen0"
Device         "Device0"
Monitor        "Monitor0"
DefaultDepth   24
Option         "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual    3840 2160
    Depth      32
EndSubSection
EndSection
```

Per configurare un desktop interattivo su Amazon Linux 2

1. Installare l'archivio EPEL.

   ```
   $ C:\> sudo amazon-linux-extras install epel -y
   ```

2. Installare il desktop MATE.

   ```
   $ C:\> sudo amazon-linux-extras install mate-desktop1.x -y
   ```

```
$ C:\> sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copiare il file `xorg.conf` su `/etc/X11/xorg.conf`.
4. Riavviare l'istanza.

```
$ C:\> sudo reboot
```

5. (Facoltativo) Installare il server NICE DCV per utilizzare NICE DCV come protocollo di visualizzazione ad alte prestazioni, quindi connettersi a una sessione NICE DCV utilizzando il client preferito.

Per configurare un desktop interattivo su Ubuntu

1. Installare il desktop MATE.

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y
$ C:\> sudo apt purge ifupdown -y
```

2. Copiare il file `xorg.conf` su `/etc/X11/xorg.conf`.
3. Riavviare l'istanza.

```
$ sudo reboot
```

4. Installare il codificatore AMF per la versione appropriata di Ubuntu.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Facoltativo) Installare il server NICE DCV per utilizzare NICE DCV come protocollo di visualizzazione ad alte prestazioni, quindi connettersi a una sessione NICE DCV utilizzando il client preferito.
6. Dopo l'installazione di DCV assegnare le autorizzazioni video per l'utente DCV:

```
$ sudo usermod -aG video dcv
```

Per configurare un desktop interattivo in CentOS

1. Installare l'archivio EPEL.

```
$ sudo yum update -y
$ C:\> sudo yum install epel-release -y
```

2. Installare il desktop MATE.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copiare il file `xorg.conf` su `/etc/X11/xorg.conf`.
4. Riavviare l'istanza.

```
$ sudo reboot
```

5. (Facoltativo) Installare il server NICE DCV per utilizzare NICE DCV come protocollo di visualizzazione ad alte prestazioni, quindi connettersi a una sessione NICE DCV utilizzando il client preferito.

Driver paravirtuali per le istanze Windows

Le AMI Windows contengono un insieme di driver per consentire l'accesso all'hardware virtualizzato. Tali driver vengono utilizzati da Amazon EC2 per mappare instance store e volumi Amazon EBS ai rispettivi dispositivi. Nella tabella seguente vengono illustrate le differenze principali tra i diversi driver.

	RedHat PV	Citrix PV	AWS PV
Tipo di istanza	Non supportato per tutti i tipi di istanza. Se specifichi un tipo di istanza non supportato, l'istanza sarà danneggiata.	Supportato per i tipi di istanza Xen.	Supportato per i tipi di istanza Xen.
Volumi collegati	Supporta fino a 16 volumi collegati.	Supporta più di 16 volumi collegati.	Supporta più di 16 volumi collegati.
Rete	Il driver presenta problemi noti durante i quali la connessione di rete si ristabilisce con carichi		Il driver configura automatic

	RedHat PV	Citrix PV	AWS PV
	elevati, ad esempio in caso di trasferimenti di file FTP rapidi.		amente i frame jumbo sulla scheda di rete quando si trova su un tipo di istanza compatibile. Quando l'istanza si trova in un gruppo di posizionamento del cluster, ciò offre migliori prestazioni di rete tra le istanze che fanno parte del gruppo di posizionamento del cluster. Per ulteriori informazioni, consulta Gruppi di collocamento.

La tabella seguente riporta i driver PV da eseguire su ciascuna versione di Windows Server su Amazon EC2.

Versione di Windows Server	Versione driver PV
Windows Server 2022	AWS Ultima versione PV
Windows Server 2019	AWS Ultima versione PV
Windows Server 2016	AWS Ultima versione PV
Windows Server 2012 R2	AWS Ultima versione PV
Windows Server 2012	AWS Ultima versione PV
Windows Server 2008 R2	AWS PV versione 8.3.5
Windows Server 2008	Citrix PV 5.9
Windows Server 2003	Citrix PV 5.9

Indice

AWS Driver fotovoltaici

I driver AWS PV sono memorizzati nella `%ProgramFiles%\Amazon\Xentools` directory. Questa directory contiene anche simboli pubblici e uno strumento da riga di comando che consente di accedere alle voci in XenStore. `xenstore_client.exe` Ad esempio, il PowerShell comando seguente restituisce l'ora corrente dall'Hypervisor:

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
 AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

I componenti del driver AWS PV sono elencati nel registro di Windows sotto. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` Tali componenti sono i seguenti: xenbus, xeniface, xennet, xenvbd e xenvif.

AWS I driver PV dispongono inoltre di un servizio Windows denominato LiteAgent, che viene eseguito in modalità utente. Gestisce attività come gli eventi di spegnimento e riavvio delle AWS API sulle istanze di generazione Xen. Puoi accedere ai servizi e gestirli eseguendo `Services.msc` dalla riga di comando. Quando viene eseguito su istanze di generazione Nitro, i driver AWS PV non vengono utilizzati e il LiteAgent servizio si interromperà automaticamente a partire dalla versione 8.2.4 del driver. L'aggiornamento al driver AWS PV più recente aggiorna anche LiteAgent e migliora l'affidabilità su tutte le generazioni di istanze.

Installa i driver AWS PV più recenti

Le AMI Windows di Amazon contengono un insieme di driver per consentire l'accesso all'hardware virtualizzato. Tali driver vengono utilizzati da Amazon EC2 per mappare instance store e volumi Amazon EBS ai rispettivi dispositivi. Ti consigliamo di installare i driver più recenti per migliorare la stabilità e le prestazioni delle istanze Windows di EC2.

Opzioni di installazione

- È possibile utilizzare AWS Systems Manager per aggiornare automaticamente i driver PV. Per ulteriori informazioni, consulta Spiegazione passo per passo: aggiornare automaticamente i driver PV sulle istanze EC2 di Windows (console) nella Guida per l'utente di AWS Systems Manager .
- È possibile scaricare il pacchetto di driver ed eseguire il programma di installazione manualmente. Assicurarsi di controllare il file `readme.txt` per i requisiti di sistema. Per informazioni sul download e sull'installazione di driver AWS PV, o sull'aggiornamento di un controller di dominio, consulta Aggiornamento manuale delle istanze di Windows Server (aggiornamento PV)AWS.

AWS cronologia dei pacchetti di driver PV

La tabella seguente mostra le modifiche ai driver AWS PV per ogni versione del driver.

Versione del pacchetto	Dettagli	Data di rilascio
8.4.3	Sono stati corretti i bug nel programma di installazione del pacchetto per migliorare l'esperienza di aggiornamento.	24 gennaio 2023

Versione del pacchetto	Dettagli	Data di rilascio
8.4.2	Correzioni di stabilità per affrontare le race condition.	13 aprile 2022
8.4.1	Installer di pacchetti migliorato.	7 gennaio 2022
8.4.0	• Correzioni di stabilità per risolvere rari casi di I/O del disco bloccato. • Correzioni di stabilità per risolvere rari casi di arresto anomalo durante lo scollegamento del volume EBS. • Aggiunta funzionalità per distribuire il carico su più core per carichi di lavoro che sfruttano più di 20.000 IOPS e subiscono una riduzione delle prestazioni dovuta a colli di bottiglia. Per abilitare questa funzionalità, consulta I carichi di lavoro che utilizzano più di 20.000 IOPS su disco subiscono una riduzione delle prestazioni dovuta ai colli di bottiglia della CPU. • AWS L'installazione di PV 8.4 su Windows Server 2008 R2 avrà esito negativo. AWS La versione PV 8.3.5 e precedenti sono supportate su Windows Server 2008 R2.	2 marzo 2021
8.3.5	Installer di pacchetti migliorato.	7 gennaio 2022
8.3.4	Maggiore affidabilità del collegamento del dispositivo di rete.	4 agosto 2020

Versione del pacchetto	Dettagli	Data di rilascio
8.3.3	• Aggiorna il componente XenStore -facing per impedire il controllo dei bug durante i percorsi di gestione degli errori. • Aggiornamento al componente di archiviazione per evitare arresti anomali quando viene inviato un SRB non valido. Per aggiornare questo driver nelle istanze di Windows Server 2008 R2, è necessario innanzitutto verificare che siano installate le patch appropriate per risolvere il seguente avviso di sicurezza Microsoft: Security Advisory 3033929.	4 febbraio 2020
8.3.2	Maggiore affidabilità dei componenti di rete.	30 luglio 2019
8.3.1	Miglioramenti delle prestazioni e della solidità ai componenti di archiviazione.	12 giugno 2019
8.2.7	Maggiore efficienza per supportare la migrazione ai tipi di istanza di generazione più recente.	20 maggio 2019
8.2.6	Maggiore efficienza di un percorso di chiusura inaspettata.	15 gennaio 2019
8.2.5	Altri miglioramenti di sicurezza PowerShell il programma di installazione è ora disponibile nel pacchetto.	12 dicembre 2018
8.2.4	Migliorie in termini di affidabilità.	2 ottobre 2018
8.2.3	Correzioni di bug e miglioramenti delle prestazioni. Segnalare un ID di volume EBS come numero di serie per i volumi EBS. Questo abilita gli scenari cluster come S2D.	29 maggio 2018

Versione del pacchetto	Dettagli	Data di rilascio
8.2.1	Miglioramenti delle prestazioni di rete e di archiviazione oltre a varie correzioni della solidità. Per verificare che la versione sia stata installata, fai riferimento al seguente valore di registro di Windows: `HKLM\Software\Amazon\PVDriver\Version 8.2.1` .	8 marzo 2018
7.4.6	Correzioni di stabilità per rendere i driver AWS fotovoltaici più resistenti.	26 aprile 2017
7.4.3	Aggiunta di supporto per Windows Server 2016. Correzioni della stabilità per tutte le versioni del sistema operativo Windows supportate. * La firma del driver AWS PV versione 7.4.3 scade il 29 marzo 2019. Si consiglia l'aggiornamento al driver PV più recente AWS .	18 novembre 2016
7.4.2	Correzioni della stabilità per il supporto del tipo di istanza X1.	2 agosto 2016
7.4.1	• Miglioramento delle prestazioni del AWS driver PV Storage. • Correzioni di stabilità nel driver AWS PV Storage: risolto un problema a causa del quale le istanze registravano un arresto anomalo del sistema con il codice di controllo dei bug 0x0000Dead. • Correzioni di stabilità nel driver PV Network. AWS • Aggiunta di supporto per Windows Server 2008R2.	12 luglio 2016
7.3.2	• Miglioramento di registrazione e diagnostica. • Correzione della stabilità nel driver AWS PV Storage. In alcuni casi i dischi potrebbero non comparire in Windows dopo aver ricollegato il disco all'istanza. • Aggiunta di supporto per Windows Server 2012.	24 giugno 2015

Versione del pacchetto	Dettagli	Data di rilascio
7.3.1	Aggiornamento TRIM: correzione associata a richieste TRIM. Tale correzione stabilizza le istanze e ne migliora le prestazioni in caso di gestione di una grande quantità di richieste TRIM.	
7.3.0	Supporto TRIM: il driver AWS PV ora invia le richieste TRIM all'hypervisor. I dischi temporanei elaborano correttamente le richieste TRIM dal momento che l'archiviazione sottostante supporta TRIM (SSD). L'archiviazione basata su EBS non supporta TRIM dal marzo 2015.	
7.2.5	• Correzione della stabilità nei driver AWS PV Storage: in alcuni casi il driver AWS PV poteva dereferenziare la memoria non valida e causare un errore di sistema. • Correzione della stabilità durante la generazione di un crash dump: in alcuni casi il pilota AWS fotovoltaico potrebbe rimanere bloccato in condizioni di gara mentre scriveva un crash dump. Prima di questa versione, il problema poteva essere risolto esclusivamente forzando l'arresto del driver e riavviandolo al fine di perdere il dump della memoria.	
7.2.4	Persistenza dell'ID del dispositivo: questa correzione del driver maschera l'ID del dispositivo PCI della piattaforma e obbliga il sistema a mostrare sempre lo stesso ID del dispositivo, anche quando l'istanza viene spostata. Più generalmente, la correzione influisce sul modo in cui l'hypervisor mostra i dispositivi virtuali. La correzione include anche modifiche al programma di installazione congiunta dei driver AWS PV in modo che il sistema mantenga i dispositivi virtuali mappati.	

Versione del pacchetto	Dettagli	Data di rilascio
7.2.2	• Carica i driver AWS PV in modalità Directory Services Restore Mode (DSRM): Directory Services Restore Mode è un'opzione di avvio in modalità sicura per i controller di dominio Windows Server. • Persistenza dell'ID del dispositivo quando la scheda di rete virtuale viene ricollegata: la correzione forza il sistema a controllare la mappatura dell'indirizzo MAC e mantenere l'ID del dispositivo. Questa correzione assicura che le schede mantengano le loro impostazioni statiche se ricollegate.	
7.2.1	• Esecuzione in modalità sicura: risoluzione di un problema che impediva il caricamento del driver in modalità sicura. In precedenza, i driver AWS PV venivano istanziati solo nei normali sistemi in esecuzione. • Aggiunta di dischi ai pool di archiviazione di Microsoft Windows: in precedenza sintetizzavamo le richieste di pagina 83. Questa correzione ha disabilitato il supporto di pagina 83. Ciò non interessa i pool di archiviazione utilizzati in un ambiente di cluster perché i dischi PV non sono dischi di cluster validi.	
7.2.0	Base: la versione base AWS PV.	

Driver Citrix PV

I driver Citrix PV sono archiviati nella directory `%ProgramFiles%\Citrix\XenTools` (istanze a 32 bit) o `%ProgramFiles(x86)%\Citrix\XenTools` (istanze a 64 bit).

I componenti del driver Citrix PV sono elencati nel registro di Windows in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services`. Tali componenti sono i seguenti: xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd e xenvif.

Citrix dispone anche di un componente driver denominato XenGuestAgent, che funziona come un servizio Windows. Gestisce attività come l'arresto e il riavvio di eventi dell'API. Puoi accedere ai servizi e gestirli eseguendo `Services.msc` dalla riga di comando.

Se riscontri errori di rete durante l'esecuzione di determinati carichi di lavoro, potresti aver bisogno di disabilitare la caratteristica di offload TCP per il driver Citrix PV. Per ulteriori informazioni, consulta Offload TCP.

RedHat Driver fotovoltaici

RedHat i driver sono supportati per le istanze legacy, ma non sono consigliati sulle istanze più recenti con più di 12 GB di RAM a causa delle limitazioni dei driver. Le istanze con più di 12 GB di RAM che eseguono RedHat driver possono non avviarsi e diventare inaccessibili. Si consiglia di aggiornare RedHat i driver ai driver Citrix PV e quindi di aggiornare i driver Citrix PV ai driver PV. AWS

I file di origine dei RedHat driver si trovano nella directory (istanze a 32 bit) o `%ProgramFiles%\RedHat` (istanze a 64 bit). `%ProgramFiles(x86)%\RedHat` I due driver sono `rhelnet` il driver di rete RedHat paravirtualizzato e il driver miniport SCSI. `rhelscsi` RedHat

Sottoscrizione alle notifiche di

Amazon SNS può avvisarti in caso di pubblicazione di nuove versioni dei driver Windows di EC2. Utilizza uno dei metodi seguenti per effettuare la sottoscrizione a queste notifiche.

> **Note**
>
> Devi specificare la Regione per l'argomento SNS che sottoscrivi.

Sottoscrizione alle notifiche EC2 dalla console

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario selezionare questa regione perché le notifiche SNS per le quali stai effettuando la sottoscrizione si trovano in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Create subscription (Crea sottoscrizione) segui questi passaggi:

a. In Topic ARN (ARN argomento) copia il seguente nome della risorsa Amazon (ARN):

   arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

b. In Protocol (Protocollo), scegli `Email`.

c. In Endpoint digita l'indirizzo e-mail utilizzabile per ricevere le notifiche.

d. Scegli Create Subscription (Crea sottoscrizione).

6. Riceverai a breve un'e-mail di conferma. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

Iscriviti alle notifiche EC2 utilizzando il AWS CLI

Per iscriverti alle notifiche EC2 con AWS CLI, usa il seguente comando.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-
windows-drivers --region us-east-1 --protocol email --notification-
endpoint YourUserName@YourDomainName.ext
```

Iscriviti alle notifiche EC2 utilizzando il AWS Tools for PowerShell

Per iscriverti alle notifiche EC2 con Tools for Windows PowerShell, usa il seguente comando.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Region us-east-1 -Protocol email -Endpoint 'YourUserName@YourDomainName.ext'
```

Quando i nuovi driver Windows di EC2 vengono rilasciati, inviamo notifiche ai sottoscrittori. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Annullamento della sottoscrizione alle notifiche del driver Windows per Amazon EC2

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
3. Selezionare la casella di spunta della sottoscrizione, quindi scegliere Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni). Quando viene richiesta la conferma, seleziona Elimina.

Aggiornamento dei driver PV sulle istanze Windows

Ti consigliamo di installare i driver PV più recenti per migliorare la stabilità e le prestazioni delle istanze Windows di EC2. Le istruzioni riportate in questa pagina consentono di scaricare il pacchetto di driver ed eseguire il programma di installazione.

Per verificare quale driver viene utilizzato dall'istanza Windows

Aprire Connessioni di rete nel Pannello di controllo e visualizzare Connessione alla rete locale. Verifica che il driver sia uno dei seguenti:

- AWS Dispositivo di rete PV
- Scheda Ethernet Citrix PV
- RedHat Driver NIC PV

In alternativa, puoi controllare l'output dal comando `pnputil -e`.

Requisiti di sistema

Assicurarsi di controllare il file `readme.txt` nel download per i requisiti di sistema.

Indice

Aggiorna le istanze di Windows Server (aggiornamento AWS PV) con Distributor

È possibile utilizzare Distributor, una funzionalità di AWS Systems Manager, per installare o aggiornare il AWS pacchetto driver PV. L'installazione o l'aggiornamento possono essere eseguiti una sola volta oppure è possibile installarli o aggiornarli in base a una pianificazione. L'`In-place update`opzione Tipo di installazione non è supportata per questo pacchetto Distributor.

> **Important**
>
> Se l'istanza è un controller di dominio, consulta Aggiornare un controller di dominio (aggiornamento PV)AWS. Il processo di aggiornamento per le istanze dei controller del dominio è diverso rispetto alle edizioni standard di Windows.

1. Ti consigliamo di creare un backup nel caso in cui sia necessario ripristinare le modifiche.

   > **Tip**
   >
   > Invece di creare l'AMI dalla console Amazon EC2, puoi utilizzare Systems Manager Automation per creare l'AMI utilizzando il `AWS-CreateImage` runbook. Per ulteriori informazioni, consulta AWS-CreateImagela Guida per l'utente di riferimento del runbook di AWS Systems Manager automazione.

   a. Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Prima di arrestare un'istanza, verificare di aver copiato tutti i dati necessari dai volumi di instance store nello storage persistente, ad esempio Amazon EBS o Amazon S3.
   b. Nel riquadro di navigazione, scegliere Instances (Istanze).
   c. Selezionare l'istanza che richiede l'aggiornamento del driver e scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).
   d. Dopo avere interrotto l'istanza, selezionare l'istanza, scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).
   e. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).
2. Collegati all'istanza tramite un'applicazione desktop remoto. Per ulteriori informazioni, consulta the section called “Connect alla tua istanza Windows utilizzando un client RDP”.
3. Prima di eseguire questo aggiornamento, consigliamo di portare offline tutti i dischi non di sistema e di annotare le mappature delle lettere di unità ai dischi secondari in Disk Management (Gestione disco). Questo passaggio non è necessario se si esegue un aggiornamento in loco dei driver AWS PV. Consigliamo inoltre di impostare i servizi non essenziale sull'avvio Manual (Manuale) nella console Services.
4. Per le istruzioni su come installare o aggiornare il pacchetto driver AWS PV utilizzando Distributor, consultate le procedure in Installazione o aggiornamento dei pacchetti nella Guida per l'utente.AWS Systems Manager

5. Per Nome, scegli. AWSPVDriver
6. Per Tipo di installazione, seleziona Disinstalla e reinstalla.
7. Se necessario, configurate gli altri parametri per il pacchetto ed eseguite l'installazione o l'aggiornamento utilizzando la procedura riportata in. Step 4

   Dopo aver eseguito il pacchetto Distributor, l'istanza si riavvia automaticamente e quindi aggiorna il driver. L'istanza non sarà disponibile per un massimo di 15 minuti.
8. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli di integrità nella console Amazon EC2, verifica che il nuovo driver sia stato installato connettendoti all'istanza tramite Remote Desktop.
9. Una volta effettuata la connessione, esegui il seguente PowerShell comando:

   ```
   Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
   ```
10. Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS cronologia dei pacchetti di driver PV Open Disk Management per esaminare tutti i volumi secondari offline e metterli online corrispondenti alle lettere di unità indicate inStep 3.

Se in precedenza avete disabilitato Offload TCP l'uso di Netsh per i driver Citrix PV, vi consigliamo di riattivare questa funzione dopo l'aggiornamento ai driver PV. AWS I problemi di TCP Offloading con i driver Citrix non sono presenti nei driver PV. AWS Di conseguenza, TCP Offloading offre prestazioni migliori con i driver PV. AWS

Se in precedenza avete applicato un indirizzo IP statico o una configurazione DNS all'interfaccia di rete, potrebbe essere necessario riapplicare l'indirizzo IP statico o la configurazione DNS dopo l'aggiornamento dei driver PV. AWS

Aggiornamento manuale delle istanze di Windows Server (aggiornamento PV)AWS

Utilizzate la seguente procedura per eseguire un aggiornamento sul posto dei driver AWS PV o per eseguire l'aggiornamento dai driver Citrix PV ai driver AWS PV su Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 o Windows Server 2022. Questo aggiornamento non è disponibile per RedHat i driver o per altre versioni di Windows Server.

Alcune versioni meno recenti di Windows Server non possono utilizzare i driver più recenti. Per verificare la versione del driver utilizzare per il sistema operativo, consulta la tabella delle versioni del driver nella pagina Driver paravirtuali per le istanze Windows.

> **Important**
>
> Se l'istanza è un controller di dominio, consulta Aggiornare un controller di dominio (aggiornamento PV)AWS. Il processo di aggiornamento per le istanze dei controller del dominio è diverso rispetto alle edizioni standard di Windows.

Per aggiornare i driver AWS PV manualmente

1. Ti consigliamo di creare un backup nel caso in cui sia necessario ripristinare le modifiche.

   > **Tip**
   >
   > Invece di creare l'AMI dalla console Amazon EC2, puoi utilizzare Systems Manager Automation per creare l'AMI utilizzando il `AWS-CreateImage` runbook. Per ulteriori informazioni, consulta AWS-CreateImagela Guida per l'utente di riferimento del runbook di AWS Systems Manager automazione.

   a. Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Prima di arrestare un'istanza, verificare di aver copiato tutti i dati necessari dai volumi di instance store nello storage persistente, ad esempio Amazon EBS o Amazon S3.

   b. Nel riquadro di navigazione, scegliere Instances (Istanze).

   c. Selezionare l'istanza che richiede l'aggiornamento del driver e scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).

   d. Dopo avere interrotto l'istanza, selezionare l'istanza, scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).

   e. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).

2. Collegati all'istanza tramite un'applicazione desktop remoto.

3. Prima di eseguire questo aggiornamento, consigliamo di portare offline tutti i dischi non di sistema e di annotare le mappature delle lettere di unità ai dischi secondari in Disk Management (Gestione disco). Questo passaggio non è necessario se si esegue un aggiornamento in loco

dei driver AWS PV. Consigliamo inoltre di impostare i servizi non essenziale sull'avvio Manual (Manuale) nella console Services.

4. Scarica il pacchetto di driver più recente per l'istanza.

   In alternativa, esegui il comando seguente: PowerShell

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/
   Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
   Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath
    $env:userprofile\pv_drivers
   ```

   > **Note**
   >
   > Se ricevi un errore durante il download del file e utilizzi Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo PowerShell terminale. Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il seguente comando e riprovare:
   >
   > ```
   > [Net.ServicePointManager]::SecurityProtocol =
   >  [Net.SecurityProtocolType]::Tls12
   > ```

5. Estrarre i contenuti della cartella ed eseguire `AWSPVDriverSetup.msi`.

Dopo aver eseguito l'MSI, l'istanza si riavvia automaticamente e quindi aggiorna il driver. L'istanza non sarà disponibile per un massimo di 15 minuti. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli di integrità nella console Amazon EC2, puoi verificare che il nuovo driver sia stato installato connettendoti all'istanza tramite Remote Desktop ed eseguendo il seguente PowerShell comando:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS cronologia dei pacchetti di driver PV Open Disk Management per esaminare tutti i volumi secondari offline e metterli online corrispondenti alle lettere di unità indicate inStep 3.

Se in precedenza avete disabilitato Offload TCP l'uso di Netsh per i driver Citrix PV, vi consigliamo di riattivare questa funzione dopo l'aggiornamento ai driver PV. AWS I problemi di TCP Offloading con i

driver Citrix non sono presenti nei driver PV. AWS Di conseguenza, TCP Offloading offre prestazioni migliori con i driver PV. AWS

Se in precedenza avete applicato un indirizzo IP statico o una configurazione DNS all'interfaccia di rete, potrebbe essere necessario riapplicare l'indirizzo IP statico o la configurazione DNS dopo l'aggiornamento dei driver PV. AWS

Aggiornare un controller di dominio (aggiornamento PV)AWS

Utilizzare la procedura seguente su un controller di dominio per eseguire un aggiornamento sul posto dei driver AWS PV o per eseguire l'aggiornamento dai driver Citrix PV ai driver PV. AWS

Per aggiornare un controller di dominio

1. Si consiglia di creare un backup del controller di dominio nel caso in cui sia necessario eseguire il rollback delle modifiche. L'utilizzo di un'AMI come backup non è supportato. Per ulteriori informazioni, consulta Considerazioni operative su backup e ripristino dei controller di dominio virtualizzati nella documentazione di Microsoft.
2. Esegui il comando seguente per configurare Windows per l'avvio in Directory Services Restore Mode (DSRM).

   > **Warning**
   >
   > Prima di eseguire questo comando, confermare di conoscere la password DSRM. Tale informazione è richiesta per accedere all'istanza quando l'aggiornamento è completo e l'istanza si riavvia automaticamente.

   ```
   bcdedit /set {default} safeboot dsrepair
   ```

   PowerShell:

   ```
   PS C:\> bcdedit /set "{default}" safeboot dsrepair
   ```

   Il sistema deve essere avviato in DSRM perché l'utilità di aggiornamento rimuove i driver di archiviazione Citrix PV in modo da poter installare i driver PV. AWS Pertanto, consigliamo di annotare le mappature delle lettere di unità e delle cartelle ai dischi secondari in Disk Management (Gestione disco). Quando i driver di archiviazione Citrix PV non sono presenti, le

unità secondarie non vengono rilevate. I controller di dominio che utilizzano una cartella NTDS su unità secondarie non si avviano perché il disco secondario non sarà rilevato.

> **Warning**
>
> Una volta eseguito il comando, non riavviare manualmente il sistema. Il sistema risulterà irraggiungibile perché i driver Citrix PV non supportano DSRM.

3. Eseguire il seguente comando per aggiungere **`DisableDCCheck`** al registro:

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t
 REG_SZ /d true
```

4. Scarica il pacchetto di driver più recente per l'istanza.
5. Estrarre i contenuti della cartella ed eseguire `AWSPVDriverSetup.msi`.

   Dopo aver eseguito l'MSI, l'istanza si riavvia automaticamente e quindi aggiorna il driver. L'istanza non sarà disponibile per un massimo di 15 minuti.
6. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli dello stato nella console Amazon EC2, connettersi all'istanza utilizzando Desktop remoto. Apri Disk Management (Gestione disco) per esaminare i volumi secondari offline e portarli online in base alle mappature delle lettere di unità e delle cartelle annotate in precedenza.

   È necessario connettersi all'istanza specificando il nome utente nel seguente formato hostname\administrator. Ad esempio, Win2k12\ administrator. TestBox
7. Eseguire il comando riportato di seguito per rimuovere la configurazione di avvio DSRM:

```
bcdedit /deletevalue safeboot
```

8. Riavviare l'istanza.
9. Per completare il processo di aggiornamento, verificare che il nuovo driver sia istallato. In Gestione dispositivi, in Storage Controllers (Controller di archiviazione), individuare PV Storage Host Adapter (Adattatore host archiviazione PV)AWS Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS cronologia dei pacchetti di driver PV.
10. Eseguire il seguente comando per eliminare **`DisableDCCheck`** dal registro:

```
reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
```

> **Note**
>
> Se in precedenza avete disabilitato Offload TCP l'utilizzo di Netsh per i driver Citrix PV, vi consigliamo di riattivare questa funzione dopo l'aggiornamento a PV Drivers. AWS I problemi di TCP Offloading con i driver Citrix non sono presenti nei driver PV. AWS Di conseguenza, TCP Offloading offre prestazioni migliori con i driver PV. AWS

Aggiornamento delle istanze Windows Server 2008 e 2008 R2 (aggiornamento da Redhat a Citrix PV)

Prima di iniziare ad aggiornare i RedHat driver ai driver Citrix PV, assicuratevi di fare quanto segue:

- Installare la versione più recente del servizio EC2Config. Per ulteriori informazioni, consulta Installazione della versione più recente di EC2Config.
- Verificate di avere installato Windows 3.0. PowerShell Per verificare la versione installata, esegui il seguente comando in una PowerShell finestra:

  ```
  PS C:\> $PSVersionTable.PSVersion
  ```

  Windows PowerShell 3.0 è incluso nel pacchetto di installazione di Windows Management Framework (WMF) versione 3.0. Se è necessario installare Windows PowerShell 3.0, vedere Windows Management Framework 3.0 nell'Area download Microsoft.
- Esegui il backup delle informazioni importanti dell'istanza o crea un'AMI dall'istanza. Per ulteriori informazioni sulla creazione di un'AMI, consulta Crea un'AMI supportata da Amazon EBS.

  > **Tip**
  >
  > Invece di creare l'AMI dalla console Amazon EC2, puoi utilizzare Systems Manager Automation per creare l'AMI utilizzando il `AWS-CreateImage` runbook. Per ulteriori informazioni, consulta AWS-CreateImagela Guida per l'utente di riferimento del runbook di AWS Systems Manager automazione.

Se crei un'AMI, assicurati di completare quanto segue:

- Prendi nota della tua password.
- Non eseguire lo strumento Sysprep o utilizzare il servizio EC2Config.
- Imposta la scheda Ethernet in modo da ottenere automaticamente un indirizzo IP utilizzando DHCP. Per ulteriori informazioni, vedere Configurare le impostazioni TCP/IP nella libreria Microsoft. TechNet

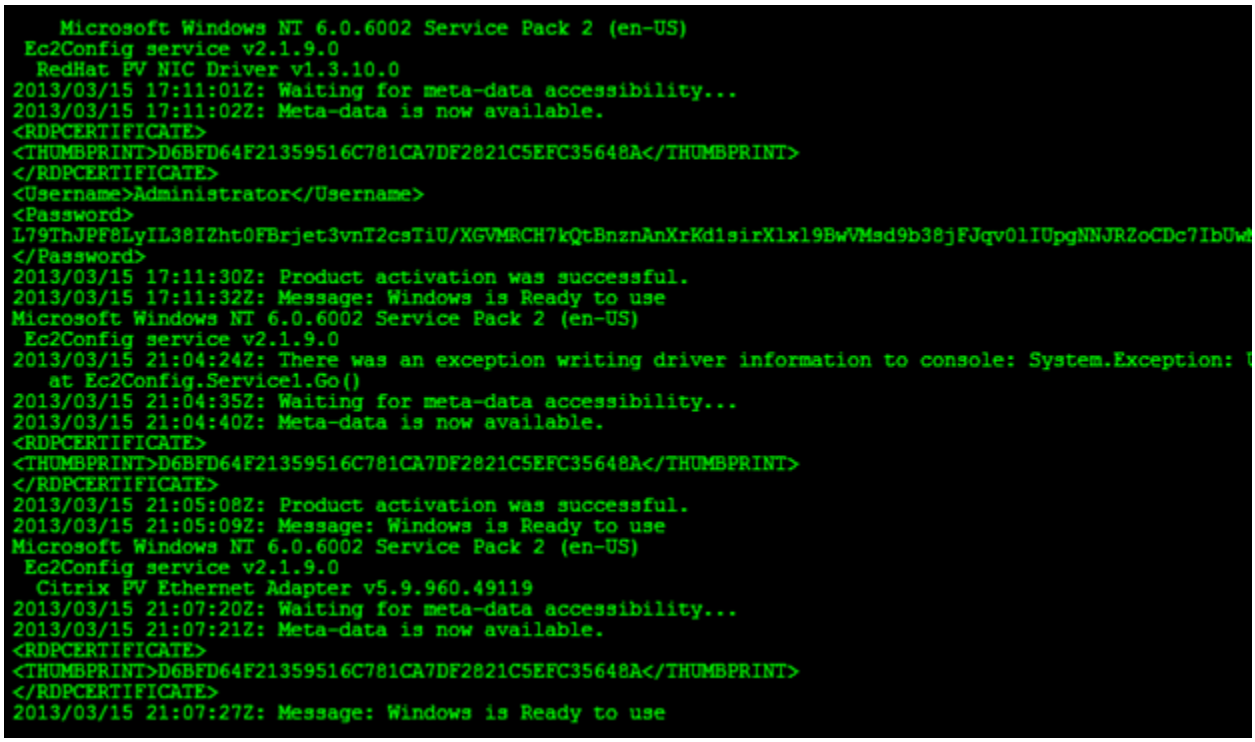
Per aggiornare i driver RedHat

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale. Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti all'istanza Windows .
2. Nell'istanza, scaricare il pacchetto di aggiornamento Citrix PV.
3. Estrarre il contenuto del pacchetto di aggiornamento in una ubicazione a scelta.
4. Fare doppio clic sul file Upgrade.bat. In caso di avviso di sicurezza, scegliere Run (Esegui).
5. Nella finestra di dialogo Upgrade Drivers (Aggiorna driver), rivedere le informazioni e scegliere Yes (Sì) se si è pronti ad avviare l'aggiornamento.
6. Nella finestra di dialogo del programma di disinstallazione di Red Hat Paravirtualized Xen Drivers for Windows, scegliete Sì per rimuovere il software. RedHat L'istanza sarà riavviata.

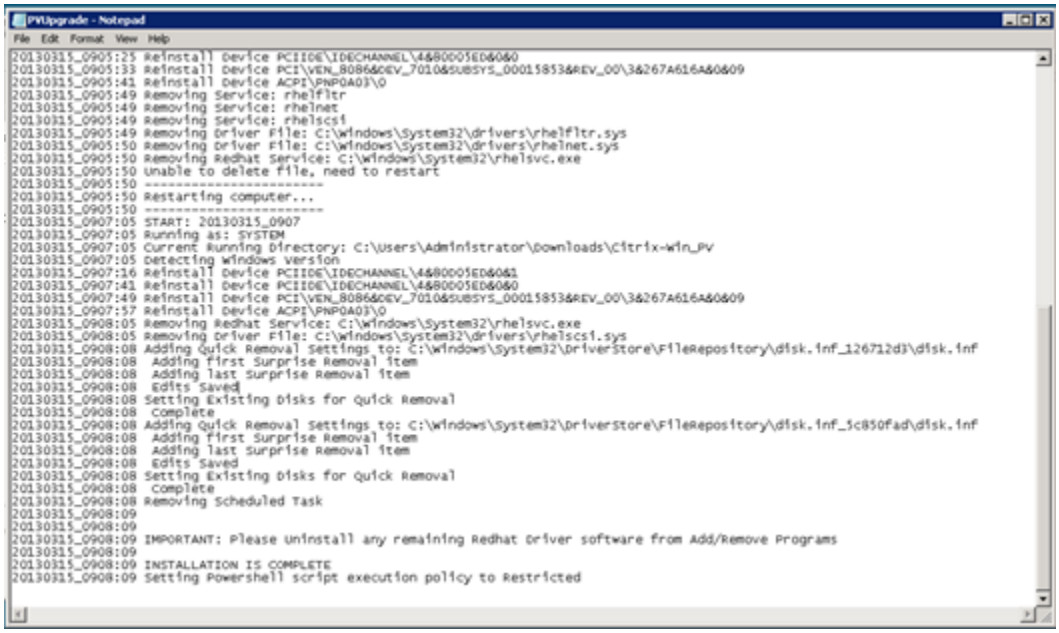
> **Note**
>
> Se non si visualizza la finestra di dialogo del programma di disinstallazione, scegliere Red Hat Paravirtualize nella barra delle applicazioni di Windows.

7. Controllare che l'istanza si sia riavviata che sia pronta all'uso.
   a. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   b. Nella pagina Instances (Istanze) selezionare Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi scegliere Get system log (Ottieni registro di sistema).

c. Le operazioni di aggiornamento dovrebbero aver riavviato il server 3 o 4 volte. È possibile verificarlo nel file di log in base al numero di volte in cui viene visualizzato `Windows is Ready to use`.



8. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
9. Chiudere la finestra di dialogo Red Hat Paravirtualized Xen Drivers for Windows uninstaller (Driver Xen Red Hat paravirtualizzati per il programma di disinstallazione di Windows).
10. Confermare che l'installazione è completa. Andare alla cartella `Citrix-WIN_PV` estratta in precedenza, aprire il file `PVUpgrade.log` e cercare il testo `INSTALLATION IS COMPLETE`.



Aggiornamento del servizio di agente guest Citrix Xen

Se utilizzi driver PV Citrix Xen su Windows Server, puoi aggiornare il servizio d'agente guest Citrix Xen. Questo servizio di Windows gestisce attività come l'arresto e il riavvio di eventi dell'API. Puoi eseguire questo pacchetto di aggiornamento su qualsiasi versione di Windows Server, purché l'istanza esegua driver Citrix PV.

> **Important**
>
> Per Windows Server 2008 R2 e versioni successive, si consiglia di eseguire l'aggiornamento ai driver AWS PV che includono l'aggiornamento Guest Agent.

Prima di avviare l'aggiornamento dei driver, esegui il backup delle informazioni importanti dell'istanza oppure crea un'AMI per tale istanza. Per ulteriori informazioni sulla creazione di un'AMI, consulta Crea un'AMI supportata da Amazon EBS.

> **Tip**
>
> Invece di creare l'AMI dalla console Amazon EC2, puoi utilizzare Systems Manager Automation per creare l'AMI utilizzando il `AWS-CreateImage` runbook. Per ulteriori

informazioni, consulta AWS-CreateImagela Guida per l'utente di riferimento del runbook di AWS Systems Manager automazione.

Se crei un'AMI, assicurati di completare quanto segue:

- Non abilitare lo strumento Sysprep nel servizio EC2Config.
- Prendi nota della tua password.
- Imposta la scheda Ethernet su DHCP.

Per aggiornare il servizio d'agente guest Citrix Xen

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale. Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti all'istanza Windows .
2. Nell'istanza, scaricare il pacchetto di aggiornamento Citrix.
3. Estrarre il contenuto del pacchetto di aggiornamento in una ubicazione a scelta.
4. Fare doppio clic sul file Upgrade.bat. In caso di avviso di sicurezza, scegliere Run (Esegui).
5. Nella finestra di dialogo Upgrade Drivers (Aggiorna driver), rivedere le informazioni e scegliere Yes (Sì) se si è pronti ad avviare l'aggiornamento.
6. Quando l'aggiornamento è completo, si aprirà il file `PVUpgrade.log` con il testo `UPGRADE IS COMPLETE`.
7. Riavviare l'istanza.

Risolvi i problemi relativi ai driver PV nelle istanze di Windows

Le seguenti solo soluzioni a problemi che si potrebbero verificare con vecchie immagini Amazon EC2 e driver PV.

Indice

Windows Server 2012 R2 perde la connettività di rete e archiviazione dopo un riavvio dell'istanza

> **Important**
>
> Questo problema si verifica solo con AMI disponibili prima del settembre 2014.

Le Amazon Machine Image (AMI) per Windows Server 2012 R2 rese disponibili prima del 10 settembre 2014 possono perdere connettività di rete e archiviazione dopo un riavvio dell'istanza. L'errore nel registro di AWS Management Console sistema indica: «Difficoltà a rilevare i dettagli del driver PV per Console Output». La perdita di connettività è causata dalla funzione di pulizia Plug and Play. Questa caratteristica ricerca e disabilita i dispositivi inattivi del sistema ogni 30 giorni. La funzione identifica erroneamente il dispositivo di rete EC2 come inattivo e lo rimuove dal sistema. Quando ciò accade, l'istanza perde la connettività di rete dopo un riavvio.

Per i sistemi ritenuti potenzialmente soggetti a tale problema, puoi scaricare ed eseguire un aggiornamento in sede del driver. Se non riesci a completare tale aggiornamento, puoi eseguire uno script helper. Questo stabilisce se l'istanza è interessata. Se lo è, e se il dispositivo di rete Amazon EC2 non è stato rimosso, lo script disabilita la scansione di pulizia Plug and Play. Se il dispositivo di rete è stato rimosso, lo script ripara il dispositivo, disabilita la scansione di pulizia Plug and Play e abilita il riavvio dell'istanza con la connessione di rete abilitata.

Indice

Scegliere come risolvere i problemi

Sono disponibili due metodi per ripristinare la connettività di rete e archiviazione di un'istanza interessata dal problema. Seleziona uno dei seguenti metodi:

Metodo	Prerequisiti	Panoramica della procedura
Metodo 1 – Connettività di rete migliorata	La connettività di rete migliorata è disponibile solo in un cloud	Cambia il tipo di istanza del server in istanza C3. La

Metodo	Prerequisiti	Panoramica della procedura
	privato virtuale (VPC) che richiede un tipo di istanza C3. Se il server non utilizza al momento il tipo di istanza C3, è necessario cambiarlo temporaneamente.	connettività di rete migliorata ti permette quindi di connetter ti all'istanza interessata e di correggere il problema. Dopo aver risolto il problema, modifica l'istanza riportand ola al tipo originale. Questo metodo è in genere più rapido del Metodo 2 e meno soggetto a errori da parte dell'uten te. Saranno applicati costi aggiuntivi finché l'istanza C3 resta in esecuzione.
Metodo 2 – Configurazione del registro	Capacità di creare o accedere a un secondo server. Capacità di modificare le impostazioni del registro.	Distacca il volume root dall'ista nza interessata, collegalo a un'istanza differente, connettit i e apporta le modifiche nel registro. Saranno applicati costi aggiuntivi finché il server aggiuntivo resta in esecuzion e. Questo metodo è più lento del Metodo 1, ma si è dimostrato efficace in situazion i in cui il Metodo 1 non ha consentito la risoluzione del problema.

Metodo 1 – Connettività di rete migliorata

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Individua l'istanza interessata. Selezionare l'istanza e scegliere Instance state (Stato istanza), quindi Stop (Arresta).

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

4. Dopo l'arresto dell'istanza, creare un backup. Selezionare l'istanza e scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).
5. Cambiare il tipo di istanza con qualsiasi tipo di istanza C3.
6. Avviare l'istanza.
7. Connect all'istanza utilizzando Remote Desktop, quindi scarica il pacchetto AWS PV Drivers Upgrade sull'istanza.
8. Estrai i contenuti della cartella ed esegui `AWSPVDriverSetup.msi`.

   Dopo aver eseguito l'MSI, l'istanza si riavvia automaticamente e quindi aggiorna i driver. L'istanza non sarà disponibile per un massimo di 15 minuti.
9. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli dello stato nella console Amazon EC2, connettersi all'istanza utilizzando Desktop remoto e verificare che i nuovi driver siano istallati. In Gestione dispositivi, in Controller di storage, individua AWS Scheda host storage PV. Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS cronologia dei pacchetti di driver PV.
10. Arrestare l'istanza e modificarla riportandola al suo tipo originale.
11. Avviare l'istanza e ripristinare un utilizzo normale.

Metodo 2 – Configurazione del registro

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Individua l'istanza interessata. Seleziona l'istanza e scegli Instance state (Stato istanza), quindi Stop instance (Arresta istanza).

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

4. Scegli Launch Instance (Avvia istanza) e crea un'istanza temporanea di Windows Server 2008 o Windows Server 2012 nella stessa zona di disponibilità dell'istanza interessata. Non creare un'istanza Windows Server 2012 R2.

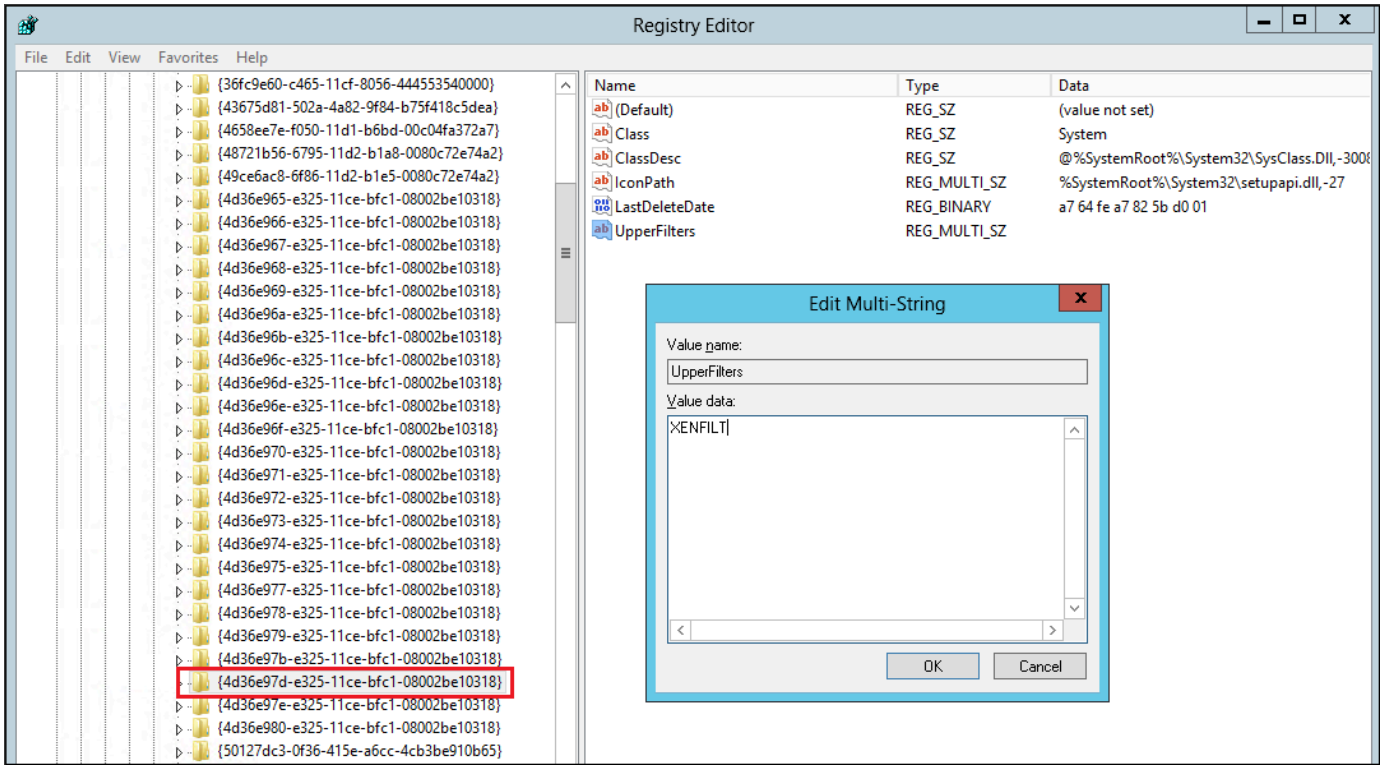
> **Important**
>
> Se non crei l'istanza nella stessa Zona di disponibilità dell'istanza interessata, non potrai collegare il volume root dell'istanza interessata sulla nuova istanza.

5. Nel riquadro di navigazione, selezionare Volumes (Volumi).
6. Individua il volume root dell'istanza interessata. Scollega il volume e collega il volume all'istanza temporanea creata in precedenza. Collegala con il nome del dispositivo predefinito (xvdf).
7. Utilizzare Desktop remoto per collegarsi all'istanza temporanea, quindi usare l'utilità Disk Management (Gestione disco) per rendere il volume disponibile per l'uso.
8. Nell'istanza temporanea, aprire la finestra di dialogo Run (Esegui), digitare **`regedit`** e premere Invio.
9. Nel riquadro di navigazione dell'editor del Registro, scegliere HKEY_Local_Machine, quindi dal menu File scegliere Load Hive (Carica Hive).
10. Nella finestra di dialogo Load Hive (Carica Hive), andare a Volume interessato\Windows \System32\config\System e digitare un nome temporaneo nella finestra di dialogo Key Name (Nome chiave). Ad esempio, specifica OldSys.
11. Nel riquadro di navigazione dell'editor del Registro, individuare le chiavi seguenti:

    HKEY_LOCAL_MACHINE\ ***`your_temporary_key_name\ 001\ Control\ Class\ 4d36e97d-e325-11ce-bfc1-08002be10318`*** ControlSet

    HKEY_LOCAL_MACHINE\ ***`nome_chiave_temporaneo\ ControlSet 001\ Control\ Class\ 4d36e96a-e325-11ce-bfc1-08002be10318`***

12. Per ogni chiave, fate doppio clic, immettete un valore di UpperFiltersXENFILT, quindi scegliete OK.



13. Individuare la chiave seguente:

    HKEY_LOCAL_MACHINE\ your_temporary_key_name\ 001\ Services\ XENBUS\ Parameters ControlSet

14. Crea una nuova stringa (REG_SZ) con il nome e il seguente valore: ActiveDevice

    PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Individuare la chiave seguente:

    HKEY_LOCAL_MACHINE\ your_temporary_key_name\ 001\ Services\ XENBUS ControlSet

16. Cambiare il valore Count (Conteggio) da 0 a 1.

17. Individuare ed eliminare le chiavi seguenti:

    HKEY_LOCAL_MACHINE\ ***nome_chiave_temporanea***\ ControlSet 001\ Services\ xenvbd\ StartOverride

    HKEY_LOCAL_MACHINE\ ***nome_chiave_temporaneo***\ ControlSet 001\ Services\ xenfilt\ StartOverride

18. Nel riquadro di navigazione dell'editor del Registro, scegliere la chiave temporanea creata contestualmente alla prima apertura dell'editor del Registro.

19. Dal menu File, scegliere Unload Hive (Scarica Hive).
20. Nell'utilità Disk Management (Gestione disco), scegliere l'unità collegata in precedenza, aprire il menu contestuale (pulsante destro del mouse) e scegliere Offline.
21. Nella console Amazon EC2, distaccare il volume interessato dall'istanza temporanea e ricollegarlo all'istanza Windows Server 2012 R2 con il nome dispositivo /dev/sda1. Devi specificare questo nome del dispositivo per indicare il volume come volume root.
22. Avviare l'istanza.
23. Connect all'istanza utilizzando Remote Desktop, quindi scarica il pacchetto AWS PV Drivers Upgrade sull'istanza.
24. Estrai i contenuti della cartella ed esegui `AWSPVDriverSetup.msi`.

    Dopo aver eseguito l'MSI, l'istanza si riavvia automaticamente e quindi aggiorna i driver. L'istanza non sarà disponibile per un massimo di 15 minuti.
25. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli dello stato nella console Amazon EC2, connettersi all'istanza utilizzando Desktop remoto e verificare che i nuovi driver siano istallati. In Gestione dispositivi, in Controller di storage, individua AWS Scheda host storage PV. Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS cronologia dei pacchetti di driver PV.
26. Cancella o interrompi l'istanza temporanea creata durante questa procedura.

Esecuzione dello script di correzione

Se non riesci a eseguire un aggiornamento in sede del driver o a migrare a un'istanza più recente, puoi eseguire lo script di correzione per risolvere i problemi causati dall'attività di pulizia Plug and Play.

Per eseguire lo script di correzione

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Scegliere l'istanza per la quale si intende eseguire lo script di correzione. Selezionare Instance state (Stato istanza), quindi Stop instance (Arresta istanza).

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

4. Dopo l'arresto dell'istanza, creare un backup. Selezionare l'istanza e scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).
5. Selezionare Instance state (Stato istanza), quindi Start instance (Avvia istanza).
6. Connettiti all'istanza utilizzando Remote Desktop, quindi scarica la RemediateDriverIssue cartella.zip sull'istanza.
7. Estrarre i contenuti della cartella.
8. Eseguire lo script di correzione in base alle istruzioni nel file Readme.txt. Il file si trova nella cartella in cui è stato estratto RemediateDriverIssue il file.zip.

Offload TCP

> **Important**
>
> Questo problema non si applica alle istanze che eseguono driver di rete AWS PV o Intel.

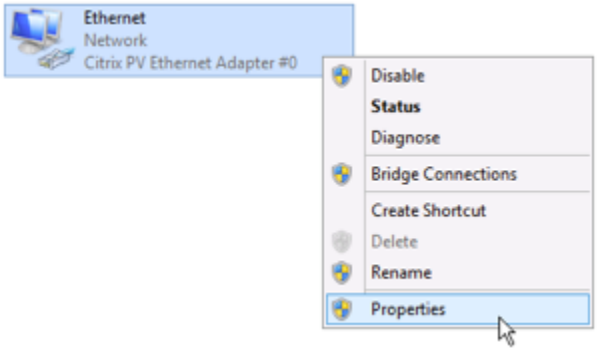
Per impostazione predefinita, l'offload TCP viene abilitato per i driver Citrix PV nelle AMI Windows. Se riscontri errori a livello di trasporto o anomalie nella trasmissione dei pacchetti (come indicato su Windows Performance Monitor), ad esempio quando stai eseguendo determinati carichi di lavoro SQL, potrebbe essere necessario disabilitare questa caratteristica.

> **Warning**
>
> La disabilitazione dell'offload TCP potrebbe ridurre le prestazioni di rete dell'istanza.

Per disabilitare l'offload TCP per Windows Server 2012 e 2008

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.

2. Se si utilizza Windows Server 2012, premere Ctrl+Esc per accedere alla schermata Start (Avvia), quindi scegliere Control Panel (Pannello di controllo). Se si utilizza Windows Server 2008, scegliere Start (Avvia) e selezionare Control Panel (Pannello di controllo).
3. Scegliere Network and Internet (Rete e Internet), quindi Network and Sharing Center (Centro connessioni di rete e condivisione).
4. Scegliere Change adapter settings (Modifica le impostazioni della scheda).
5. Fai clic con il pulsante destro del mouse su Citrix PV Ethernet Adapter #0 (Scheda Ethernet Citrix PV #0) e selezionare Properties (Proprietà).



6. Nella finestra di dialogo Local Area Connection Properties (Proprietà connessione alla rete locale), scegliere Configure (Configura) per aprire la finestra di dialogo Citrix PV Ethernet Adapter #0 Properties (Proprietà scheda Ethernet Citrix PV #0).
7. Nella scheda Advanced (Avanzato), disabilitare tutte le proprietà ad eccezione di Correct TCP/UDP Checksum Value (Correggi il valore checksum TCP/UDP). Per disabilitare una proprietà, selezionarla da Property (Proprietà) e scegliere Disabled (Disattivato) in Value (Valore).
8. Seleziona OK.
9. Nella finestra del prompt dei comandi, eseguire i comandi seguenti.

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Riavviare l'istanza.

Sincronizzazione oraria

Prima del rilascio del 13/02/2013 dell'AMI Windows, l'agente guest Citrix Xen poteva definire l'ora in modo errato. Ciò può determinare la scadenza della locazione DHCP. In caso di problemi di connessione all'istanza, potresti dover aggiornare l'agente.

Per stabilire se disponi dell'agente guest Citrix Xen aggiornato, controlla se il file `C:\Program Files\Citrix\XenGuestAgent.exe` è datato marzo 2013. Se la data è precedente, aggiorna il servizio d'agente guest Citrix Xen. Per ulteriori informazioni, consulta Aggiornamento del servizio di agente guest Citrix Xen.

I carichi di lavoro che utilizzano più di 20.000 IOPS su disco subiscono una riduzione delle prestazioni dovuta ai colli di bottiglia della CPU

È possibile che si verifichi questo problema se si utilizzano istanze di Windows che eseguono driver AWS PV che sfruttano più di 20.000 IOPS e si verifica un codice di controllo dei bug `0x9E: USER_MODE_HEALTH_MONITOR`.

Le operazioni di lettura e scrittura su disco (iOS) nei driver AWS PV avvengono in due fasi: preparazione dell'IO e completamento dell'IO. Per impostazione predefinita, la fase di preparazione viene eseguita su un singolo core arbitrario. La fase di completamento viene invece eseguita sul core `0`. La quantità di elaborazione necessaria per elaborare un IO varia in base alle dimensioni e ad altre proprietà. Alcuni IO esegue un'elaborazione maggiore nella fase di preparazione mentre altri nella fase di completamento. Quando un'istanza gestisce più di 20.000 IOPS, la fase di preparazione o di completamento può comportare un collo di bottiglia in cui la CPU su cui viene eseguita è al 100% di capacità. Il fatto che la fase di preparazione o di completamento diventi un collo di bottiglia dipende dalle proprietà degli IO utilizzati dall'applicazione.

A partire dai driver AWS PV 8.4.0, il carico della fase di preparazione e della fase di completamento può essere distribuito su più core, eliminando i colli di bottiglia. Ogni applicazione utilizza proprietà IO diverse. Pertanto, l'applicazione di una delle seguenti configurazioni potrebbe aumentare, ridurre o non influire affatto sulle prestazioni dell'applicazione. Dopo aver applicato una di queste configurazioni, monitorare l'applicazione per verificare di raggiungere le prestazioni desiderate.

1. Prerequisiti

   Prima di iniziare questa procedura di risoluzione dei problemi, verificare i seguenti prerequisiti:

   - L'istanza utilizza i driver AWS PV versione 8.4.0 o successiva. Per eseguire l'aggiornamento, consulta Aggiornamento dei driver PV sulle istanze Windows.

- Hai accesso RDP all'istanza. Per la procedura di connessione all'istanza Windows tramite RDP, consulta Connect alla tua istanza Windows utilizzando un client RDP.
- Disponi dell'accesso amministratore sull'istanza.

2. Osservazione del carico della CPU sull'istanza

   Puoi utilizzare Gestione attività di Windows per visualizzare il carico su ogni CPU in modo da determinare potenziali colli di bottiglia per l'IO del disco.

   1. Verifica che l'applicazione sia in esecuzione e gestisca il traffico come il carico di lavoro di produzione.
   2. Connettiti all'istanza tramite RDP.
   3. Seleziona il menu Avvia sull'istanza.
   4. Specifica `Task Manager` nel menu Avvia per aprire Gestione attività.
   5. Se Gestione attività visualizza la visualizzazione di riepilogo, seleziona Maggiori dettagli per espandere la vista dettagliata.
   6. Scegliere la scheda Performance (Prestazioni).
   7. Seleziona CPU nel riquadro sinistro.
   8. Fai clic con il pulsante destro del mouse sul grafico nel riquadro principale e seleziona Cambia il grafico in > Processori logici per visualizzare ogni singolo core.
   9. A seconda del numero di core presenti nella tua istanza, potresti vedere le righe che visualizzano il carico della CPU nel tempo oppure potresti semplicemente vedere un numero.
      - Se vedi grafici che mostrano il carico nel tempo, cerca le CPU in cui il riquadro è quasi completamente ombreggiato.
      - Se visualizzi un numero su ciascun core, cerca i core che riportano costantemente il 95% o un valore maggiore.
   10. Prendi nota se per il core `0` o un altro core si sta verificando un carico pesante.

3. Scelta della configurazione da applicare

Nome configurazione	Quando applicare questa configurazione	Note
Default configuration	Il carico di lavoro è inferiore a 20.000 IOPS o altre configurazioni non hanno	Per questa configurazione, l'IO si verifica su pochi core che possono beneficia

Nome configurazione	Quando applicare questa configurazione	Note
	migliorato le prestazioni o la stabilità.	re di carichi di lavoro più piccoli aumentando la localizzazione della cache e riducendo la commutazione di contesto.
Allow driver to choose whether to distribute completion	Il carico di lavoro sta conducendo oltre 20.000 IOPS e si osserva un carico moderato o elevato sul core `0` .	Questa configurazione è consigliata per tutte le istanze Xen che utilizzano PV 8.4.0 o versioni successive e che utilizzano più di 20.000 IOPS, indipendentemente dal fatto che si riscontrino o meno problemi.
Distribute both preparation and completion	Il carico di lavoro sta utilizzando oltre 20.000 IOPS e consente al driver di scegliere la distribuzione che non ha migliorato le prestazioni o per un core diverso da `0` si sta verificando un carico elevato.	Questa configurazione consente la distribuzione sia della fase di preparazione IO che della fase di completamento.

> **Note**
>
> Si consiglia di non distribuire la preparazione IO senza distribuire anche il completamento (impostazione `DpcRedirection` senza impostazione `NotifierDistributed`) perché la fase di completamento è sensibile al sovraccarico dovuto alla fase di preparazione quando la fase di preparazione è in esecuzione in parallelo.

Valori chiave del registro

- NotifierDistributed

  Valore `0` o non presente — La fase di completamento verrà eseguita sul core `0` .

  Valore `1` — Il driver sceglie di eseguire la fase di completamento sul core `0` o un core aggiuntivo per disco collegato.

  Valore `2` — Il driver esegue la fase di completamento su un core aggiuntivo per ogni disco collegato.

- DpcRedirection

  Valore `0` o non presente — La fase di preparazione verrà eseguita su un unico core arbitrario.

  Valore `1` — La fase di preparazione è distribuita su più core.

Configurazione di default

Applica la configurazione predefinita con le versioni dei driver AWS PV precedenti alla 8.4.0 o se si osserva un peggioramento delle prestazioni o della stabilità dopo l'applicazione di una delle altre configurazioni in questa sezione.

1. Connettiti all'istanza tramite RDP.
2. Aprire un nuovo prompt dei PowerShell comandi come amministratore.
3. Emettere i seguenti comandi per rimuovere le chiavi di registro `NotifierDistributed` e `DpcRedirection`.

   ```
   Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
   \Parameters -Name NotifierDistributed
   ```

   ```
   Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
   \Parameters -Name DpcRedirection
   ```

4. Riavviare l'istanza.

Consenti al driver di scegliere se distribuire il completamento

Impostare la chiave di registro `NotiferDistributed` in modo da consentire al driver di archiviazione PV di scegliere se distribuire o meno il completamento dell'IO.

1. Connettiti all'istanza tramite RDP.
2. Aprire un nuovo PowerShell prompt dei comandi come amministratore.
3. Emettere il seguente comando per impostare la chiave di registro `NotiferDistributed`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Riavviare l'istanza.

Distribuisci sia la preparazione che il completamento

Impostare le chiavi di registro `NotifierDistributed` e `DpcRedirection` per distribuire sempre sia la fase di preparazione che quella di completamento.

1. Connettiti all'istanza tramite RDP.
2. Aprire un nuovo PowerShell prompt dei comandi come amministratore.
3. Emettere i seguenti comandi per impostare le chiavi di registro `NotifierDistributed` e `DpcRedirection`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Riavviare l'istanza.

AWS Driver NVMe per istanze Windows

I volumi Amazon EBS e i volumi di instance store sono esposti come dispositivi a blocchi NVMe su istanze basate sul sistema Nitro. AWS Per utilizzare appieno le prestazioni e le funzionalità delle funzionalità di Amazon EBS per i volumi esposti come dispositivi a blocchi NVMe, sull'istanza deve essere installato il AWS driver NVMe. Tutte le AMI AWS Windows di ultima generazione sono dotate del driver NVMe installato per impostazione predefinita. AWS

Per ulteriori informazioni su EBS e NVMe, consulta Amazon EBS e NVMe nella Amazon EBS User Guide. Per ulteriori informazioni sulle instance store SSD e NVMe, consulta Volumi di instance store SSD.

Installa o aggiorna i driver NVMe utilizzando AWS PowerShell

Se non utilizzi le AMI AWS Windows più recenti fornite da Amazon, utilizza la seguente procedura per installare il driver AWS NVMe corrente. Devi eseguire questo aggiornamento quando è opportuno riavviare l'istanza. L'istanza verrà riavviata dallo script di installazione oppure devi riavviarla come fase finale.

Prerequisiti

PowerShell 3.0 o versione successiva

Per scaricare e installare il driver AWS NVMe più recente

1. Si consiglia di creare un'AMI come backup come segue, nel caso in cui sia necessario eseguire il rollback delle modifiche.
    a. Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Prima di arrestare un'istanza, verificare di aver copiato tutti i dati necessari dai volumi di instance store nello storage persistente, ad esempio Amazon EBS o Amazon S3.
    b. Nel riquadro di navigazione, scegliere Instances (Istanze).
    c. Selezionare l'istanza che richiede l'aggiornamento del driver e scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).
    d. Dopo avere interrotto l'istanza, selezionare l'istanza, scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).
    e. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).
2. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.

3. Scaricare ed estrarre i driver sull'istanza utilizzando una delle seguenti opzioni:
   - Utilizzo di un browser:
     a. Scarica il pacchetto di driver più recente per l'istanza.
     b. Estrai l'archivio .zip.
   - Usando: PowerShell

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/
Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
 $env:userprofile\nvme_driver
```

> **Note**
>
> Se ricevi un errore durante il download del file e utilizzi Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo PowerShell terminale. Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il seguente comando e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Installa il driver sulla tua istanza eseguendo lo `install.ps1` PowerShell script dalla `nvme_driver` directory (`.\install.ps1`). Se ricevi un errore, assicurati di utilizzare la PowerShell versione 3.0 o una versione successiva.

   a. (Facoltativo) A partire dalla versione AWS NVMe`1.5.0`, le prenotazioni persistenti di Small Computer System Interface (SCSI) sono supportate per Windows Server 2016 e versioni successive. Questa funzionalità aggiunge il supporto per Windows Server Failover Clustering con archiviazione Amazon EBS condivisa. Per impostazione predefinita, questa funzionalità non è abilitata durante l'installazione.

   È possibile abilitare la funzionalità durante l'esecuzione dello script `install.ps1` per installare il driver specificando il parametro `EnableSCSIPersistentReservations` con un valore di `$true`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
```

È possibile disabilitare la funzionalità durante l'esecuzione dello script `install.ps1` per installare il driver specificando il parametro `EnableSCSIPersistentReservations` con un valore di `$false`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
```

b. A partire da AWS NVMe`1.5.0`, `install.ps1` lo script installa sempre lo strumento con il driver. `ebsnvme-id`

(Facoltativo) Per le versioni `1.4.0`, `1.4.1` e `1.4.2`, lo script `install.ps1` consente di specificare se lo strumento `ebsnvme-id` deve essere installato con il driver.

i. Per installare lo strumento `ebsnvme-id`, specificare `InstallEBSNVMeIdTool 'Yes'`.

ii. Se non si desidera installare lo strumento, specificare `InstallEBSNVMeIdTool 'No'`.

Se non si specifica `InstallEBSNVMeIdTool` e lo strumento è già presente su `C:\ProgramData\Amazon\Tools`, il pacchetto aggiornerà lo strumento per impostazione predefinita. Se lo strumento non è presente, `install.ps1` non aggiornerà lo strumento per impostazione predefinita.

Se non desideri installare lo strumento come parte del pacchetto ma desideri installarlo in un secondo momento, puoi trovare la versione più recente o lo strumento nel pacchetto driver. In alternativa, puoi scaricare la versione `1.0.0` da Amazon S3:

Scarica lo strumento `ebsnvme-id`.

5. Se il programma di installazione non riavvia l'istanza, riavviala manualmente.

Installa o aggiorna i driver AWS NVMe con Distributor

È possibile utilizzare Distributor, una funzionalità di AWS Systems Manager, per installare il pacchetto driver NVMe una sola volta o con aggiornamenti pianificati.

1. Per istruzioni su come installare il pacchetto di driver NVMe utilizzando Distributor, consulta le procedure descritte in Installazione o aggiornamento dei pacchetti nella Guida per l'utente di Amazon EC2 Systems Manager.
2. Per Tipo di installazione, seleziona Disinstalla e reinstalla.

3. Per Nome, scegli AWSNVMe.
4. (Facoltativo) Per Argomenti aggiuntivi, è possibile personalizzare l'installazione specificando i valori. I valori devono essere formattati utilizzando una sintassi JSON valida. Per esempi di come passare argomenti aggiuntivi per il pacchetto `aws configure`, consultare la Documentazione di Amazon EC2 Systems Manager.

   a. A partire da AWS NVMe`1.5.0`, il driver supporta le prenotazioni persistenti SCSI per Windows Server 2016 e versioni successive. Per impostazione predefinita, questa funzionalità non è abilitata durante l'installazione.

      - Per abilitare questa funzionalità, specificare. `{"SSM_EnableSCSIPersistentReservations": true}`
      - Se non desideri abilitare questa funzionalità, specifica`{"SSM_EnableSCSIPersistentReservations": false}`.

   b. A partire da AWS NVMe`1.5.0`, lo `install.ps1` script installerà sempre lo `ebsnvme-id` strumento.

      (Facoltativo) Per le versioni `1.4.0`, `1.4.1` e `1.4.2`, lo script `install.ps1` consente di specificare se lo strumento ebsnvme-id deve essere installato con il driver.

      - Per installare lo strumento ebsnvme-id, specificare. `{"SSM_InstallEBSNVMeIdTool": "Yes"}`
      - Se non si desidera installare lo strumento, specificare `{"SSM_InstallEBSNVMeIdTool": "No"}`.

        Se `SSM_InstallEBSNVMeIdTool` non è specificato per Argomenti aggiuntivi e lo strumento è già presente in `C:\ProgramData\Amazon\Tools`, il pacchetto aggiornerà lo strumento per impostazione predefinita. Se lo strumento non è presente, il pacchetto non aggiornerà lo strumento per impostazione predefinita.

        Se non desideri installare lo strumento come parte del pacchetto ma desideri installarlo in un secondo momento, puoi trovare la versione più recente dello strumento nel pacchetto driver. In alternativa, puoi scaricare la versione `1.0.0` da Amazon S3:

        Scarica lo strumento `ebsnvme-id`.
5. Se il programma di installazione non riavvia l'istanza, riavviala manualmente.

Configura le prenotazioni persistenti SCSI

Dopo aver installato la versione `1.5.0` o successiva del driver AWS NVMe, è possibile abilitare o disabilitare le prenotazioni permanenti SCSI utilizzando il registro di Windows per Windows Server 2016 e versioni successive. Per applicare le modifiche al registro è necessario riavviare l'istanza.

È possibile abilitare le prenotazioni persistenti SCSI con il seguente comando che imposta il valore `EnableSCSIPersistentReservations` su `1`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

È possibile disabilitare le prenotazioni persistenti SCSI con il seguente comando che imposta il valore `EnableSCSIPersistentReservations` su `0`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

AWS Cronologia delle versioni del driver NVMe

La tabella seguente descrive le versioni rilasciate del driver AWS NVMe.

Versione del pacchetto	Versione driver	Dettagli	Data di rilascio
1.5.1	1.5.0	È stato corretto lo script di installazione per creare una cartella per lo strumento ebsnvme-id se non è presente.	17 novembre 2023
1.5.0	1.5.0	È stato aggiunto il supporto per le prenotazioni persistenti SCSI (Small Computer System Interface) per le istanze che eseguono Windows Server 2016 e versioni successive. Lo strumento ebsnvme-id (`ebsnvme-id.exe`) è ora installato per impostazione predefinita.	31 agosto 2023

Versione del pacchetto	Versione driver	Dettagli	Data di rilascio
1.4.2	1.4.2	È stato corretto un bug che Driver AWS NVMe impediva il supporto dei volumi di Instance Store sulle istanze D3.	16 marzo 2023
1.4.1	1.4.1	Riferisce su Namespace Preferred Write Granularity (NPGW) per i volumi EBS che supportano questa caratteristica NVMe opzionale. Per ulteriori informazioni, consulta la sezione 8.25, "Miglioramento delle prestazioni attraverso la dimensione I/O e l'aderenza dell'allineamento", in NVMe Base Specification, versione 1.4.	20 maggio 2022

Versione del pacchetto	Versione driver	Dettagli	Data di rilascio
1.4.0	1.4.0	• Aggiunto il supporto per gli IOCTL che consentono alle applicazioni di interagire con i dispositivi NVMe. Questo supporto consente alle applicazioni di ottenere l'elenco di `IdentifyController` , `IdentifyNamespace` e `NameSpace` dal dispositivo NVMe. Per ulteriori informazioni, consultare Query specifiche del protocollo nella documentazione Microsoft. • AWSNVMe L'installazione 1.4.0 su Windows Server 2008 R2 avrà esito negativo. AWSNVMe la versione 1.3.2 e precedenti sono supportate in Windows Server 2008 R2. • La versione del driver 1.4.0 e lo strumento `ebsnvme-id` più recente (`ebsnvme-id.exe`) sono combinati in un unico pacchetto. Questa combinazione consente di installare sia il driver che lo strumento da un unico pacchetto. Per ulteriori dettagli, consulta Installa o aggiorna i driver NVMe utilizzando AWS PowerShell. • Correzioni di bug e miglioramenti dell'affidabilità.	23 novembre 2021
1.3.2	1.3.2	È stato risolto un problema che potrebbe causare il danneggiamento dei dati relativo alla modifica dei volumi EBS che elaborano attivamente operazioni di I/O. I clienti che non modificano i volumi EBS online (ad esempio attraverso ridimensionamento o modifica del tipo) non sono interessati.	10 settembre 2019

Versione del pacchetto	Versione driver	Dettagli	Data di rilascio
1.3.1	1.3.1	Migliorie in termini di affidabilità.	21 maggio 2019
1.3.0	1.3.0	Miglioramenti dell'ottimizzazione dei dispositivi.	31 agosto 2018
1.2.0	1.2.0	Miglioramenti delle prestazioni e dell'affidabilità dei dispositivi AWS NVMe su tutte le istanze supportate, incluse le istanze bare metal.	13 giugno 2018
1.0.0	1.0.0	AWS Driver NVMe per i tipi di istanze supportati che eseguono Windows Server.	12 febbraio 2018

Sottoscrizione alle notifiche di

Amazon SNS può avvisarti in caso di pubblicazione di nuove versioni dei driver Windows di EC2. Utilizza la procedura seguente per effettuare l'iscrizione a queste notifiche.

Per effettuare la sottoscrizione alle notifiche EC2 dalla console

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario selezionare questa regione perché le notifiche SNS per le quali stai effettuando la sottoscrizione si trovano in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Create subscription (Crea sottoscrizione) segui questi passaggi:
   a. In Topic ARN (ARN argomento) copia il seguente nome della risorsa Amazon (ARN):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. In Protocol (Protocollo), scegli `Email`.
   c. In Endpoint digita l'indirizzo e-mail utilizzabile per ricevere le notifiche.

d. Scegli Create Subscription (Crea sottoscrizione).

6. Riceverai a breve un'e-mail di conferma. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

Quando i nuovi driver Windows di EC2 vengono rilasciati, inviamo notifiche ai sottoscrittori. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Per annullare la sottoscrizione alle notifiche dei driver Windows per Amazon EC2

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
3. Selezionare la casella di spunta della sottoscrizione, quindi scegliere Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni). Quando viene richiesta la conferma, seleziona Elimina.

Per sottoscrivere le notifiche EC2 utilizzando il AWS CLI

Per sottoscrivere le notifiche EC2 con AWS CLI, usa il seguente comando.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Per iscriverti alle notifiche EC2 utilizzando AWS Tools for Windows PowerShell

Per iscriverti alle notifiche EC2 con AWS Tools for Windows PowerShell, usa il seguente comando.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Configurazione dell'istanza Windows

Dopo aver avviato un'istanza di Windows, puoi accedere come amministratore per eseguire configurazioni aggiuntive per gli agenti di avvio e le funzionalità specifiche di Windows. I seguenti argomenti si concentrano sulla configurazione delle istanze di Windows.

Indice

- Usa EC2 Fast Launch per le tue istanze Windows
- Usa gli acceleratori Amazon Elastic Graphics su istanze Windows
- Installazione di WSL sulla tua istanza di Windows

Configura le impostazioni di avvio per le istanze Windows di Amazon EC2

Gli agenti di avvio di Amazon EC2 eseguono attività durante l'avvio dell'istanza ed eseguono se un'istanza viene arrestata e successivamente avviata o riavviata. Per informazioni su un agente specifico, consulta le pagine di dettaglio nell'elenco seguente.

- Configurare un'istanza Windows tramite EC2Launch v2
- Configurazione dell'istanza Windows tramite EC2Launch
- Configurare un'istanza di Windows utilizzando il servizio EC2Config (legacy)

Contenuti

Confronta gli agenti di lancio di Amazon EC2

Nella tabella seguente vengono illustrate le principali differenze funzionali tra EC2Config, EC2Launch v1 e EC2Launch v2.

Caratteristica	EC2Config	EC2Launch v1	EC2Launch v2
Run as (Esegui come)	Servizio Windows	PowerShell Script	Servizio Windows
Supporta	Solo sistemi operativi legacy	Windows 2016 Windows 2019 (LTSC e SAC)	Windows 2016 Windows 2019 (LTSC e SAC) Windows 2022
File di configurazione	XML	XML	YAML

Caratteristica	EC2Config	EC2Launch v1	EC2Launch v2
Imposta nome utente amministratore	No	No	Sì
Dimensione dei dati utente	16 KB	16 KB	60 KB (compresso)
Dati utente locali inseriti in AMI	No	No	Sì, configurabile
Configurazione delle attività nei dati utente	No	No	Sì
Sfondo configurabile	No	No	Sì
Personalizza l'ordine di esecuzione delle attività	No	No	Sì
Attività configurabili	15	9	20 all'avvio
Supporta il Visualizzatore eventi di Windows	Sì	No	Sì
Numero di tipi di evento del Visualizzatore eventi	2	0	30

Note

La documentazione di EC2Config viene fornita solo come riferimento storico. Le versioni del sistema operativo su cui viene eseguito non sono più supportate da Microsoft. Ti consigliamo vivamente di eseguire l'aggiornamento al servizio di avvio più recente.

Configura il suffisso DNS per gli agenti di avvio di Windows

Con gli agenti di avvio di Amazon EC2, puoi configurare un elenco di suffissi DNS utilizzati dalle istanze Windows per la risoluzione dei nomi di dominio. Gli agenti di avvio sostituiscono le impostazioni standard di Windows nella chiave di `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` registro aggiungendo i seguenti valori all'elenco di ricerca dei suffissi DNS:

- Il dominio dell'istanza
- I suffissi che risultano dalla devoluzione del dominio dell'istanza
- Dominio NV
- I domini specificati da ciascuna scheda di interfaccia di rete

Tutti gli agenti di avvio supportano la configurazione dei suffissi DNS. Per ulteriori informazioni, consulta la versione specifica del Launch Agent:

- Per informazioni sull'`setDnsSuffix`attività e su come configurare i suffissi DNS in EC2Launch v2, consulta. setDnsSuffix
- Per informazioni sulla configurazione dell'elenco dei suffissi DNS e su come abilitare o disabilitare la devoluzione per EC2Launch v1, consulta. Configurazione di EC2Launch
- Per informazioni sulla configurazione dell'elenco dei suffissi DNS e su come abilitare o disabilitare la devoluzione per EC2Config, consulta. File delle impostazioni di EC2Config

Devoluzione del nome di dominio

La devoluzione del nome di dominio è un comportamento di Active Directory che consente ai computer di un dominio figlio di accedere alle risorse del dominio principale senza utilizzare un nome di dominio completo. Per impostazione predefinita, la devoluzione del nome di dominio continua fino a quando rimangono solo due nodi nella progressione del nome di dominio.

Gli agenti di avvio eseguono la devoluzione sul nome di dominio se l'istanza è connessa a un dominio e aggiungono i risultati all'elenco di ricerca dei suffissi DNS mantenuto nella chiave di registro. **`System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`** Gli agenti utilizzano le impostazioni delle seguenti chiavi di registro per determinare il comportamento di devoluzione.

- **`System\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution`**
  - Quando non è impostata, disabilita la devoluzione
  - Se impostato su`1`, abilita la devoluzione (impostazione predefinita)
  - Se impostato su, disabilita la `0` devoluzione
- **`System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel`**
  - Quando non è impostata, usa level of 2 (impostazione predefinita)
  - Se impostato su `3` o superiore, usa il valore per impostare il livello

Quando si disabilita la devoluzione o si modificano le impostazioni di devoluzione a un livello superiore, la chiave di `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` registro contiene ancora i suffissi aggiunti in precedenza. Non vengono rimossi automaticamente. Puoi aggiornare manualmente l'elenco oppure puoi cancellarlo e lasciare che il tuo agente si occupi della procedura per configurare il nuovo elenco.

> **Note**
>
> Per cancellare l'elenco dei suffissi DNS dal registro, puoi eseguire il comando seguente.
>
> ```
> PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -
> MethodName "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =
>  $null } | Out-Null
> ```

Esempi di devoluzione

Gli esempi seguenti mostrano la progressione dei nomi di dominio attraverso il processo di devoluzione.

`corp.example.com`

- Passa a `example.com`

`locale.region.corp.example.com`

1. Passa a `region.corp.example.com`

2. Passa a `corp.example.com`
3. Passa a `example.com`

`locale.region.corp.example.com`con un'impostazione di `DomainNameDevolutionLevel=3`

1. Passa a `region.corp.example.com`
2. Passa a. `corp.example.com` La progressione si interrompe qui, a causa dell'impostazione del livello.

Configurare un'istanza Windows tramite EC2Launch v2

Tutte le istanze supportate di Amazon EC2 che eseguono Windows Server 2022 includono l'agente di avvio EC2Launch v2 (`EC2Launch.exe`) di default. Forniamo inoltre le AMI di Windows Server 2016 e 2019 con EC2Launch v2 installato come agente di avvio di default. Queste AMI sono fornite in aggiunta alle AMI di Windows Server 2016 e 2019 che includono EC2Launch v1. È possibile cercare le AMI di Windows che includono EC2Launch v2 di default inserendo il seguente prefisso nella ricerca dalla pagina AMI nella console Amazon EC2: `EC2LaunchV2-Windows_Server-*`.

EC2Launch v2 esegue attività durante il startup dell'istanza e viene eseguito se un'istanza viene arrestata e successivamente avviata o se viene riavviata. EC2Launch v2 può anche eseguire attività on demand. Alcune di queste attività sono abilitate automaticamente, mentre altre devono essere abilitate manualmente. Il servizio EC2Launch v2 supporta tutte le caratteristiche di EC2Config ed EC2Launch.

Questo servizio utilizza un file di configurazione per controllarne il funzionamento. Puoi aggiornare il file di configurazione utilizzando uno strumento grafico o modificandolo direttamente come un singolo file .yml (`agent-config.yml`). I file binari del servizio si trovano nella directory `%ProgramFiles%\Amazon\EC2Launch`.

EC2Launch v2 pubblica i log di eventi di Windows per facilitare la risoluzione degli errori e l'impostazione dei trigger. Per ulteriori informazioni, consulta Log di eventi di Windows.

Sistemi operativi supportati

- Windows Server 2022
- Windows Server 2019 (canale di manutenzione a lungo termine e canale semestrale)
- Windows Server 2016

Contenuto della sezione EC2launch v2

Panoramica di EC2Launch v2

EC2Launch v2 è un servizio che esegue attività durante l'avvio dell'istanza e viene eseguito se un'istanza viene arrestata e successivamente avviata o se viene riavviata.

Argomenti della panoramica

Per confrontare le funzionalità della versione Launch Agent, consultaConfronta gli agenti di lancio di Amazon EC2.

Concetti di EC2Launch v2

I seguenti concetti sono utili per capire quando utilizzare EC2Launch v2.

Attività

Puoi richiamare un'attività per eseguire un'operazione su un'istanza. Puoi configurare le attività nel file `agent-config.yml` o tramite i dati utente. Per un elenco delle attività disponibili per EC2Launch v2, consulta Attività EC2Launch v2. Per lo schema di configurazione delle attività e informazioni dettagliate, consulta Configurazione dell'attività di EC2Launch v2.

Stage

Una fase è un raggruppamento logico di attività eseguito dall'agente EC2Launch v2. Alcune attività possono essere eseguite solo in una fase specifica. Altre possono essere eseguite in più fasi. Quando utilizzi `agent-config.yml`, è necessario specificare un elenco di fasi e un elenco di attività da eseguire all'interno di ciascuna fase.

Il servizio esegue le fasi nel seguente ordine:

Fase 1: Avvio

Fase 2: Rete

Fase 3: PreReady

Windows è pronto

Al termine della PreReady fase, il servizio invia il `Windows is ready` messaggio alla console Amazon EC2.

Fase 4: PostReady

I dati dell'utente vengono eseguiti durante la PostReadyfase. Alcune versioni degli script vengono eseguite prima della PostReadyfase del `agent-config.yml` file e altre vengono eseguite dopo, come segue:

Prima di `agent-config.yml`

- Versione 1.1 dei dati utente in YAML
- Dati utente XML

Dopo di `agent-config.yml`

- Dati utente YAML versione 1.0 (versione legacy per compatibilità con le versioni precedenti)

Per le fasi e attività di esempio, consulta Esempio: `agent-config.yml`.

Quando utilizzi i dati utente, devi specificare un elenco di attività per l'esecuzione dell'agente di avvio. La fase è implicita. Per le attività di esempio, consulta Esempio: dati utente.

EC2Launch v2 esegue l'elenco delle attività nell'ordine specificato in `agent-config.yml` e nei dati utente. Le fasi vengono eseguite in sequenza. La fase successiva inizia dopo il completamento della fase precedente. Anche le attività vengono eseguite in sequenza.

Frequenza

La frequenza delle attività stabilisce quando le attività devono essere eseguite a seconda del contesto di avvio. La maggior parte delle attività ha una sola frequenza consentita. È possibile specificare una frequenza per le attività `executeScript`.

Vedrai le seguenti frequenze nella Configurazione dell'attività di EC2Launch v2.

- Una volta: l'attività viene eseguita una volta, quando l'AMI viene avviata per la prima volta (Sysprep terminato).
- Sempre: l'attività viene eseguita ogni volta che viene attivato l'agente di avvio. L'agente di avvio viene eseguito quando:
  - un'istanza viene avviata o riavviata
  - viene eseguito il servizio EC2Launch
  - viene richiamato `EC2Launch.exe run`

agent-config

`agent-config` è un file che si trova nella cartella di configurazione per EC2Launch v2. Include la configurazione per l'avvio, la rete e PostReady le fasi. PreReady Questo file viene utilizzato per specificare la configurazione di un'istanza per le attività che devono essere eseguite quando l'AMI viene avviata per la prima volta o per le volte successive.

Di default, l'installazione di EC2Launch v2 installa un file `agent-config` che include le configurazioni consigliate utilizzate nelle AMI standard di Amazon Windows. Puoi aggiornare il file di configurazione per modificare l'esperienza di avvio predefinita per l'AMI specificata da EC2Launch v2.

Dati utente

I dati utente sono dati configurabili quando si avvia un'istanza. Puoi aggiornare i dati utente per modificare dinamicamente la modalità di configurazione delle AMI personalizzate o delle AMI di avvio rapido. EC2Launch v2 supporta una lunghezza di input dei dati utente di 60 kB. I dati utente includono solo la UserData fase e pertanto vengono eseguiti dopo il `agent-config` file. È possibile immettere i dati utente quando si avvia un'istanza utilizzando la procedura guidata di avvio dell'istanza, oppure è possibile modificare i dati utente dalla console EC2. Per informazioni sull'utilizzo dei dati utente, consulta In che modo Amazon EC2 gestisce i dati utente per le istanze Windows.

Attività di EC2Launch v2

EC2Launch v2 può eseguire ad ogni avvio le seguenti attività:

- Impostare un nuovo sfondo personalizzato e facoltativo che esegue il rendering delle informazioni riguardanti l'istanza.
- Impostare gli attributi per l'account amministratore creato nel computer locale.
- Aggiungere i suffissi DNS all'elenco dei suffissi di ricerca. All'elenco vengono aggiunti solo i suffissi che non esistono già.
- Impostare le lettere di unità per eventuali volumi aggiuntivi ed estenderli per utilizzare lo spazio disponibile.
- Scrive i file dalla configurazione sul disco.
- Esegui gli script specificati nel file di configurazione EC2Launch v2 o da. `user-data` Gli script di `user-data` possono essere in testo semplice o compressi e forniti in formato base64.
- Eseguire un programma con argomenti specificati.
- Impostare il nome del computer.
- Inviare le informazioni sull'istanza alla console Amazon EC2.
- Inviare l'impronta del certificato RDP alla console Amazon EC2.
- Estendere in modo dinamico la partizione del sistema operativo per includere qualsiasi spazio non partizionato.
- Eseguire i dati utente. Per ulteriori informazioni sulla specifica dei dati utente, consulta Configurazione dell'attività di EC2Launch v2.
- Imposta istradamenti statici non persistenti per raggiungere il servizio metadati e i server AWS KMS .
- Imposta le partizioni non di avvio su o. `mbr` `gpt`
- Avviare il servizio Systems Manager dopo Sysprep.
- Ottimizzare le impostazioni ENA.
- Abilitare OpenSSH per le versioni successive di Windows.
- Abilitare i frame jumbo.
- Impostare Sysprep per l'esecuzione con EC2Launch v2.
- Pubblicare i log di eventi di Windows.

Telemetria

La telemetria è un'informazione aggiuntiva che consente di AWS comprendere meglio i requisiti, diagnosticare i problemi e fornire funzionalità con cui migliorare l'esperienza. Servizi AWS

EC2Launch v2 versione `2.0.592` e successive raccolgono dati di telemetria, ad esempio parametri ed errori di utilizzo. Questi dati vengono raccolti dall'istanza Amazon EC2 in cui viene eseguito EC2Launch v2. Sono incluse tutte le AMI Windows di proprietà di. AWS

I seguenti tipi di telemetria vengono raccolti da EC2Launch v2:

- Informazioni di utilizzo: comandi dell'agente, metodo di installazione e frequenza di esecuzione pianificata.
- Errori e informazioni diagnostiche: codici di errore di installazione dell'agente, codici di errore di esecuzione e stack di chiamate di errore.

Esempi di dati raccolti:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

La telemetria è abilitata per impostazione predefinita. Puoi disabilitare la raccolta dati di telemetria in qualsiasi momento. Se la telemetria è abilitata, EC2Launch v2 invia i dati di telemetria senza ulteriori notifiche ai clienti.

Visibilità della telemetria

Quando la telemetria è abilitata, viene visualizzata nell'output della console Amazon EC2 come segue:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Disabilitare la telemetria su un'istanza

Per disattivare la telemetria per una singola istanza, puoi impostare una variabile di ambiente di sistema oppure utilizzare MSI per modificare l'installazione.

Per disattivare la telemetria impostando una variabile di ambiente di sistema, esegui il comando seguente come amministratore.

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Per disabilitare la telemetria utilizzando MSI, esegui il comando seguente dopo il download dell'MSI.

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Installare la versione più recente di EC2Launch v2

Puoi utilizzare uno dei seguenti metodi per installare l'agente EC2Launch v2 sulla tua istanza EC2:

- Scarica l'agente da Amazon S3 e installalo con Windows. PowerShell Per gli URL dei download, consulta Download di EC2Launch v2 su Amazon S3.
- Installazione con SSM Distributor
- Installazione da componente EC2 Image Builder.
- Avvia la tua istanza da un'AMI su cui è preinstallato EC2Launch v2.

> **Warning**
>
> AmazonEC2Launch.msi disinstalla le versioni precedenti dei servizi di avvio EC2, ad esempio EC2Launch (v1) o EC2config.

Per l'installazione, seleziona la scheda corrispondente al tuo metodo preferito.

Windows PowerShell

Per installare l'ultima versione dell'agente EC2Launch v2 con Windows PowerShell, segui questi passaggi.

1. Crea la tua directory locale.

   ```
   New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
   ```

2. Imposta l'URL per la posizione di download. Esegui il comando seguente con l'URL Amazon S3 che utilizzerai. Per gli URL dei download, consulta Download di EC2Launch v2 su Amazon S3.

   ```
   $Url = "Amazon S3 URL/AmazonEC2Launch.msi"
   ```

3. Utilizza il seguente comando composito per scaricare l'agente e avviare l'installazione

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path
 $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

> **Note**
>
> Se ricevi un errore durante il download del file e utilizzi Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il seguente comando e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Per verificare l'installazione, controlla che il file msi esista nella directory EC2Launch v2 della tua istanza (`C:\ProgramData\Amazon\EC2Launch`).

AWS Systems Manager Distributor

Per configurare gli aggiornamenti automatici per EC2Launch v2 con AWS Systems Manager Quick Setup, consulta. Installa e aggiorna automaticamente con Distributor Quick Setup

Puoi anche eseguire un'installazione unica del pacchetto dal Distributore. `AWSEC2Launch-Agent` AWS Systems Manager Per istruzioni su come installare un pacchetto da System Manager Distributor, consulta Installazione o pacchetti di aggiornamento nella AWS Systems Manager Guida per l'utente.

EC2 Image Builder component

Quando si costruisce un'immagine personalizzata con EC2 Image Builder, è possibile installare il componente `ec2launch-v2-windows`. Per istruzioni su come creare un'immagine personalizzata con EC2 Image Builder, vedi Creazione di una pipeline di immagini utilizzando la procedura guidata della console EC2 Image Builder nellaGuida per l'utente di EC2 Image Builder.

AMI

Per impostazione predefinita, EC2Launch v2 è preinstallato sulle AMI e sulle seguenti AMI UEFI di Windows Server 2022:

- Windows_Server-2022-English-Full-Base
- Windows_Server-2022-English-Core-Base
- AMI di Windows Server 2022 con tutte le altre lingue
- AMI di Windows Server 2022 con SQL installato
- Windows_Server-2022-English-Core-EKS_Optimized

EC2Launch è inoltre preinstallato sulle seguenti AMI Windows Server. Puoi trovare queste AMI dalla console Amazon EC2 oppure utilizzando il seguente prefisso di ricerca `EC2LaunchV2-` nel AWS CLI.

- EC2LaunchV2_Preview-Windows_Server-2019-English-Core-Base
- EC2LaunchV2_Preview-Windows_Server-2019-English-Full-Base
- EC2LaunchV2_Preview-Windows_Server-2016-English-Core-Base
- EC2LaunchV2_Preview-Windows_Server-2016-English-Full-Base
- EC2LaunchV2-Windows_Server-2012_R2_RTM-English-Full-Base
- EC2LaunchV2-Windows_Server-2012_RTM-English-Full-Base

Installa e aggiorna automaticamente EC2Launch v2 con Distributor Quick Setup AWS Systems Manager

Con AWS Systems Manager Distributor Quick Setup, puoi configurare gli aggiornamenti automatici per EC2Launch v2. Il processo seguente configura una Systems Manager Association sull'istanza che aggiorna automaticamente l'agente EC2Launch v2 con una frequenza specificata dall'utente. L'associazione creata da Distributor Quick Setup può includere istanze all'interno di una regione Account AWS and o istanze all'interno di un'organizzazione. AWS Per ulteriori informazioni sulla configurazione di un'organizzazione, vedere Tutorial: Creazione e configurazione di un'organizzazione nella Guida per l'utente.AWS Organizations

Prima di iniziare, assicurati che le istanze soddisfino tutti i prerequisiti.

Prerequisiti

Per configurare gli aggiornamenti automatici con Distributor Quick Setup, le istanze devono soddisfare i seguenti prerequisiti.

- Hai almeno un'istanza in esecuzione che supporta EC2Launch v2. Consulta i sistemi operativi supportati per. EC2Launch v2

- Hai eseguito le attività di configurazione di Systems Manager sulle tue istanze. Per ulteriori informazioni, vedere Configurazione di Systems Manager nella Guida AWS Systems Manager per l'utente.
- EC2Launch v2 deve essere l'unico agente di avvio installato sull'istanza. Se hai installato più di un agente di lancio, la configurazione di Distributor Quick Setup avrà esito negativo. Prima di configurare EC2Launch v2 con un Distributor Quick Setup, disinstalla gli agenti di lancio EC2Config o EC2Launch v1, se esistono.

Configura Distributor Quick Setup per EC2Launch v2

Per creare una configurazione per EC2Launch v2 con Distributor Quick Setup, utilizza le seguenti impostazioni quando completi i passaggi per la distribuzione del pacchetto Distributor:

- Pacchetti software: agente Amazon EC2Launch v2.
- Frequenza di aggiornamento: seleziona una frequenza dall'elenco.
- Obiettivi: scegli tra le opzioni di distribuzione disponibili.

Per verificare lo stato della configurazione, accedere alla scheda Systems Manager Quick Setup Configurations nel AWS Management Console.

1. Aprire la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel pannello di navigazione, scegli Configurazione rapida.
3. Nella scheda Configurazioni, seleziona la riga associata alla configurazione che hai creato. La scheda Configurazioni elenca le configurazioni e include un riepilogo dei dettagli chiave, come la regione, lo stato di distribuzione e lo stato dell'associazione.

   > **Note**
   >
   > Il nome dell'associazione per ogni configurazione del distributore EC2Launch v2 inizia con il seguente prefisso:. `AWS-QuickSetup-Distributor-EC2Launch-Agent-`

4. Per visualizzare i dettagli, seleziona la configurazione e scegli Visualizza dettagli.

Per ulteriori informazioni e procedure di risoluzione dei problemi, consulta Risoluzione dei problemi relativi ai risultati della configurazione rapida nella Guida per AWS Systems Manager l'utente.

Download di EC2Launch v2 su Amazon S3

Per installare la versione più recente di EC2Launch v2, scarica l'installer dai seguenti percorsi:

> **Note**
>
> Il link di installazione a 32 bit diverrà obsoleto. Suggeriamo di utilizzare il link di installazione a 64 bit per installare EC2Launch v2. Se occorre un agente di avvio a 32 bit, usa EC2Config.

- 64 bit — https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi
- 32 bit — https://s3.amazonaws.com/amazon-ec2launch-v2/windows/386/latest/AmazonEC2Launch.msi

Configurazione delle opzioni di installazione

Durante l'installazione o l'aggiornamento di EC2Launch v2, puoi configurare le opzioni di installazione con la finestra di installazione di EC2Launch v2 o con il msiexeccomando in una shell a riga di comando.

Alla prima esecuzione su un'istanza di EC2Launch v2, inizializza le impostazioni dell'agente di avvio sull'istanza come segue:

- Crea il percorso locale e vi scrive il file dell'agente di avvio. Questo a volte viene definito come installazione pulita.
- Crea la variabile d'ambiente `EC2LAUNCH_TELEMETRY` se non esiste già e la imposta in base alla tua configurazione.

Per i dettagli della configurazione, seleziona la scheda che corrisponde al metodo di configurazione che utilizzerai.

Amazon EC2Launch Setup dialog

Quando installi o aggiorni EC2Launch v2, puoi configurare le seguenti opzioni di installazione tramite la finestra di dialogo di installazione di EC2Launch v2.

Opzioni Installazione di base

Invia telemetria

Se includi questa funzionalità nella finestra di configurazione, l'installatore imposta la `EC2LAUNCH_TELEMETRY` variabile di ambiente con un valore di`1`. Se disabiliti Invia telemetria, l'installatore imposta la variabile di ambiente su un valore di `0`.

Quando l'agente EC2Launch v2 è in esecuzione, legge la`EC2LAUNCH_TELEMETRY` variabile di ambiente per determinare se caricare dati di telemetria. Se il valore è `1`, carica i dati. Altrimenti, non li carica.

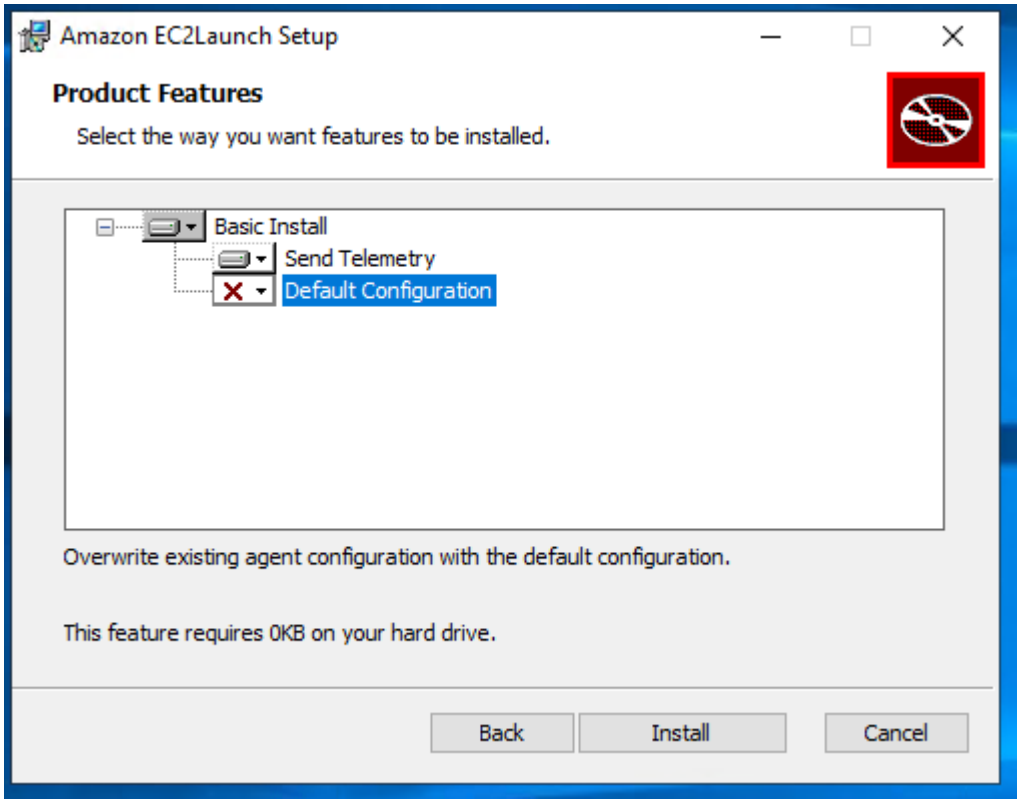
Configurazione di default

La configurazione predefinita per EC2Launch v2 consiste nel sovrascrivere l'agente di avvio locale se già esistente. La prima volta che esegui un'installazione su un'istanza, la configurazione predefinita esegue un'installazione pulita. Se disattivi la configurazione predefinita nell'installazione iniziale, l'installazione non riesce.

Se esegui nuovamente l'installazione sull'istanza, puoi disabilitare la configurazione predefinita per eseguire un aggiornamento che non sostituisca il file `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`.

Esempio: installazione di EC2Launch v2 con telemetria

L'esempio seguente mostra la finestra di configurazione di EC2Launch v2 configurata per aggiornare l'installazione corrente e abilitare la telemetria. Questa configurazione esegue un'installazione senza sostituire il file di configurazione dell'agente e imposta la `EC2LAUNCH_TELEMETRY` variabile di ambiente al valore `1`.



Command line

Quando installi o aggiorni EC2Launch v2, puoi configurare le seguenti opzioni di installazione con il comando msiexec in una shell a riga di comando.

`ADDLOCAL`Valori parametri

Base (richiesto)

Installa l'agente di avvio. Se questo valore non è presente nel parametro `ADDLOCAL` l'installazione termina.

Elimina

Quando includi il valore `Clean` nel parametro `ADDLOCAL`, l'installatore scrive il file di configurazione dell'agente nella seguente posizione:`%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Se il file di configurazione dell'agente esiste già, lo sovrascrive.

Se lasci il valore `Clean` al di fuori del parametro `ADDLOCAL`, l'installatore esegue un aggiornamento che non sostituisce il file di configurazione dell'agente.

Telemetria

Se includi il valore `Telemetry` nel parametro `ADDLOCAL`, l'installatore imposta la variabile di ambiente `EC2LAUNCH_TELEMETRY` a un valore di `1`.

Se lasci il valore `Telemetry` al di fuori del parametro `ADDLOCAL`, l'installatore imposta la variabile di ambiente a valore di `0`.

Quando l'agente EC2Launch v2 è in esecuzione, legge la`EC2LAUNCH_TELEMETRY` variabile di ambiente per determinare se caricare dati di telemetria. Se il valore è `1`, carica i dati. Altrimenti, non li carica.

Esempio: installazione di EC2Launch v2 con telemetria

```
& msiexec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"
 ADDLOCAL="Basic,Clean,Telemetry" /q
```

Verifica la versione EC2Launch v2

Utilizzare la procedura seguente per verificare la versione di EC2Launch v2 installata sulle istanze.

Windows PowerShell

Verifica la versione installata di EC2Launch v2 con Windows, come segue. PowerShell

1. Lancia un'istanza dall'AMI e connettila.
2. Esegui il seguente comando PowerShell per verificare la versione installata di EC2Launch v2:

   ```
   & "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
   ```

Windows Control Panel

Verifica la versione installata di EC2Launch v2 nel Pannello di Controllo di Windows come segue:

1. Lancia un'istanza dall'AMI e connettila.
2. Apri il Pannello di Controllo e scegli Programmi e funzionalità.
3. Nella lista dei programmi installati, cerca `Amazon EC2Launch`. Il numero della versione viene mostrato nella colonna Version (Versione).

Per visualizzare gli aggiornamenti più recenti per le AMI AWS Windows, consulta la cronologia delle versioni di Windows AMI nel AWS Windows AMI Reference.

Per la versione più recente di EC2Launch v2, consulta Cronologia delle versioni di EC2Launch v2.

Per la versione più recente dello strumento di migrazione di EC2Launch v2, consulta Cronologia delle versioni dello strumento di migrazione di EC2Launch v2.

Puoi ricevere notifiche quando vengono rilasciate nuove versioni del servizio EC2Launch v2. Per ulteriori informazioni, consulta Sottoscrizione alle notifiche del servizio EC2Launch v2.

Migrazione a EC2Launch v2

Lo strumento di migrazione EC2Launch aggiorna l'agente di avvio installato (EC2config ed EC2Launch v1) disinstallandolo e installando EC2Launch v2. Le configurazioni applicabili dei servizi di avvio precedenti vengono migrate automaticamente al nuovo servizio. Lo strumento di migrazione non rileva alcuna attività pianificata collegata agli script EC2Launch v1, pertanto non imposta automaticamente tali attività in EC2Launch v2. Per configurare queste attività, modificare il file `agent-config.yml` o utilizzare la finestra di dialogo Impostazioni di EC2Launch v2. Ad esempio, se un'istanza dispone di un'attività pianificata che esegue `InitializeDisks.ps1`, dopo avere eseguito lo strumento di migrazione, è necessario specificare i volumi che si desidera inizializzare nella finestra di dialogo delle impostazioni di EC2Launch v2. Vedere il passaggio 6 della procedura per Modifica delle impostazioni utilizzando la finestra di dialogo delle impostazioni di EC2Launch v2.

Puoi scaricare lo strumento di migrazione o installarlo con un documento SSM. RunCommand

Puoi scaricare lo strumento dalle seguenti posizioni:

> **Note**
>
> Il link allo strumento di migrazione a 32 bit diverrà obsoleto. Suggeriamo di utilizzare il link di installazione a 64 bit per eseguire la migrazione a EC2Launch v2. Se occorre un agente di avvio a 32 bit, usa EC2Config.

- 64 bit: https://s3.amazonaws.com/amazon-ec2launch-v2-utils/ MigrationTool /Windows/AMD64/ latest/EC2 .zip LaunchMigrationTool
- 32 bit — https://s3.amazonaws.com/amazon-ec2launch-v2-utils/ MigrationTool /Windows/386/ Latest/EC2 .zip LaunchMigrationTool

> **Note**
>
> È necessario eseguire lo strumento di migrazione EC2Launch v2 come amministratore. EC2Launch v2 viene installato come servizio dopo l'esecuzione dello strumento di migrazione. Non viene eseguito immediatamente. Per impostazione predefinita, viene eseguito durante il startup dell'istanza e viene eseguito se un'istanza viene arrestata e successivamente avviata o se viene riavviata.

Utilizza il documento SSM `AWSEC2Launch-RunMigration` per eseguire la migrazione alla versione più recente di EC2Launch con SSM Run Command. Il documento non richiede alcun parametro. Per ulteriori informazioni sull'utilizzo di SSM Run Command, consulta Run Command di AWS Systems Manager.

Lo strumento di migrazione applica le seguenti configurazioni da EC2Config a EC2Launch v2.

- Se `Ec2DynamicBootVolumeSize` è impostato su `false`, rimuove la fase `boot` di EC2Launch v2
- Se `Ec2SetPassword` è impostato su `Enabled`, imposta il tipo di password di EC2Launch v2 su `random`
- Se `Ec2SetPassword` è impostato su `Disabled`, imposta il tipo di password di EC2Launch v2 su `donothing`
- Se `SetDnsSuffixList` è impostato su `false`, rimuove l'attività `setDnsSuffix` di EC2Launch v2
- Se `EC2SetComputerName` è impostato su true (vero), aggiunge l'attività `setHostName` di EC2Launch v2 alla configurazione `yaml`

Lo strumento di migrazione applica le seguenti configurazioni da EC2Launch v1 a EC2Launch v2.

- Se `ExtendBootVolumeSize` è impostato su `false`, rimuove la fase `boot` di EC2Launch v2
- Se `AdminPasswordType` è impostato su `Random`, imposta il tipo di password di EC2Launch v2 su `random`
- Se `AdminPasswordType` è impostato su `Specify`, imposta il tipo di password di EC2Launch v2 su `static` e i dati della password sulla password specificata in `AdminPassword`
- Se `SetWallpaper` è impostato su `false`, rimuove l'attività `setWallpaper` di EC2Launch v2
- Se `AddDnsSuffixList` è impostato su `false`, rimuove l'attività `setDnsSuffix` di EC2Launch v2

- Se `SetComputerName` è impostato su `true`, aggiunge l'attività `setHostName` di EC2Launch v2

Arresto, riavvio, eliminazione o disinstallazione di EC2Launch v2

Puoi gestire il servizio EC2Launch v2 esattamente come faresti con qualsiasi altro servizio Windows.

EC2Launch v2 viene eseguito una volta all'avvio ed esegue tutte le attività configurate. Dopo aver eseguito le attività, il servizio entra nello stato arrestato. Quando riavvii il servizio, vengono eseguite nuovamente tutte le attività configurate, quindi il servizio torna nello stato arrestato.

Per applicare le impostazioni aggiornate sull'istanza, puoi interrompere e riavviare il servizio. Se stai installando manualmente EC2Launch v2, dovrai prima arrestare il servizio.

Per arrestare il servizio EC2Launch v2

1. Avviare l'istanza Windows e connettersi a essa.
2. Scegli Strumenti di amministrazione dal menu Start quindi apri Servizi.
3. Nell'elenco dei servizi, fai clic con il pulsante destro del mouse su Amazon EC2launch e seleziona Arresta.

Per riavviare il servizio EC2Launch v2

1. Avviare l'istanza Windows e connettersi a essa.
2. Scegli Strumenti di amministrazione dal menu Start quindi apri Servizi.
3. Nell'elenco dei servizi, fai clic con il pulsante destro del mouse su Amazon EC2launch e seleziona Riavvia.

Se non devi aggiornare le impostazioni di configurazione, creare le tue AMI o utilizzare AWS Systems Manager, puoi eliminare e disinstallare il servizio. L'eliminazione di un servizio rimuove le sottochiavi del registro. La disinstallazione di un servizio rimuove i file, le sottochiavi del registro e tutti i tasti di scelta rapida del servizio.

Per eliminare il servizio EC2Launch v2

1. Avvia una finestra del prompt dei comandi
2. Esegui il comando riportato qui di seguito:

```
sc delete EC2Launch
```

Per disinstallare EC2Launch v2

1. Avviare l'istanza Windows e connettersi a essa.
2. Dal menu Start, scegli Pannello di controllo.
3. Apri Programmi, quindi apri Programmi e funzionalità.
4. Nell'elenco dei programmi, scegli Amazon EC2Launch. Per verificare di aver scelto la versione 2, controlla la colonna Version (Versione).
5. Scegliere Uninstall (Disinstalla).

Sottoscrizione alle notifiche del servizio EC2Launch v2

Amazon SNS può avvisarti in caso di pubblicazione di nuove versioni del servizio EC2Launch v2. Utilizza la procedura seguente per effettuare l'iscrizione a queste notifiche.

Sottoscrizione alle notifiche di EC2Launch v2

1. Accedi AWS Management Console e apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. Devi selezionare questa regione perché le notifiche SNS per le quali hai effettuato l'iscrizione sono state create in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Crea sottoscrizione segui questi passaggi:
    a. Per ARN argomento utilizza il seguente nome della risorsa Amazon (ARN): arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2.
    b. Per Protocol, scegliere Email.
    c. In Endpoint immetti l'indirizzo e-mail utilizzabile per ricevere le notifiche.
    d. Scegli Create Subscription (Crea sottoscrizione).
6. Riceverai un'e-mail in cui ti verrà chiesto di confermare la sottoscrizione. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

Quando viene rilasciata una nuova versione del servizio EC2Launch v2, inviamo notifiche ai sottoscrittori. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

1. Aprire la console Amazon SNS.
2. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
3. Selezionare la sottoscrizione e quindi scegliere Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni). Quando viene richiesta la conferma, seleziona Elimina.

Impostazioni di EC2Launch v2

Questa sezione contiene informazioni su come configurare le impostazioni per EC2Launch v2.

Gli argomenti includono:

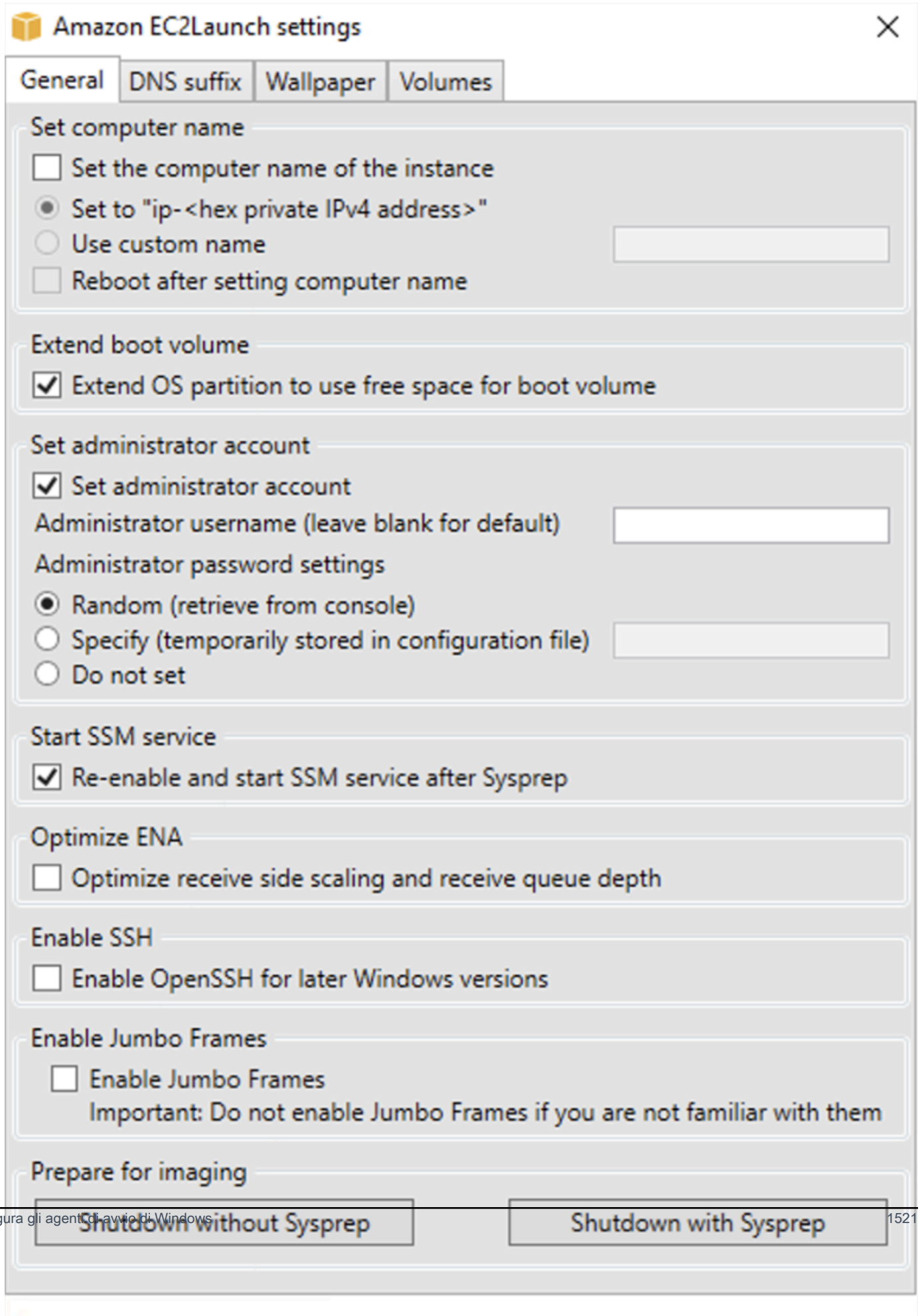
- Modifica delle impostazioni utilizzando la finestra di dialogo delle impostazioni di EC2Launch v2
- Struttura della directory di EC2Launch v2
- Configurare EC2Launch v2 tramite la CLI
- Configurazione dell'attività di EC2Launch v2
- Codici di uscita e riavvii EC2Launch v2
- EC2Launch v2 e Sysprep

Modifica delle impostazioni utilizzando la finestra di dialogo delle impostazioni di EC2Launch v2

La procedura seguente descrive come utilizzare la finestra di dialogo di EC2Launch v2 per abilitare o disabilitare le impostazioni.

> **Note**
>
> Se hai configurato erroneamente delle attività personalizzate nel file agent-config.yml e tenti di aprire la finestra di dialogo delle impostazioni di Amazon EC2Launch, verrà visualizzato un errore. Per un esempio di schema, consulta la sezione Esempio: `agent-config.yml`.

1. Avviare l'istanza Windows e connettersi a essa.
2. Dal menu Start, scegli Tutti i programmi, quindi passa alle impostazioni di EC2Launch.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set computer name
Set the computer name of the instance
Set to "ip-<hex private IPv4 address>"
Use custom name
Reboot after setting computer name
Extend boot volume
Extend OS partition to use free space for boot volume
Set administrator account
Set administrator account
Administrator username (leave blank for default)
Administrator password settings
Random (retrieve from console)
Specify (temporarily stored in configuration file)
Do not set
Start SSM service
Re-enable and start SSM service after Sysprep
Optimize ENA
Optimize receive side scaling and receive queue depth
Enable SSH
Enable OpenSSH for later Windows versions
Enable Jumbo Frames
Enable Jumbo Frames
Important: Do not enable Jumbo Frames if you are not familiar with them
Prepare for imaging
Shutdown without Sysprep
Shutdown with Sysprep

3. Nella scheda Generale della finestra di dialogo Impostazioni EC2Launch puoi abilitare o disabilitare le seguenti impostazioni.

   a. Set Computer Name (Imposta il nome del computer)

      Se questa impostazione viene abilitata (per impostazione predefinita è disabilitata), il nome host attuale viene confrontato con il nome host desiderato ad ogni avvio. Se i nomi host non corrispondono, il nome host viene reimpostato e il sistema si riavvia facoltativamente per acquisire il nuovo nome host. Se non viene specificato un nome host personalizzato, viene generato utilizzando, ad esempio, l'indirizzo IPv4 privato formattato esadecimale `ip-AC1F4E6`. Per evitare che il nome host esistente venga modificato, non abilitare questa impostazione.

   b. Estendi volume di avvio

      Questa impostazione estende in modo dinamico `Disk 0`/`Volume 0` per includere qualsiasi spazio non partizionato. Ciò può essere utile quando l'istanza viene avviata da un volume dispositivo root di dimensioni personalizzate.

   c. Imposta account amministratore

      Se abilitata, puoi impostare gli attributi di nome utente e password per l'account amministratore creato nel computer locale. Se questa caratteristica non è abilitata, non viene creato un account amministratore nel sistema dopo Sysprep. Fornire una password in `adminPassword` solo se `adminPasswordtype` è `Specify`.

      I tipi di password sono definiti come segue:

      i. `Random`

         EC2Launch genera una password e la crittografa utilizzando la chiave dell'utente. Il sistema disattiva questa impostazione dopo l'avvio dell'istanza in modo che questa password rimanga se l'istanza viene riavviata o arrestata e avviata.

      ii. `Specify`

         EC2Launch utilizza la password specificata in `adminPassword`. Se la password non soddisfa i requisiti di sistema, EC2Launch genera invece una password casuale. La password viene memorizzata in `agent-config.yml` come testo non crittografato e viene cancellata dopo che Sysprep ha impostato la password amministratore. EC2Launch crittografa la password utilizzando la chiave dell'utente.

iii. `Do not set`

EC2launch utilizza la password specificata nel file unattend.xml. Se non specifichi una password in unattend.xml, l'account amministratore viene disabilitato.

d. Avvia servizio SSM

Se questa opzione è selezionata, il servizio Systems Manager è abilitato per iniziare dopo Sysprep. EC2Config v2 esegue tutte le attività descritte precedentemente, mentre SSM Agent elabora le richieste per le funzionalità di Systems Manager come Run Command e Gestione stato.

Puoi utilizzare Run Command per aggiornare le istanze esistenti al fine di utilizzare la versione più recente del servizio EC2Launch v2 e di SSM Agent. Per ulteriori informazioni, consulta Aggiornamento di SSM Agent mediante Run Command nella Guida per l'utente di AWS Systems Manager.

e. Ottimizza ENA

Se selezionate, le impostazioni ENA sono configurate per garantire che le impostazioni ENA Receive Side Scaling e Receive Queue Depth siano ottimizzate per. AWS Per ulteriori informazioni, consulta Configurazione di RSS CPU Affinity.

f. Abilita SSH

Questa impostazione abilita OpenSSH per consentire l'amministrazione remota del sistema per le versioni successive di Windows.

g. Abilita frame jumbo

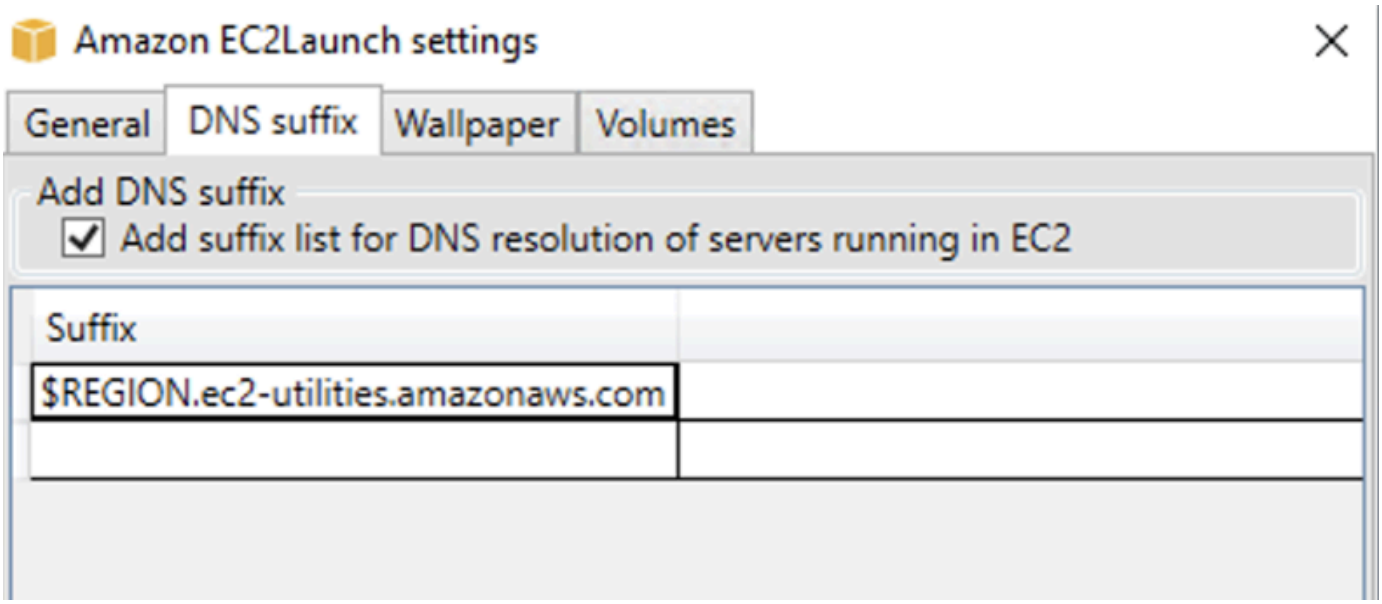
Seleziona questa opzione per abilitare i frame jumbo. I frame jumbo possono avere effetti indesiderati sulle comunicazioni di rete, quindi assicurati di capire in che modo i frame jumbo influiscono sul tuo sistema prima di attivarli. Per ulteriori informazioni sui frame jumbo, consulta Frame jumbo (9001 MTU).

h. Preparazione per l'imaging

Seleziona questa impostazione se vuoi che l'istanza EC2 venga arrestate con o senza Sysprep. Quando vuoi eseguire Sysprep con EC2Launch v2, scegli Arresto con Sysprep.

4. Nella scheda Suffisso DNS puoi selezionare se aggiungere un elenco di suffissi DNS per la risoluzione DNS dei server in esecuzione in EC2, senza specificare il nome di dominio completo.

I suffissi DNS possono contenere le variabili `$REGION` e `$AZ`. All'elenco vengono aggiunti solo i suffissi che non sono già presenti.

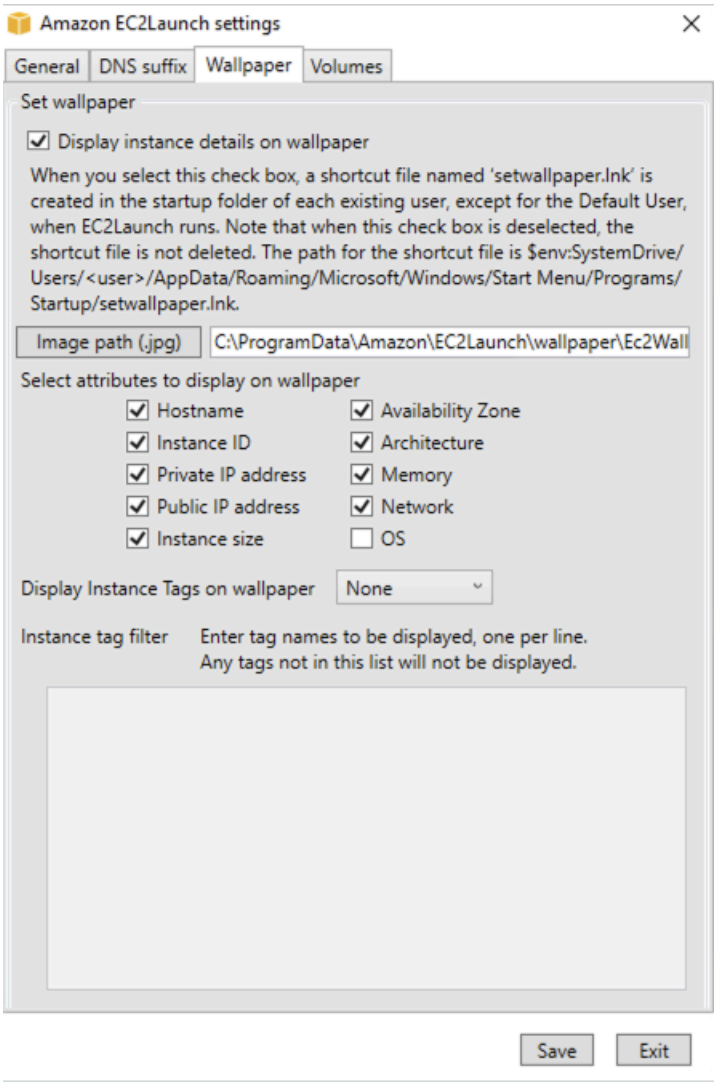


5. Nella scheda Sfondo, puoi configurare lo sfondo dell'istanza con un'immagine di sfondo e specificare i dettagli dell'istanza per lo sfondo da visualizzare. Amazon EC2 genera i dettagli ogni volta che effettui l'accesso.

   È possibile configurare lo sfondo con i seguenti comandi.

   - Mostra i dettagli dell'istanza sullo sfondo: questa casella di controllo attiva o disattiva la visualizzazione dei dettagli dell'istanza sullo sfondo.
   - Percorso dell'immagine (.jpg): specifica il percorso dell'immagine da utilizzare come sfondo.
   - Seleziona gli attributi da visualizzare sullo sfondo: seleziona le caselle di controllo relative ai dettagli dell'istanza che desideri visualizzare sullo sfondo. Deseleziona le caselle di controllo dei dettagli dell'istanza selezionati in precedenza che desideri rimuovere dallo sfondo.
   - Visualizza i tag delle istanze sullo sfondo: seleziona una delle seguenti impostazioni per visualizzare i tag delle istanze sullo sfondo:
     - Nessuno: non visualizzare alcun tag delle istanze sullo sfondo.
     - Mostra tutti: visualizza tutti i tag delle istanze sullo sfondo.
     - Mostra filtrati: visualizza i tag delle istanze specificati sullo sfondo. Quando selezioni questa impostazione, puoi aggiungere i tag delle istanze che desideri visualizzare sullo sfondo nella casella del Filtro dei tag delle istanze.

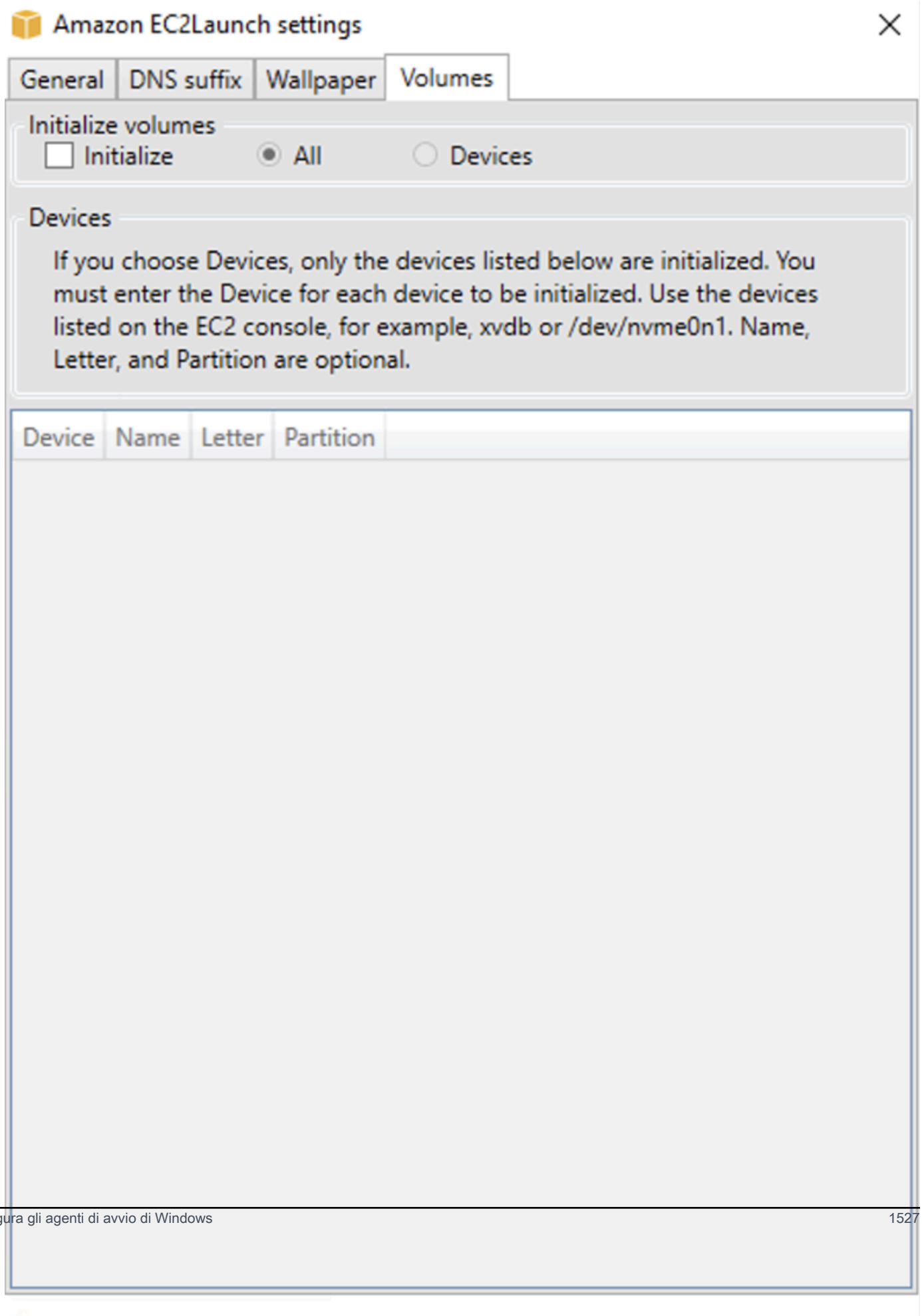
> **Note**
>
> È necessario abilitare i tag nei metadati per mostrare i tag sullo sfondo. Per ulteriori informazioni sui tag e metadati delle istanze, consulta Utilizzo dei tag dell'istanza nei metadati dell'istanza.



6. Nella scheda Volumi seleziona se vuoi inizializzare i volumi collegati all'istanza. L'abilitazione imposta le lettere di unità per eventuali volumi aggiuntivi e li estende per utilizzare lo spazio disponibile. Se si seleziona All (Tutto) vengono inizializzati tutti i volumi di archiviazione. Se selezioni Dispositivi vengono inizializzati solo i dispositivi specificati nell'elenco. Devi specificare immettere il dispositivo per ogni dispositivo da inizializzare. Utilizza i dispositivi elencati sulla console EC2, ad esempio, `xvdb` o `/dev/nvme0n1`. Nell'elenco a discesa vengono visualizzati i

volumi di archiviazione collegati all'istanza. Per immettere un dispositivo non collegato all'istanza, immetterlo nel campo di testo.

Nome, Lettera e Partizione sono campi facoltativi. Se non viene specificato alcun valore per Partition, i volumi di storage superiori a 2 TB vengono inizializzati con il tipo di `gpt` partizione e quelli inferiori a 2 TB vengono inizializzati con il tipo di partizione. `mbr` Se i dispositivi sono configurati e un dispositivo non NTFS contiene una tabella di partizione o i primi 4 KB del disco contengono dati, il disco viene ignorato e l'operazione viene registrata.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Initialize volumes
Initialize
All
Devices
Devices
If you choose Devices, only the devices listed below are initialized. You must enter the Device for each device to be initialized. Use the devices listed on the EC2 console, for example, xvdb or /dev/nvme0n1. Name, Letter, and Partition are optional.
Device
Name
Letter
Partition

Di seguito è riportato un esempio di file YAML di configurazione creato dalle impostazioni immesse nella finestra di dialogo EC2Launch.

```
version: 1.0
config:
  - stage: boot
 tasks:
      - task: extendRootPartition
  - stage: preReady
    tasks:
      - task: activateWindows
        inputs:
          activation:
            type: amazon
      - task: setDnsSuffix
        inputs:
          suffixes:
            - $REGION.ec2-utilities.amazonaws.com
      - task: setAdminAccount
        inputs:
          password:
            type: random
      - task: setWallpaper
        inputs:
          path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
          attributes:
            - hostName
            - instanceId
            - privateIpAddress
            - publicIpAddress
            - instanceSize
            - availabilityZone
            - architecture
            - memory
            - network
  - stage: postReady
    tasks:
      - task: startSsm
```

Struttura della directory di EC2Launch v2

EC2Launch v2 deve essere installato nelle seguenti directory:

- Binari del servizio: `%ProgramFiles%\Amazon\EC2Launch`
- Dati del servizio (impostazioni, file di log e file di stato): `%ProgramData%\Amazon\EC2Launch`

> **Note**
>
> Per impostazione predefinita, Windows nasconde i file e le cartelle in `C:\ProgramData`. Per visualizzare le directory e i file di EC2Launch v2 devi digitare il percorso in Esplora risorse di Windows o modificare le proprietà della cartella per visualizzare i file e le cartelle nascosti.

La directory `%ProgramFiles%\Amazon\EC2Launch` contiene binari e librerie di supporto. Include le seguenti sottodirectory:

- `settings`
  - `EC2LaunchSettingsUI.exe` - interfaccia utente per la modifica del file `agent-config.yml`
  - `YamlDotNet.dll` - DLL per supportare alcune operazioni nell'interfaccia utente
- `tools`
  - `ebsnvme-id.exe` - strumento per esaminare i metadati dei volumi EBS nell'istanza
  - `AWSAcpiSpcrReader.exe` - strumento per determinare la porta COM corretta da utilizzare
  - `EC2LaunchEventMessage.dll` - DLL per supportare il log di eventi di Windows per EC2Launch
- `service`
  - `EC2LaunchService.exe` — Eseguibile del servizio Windows che viene avviato quando l'agente di avvio viene attivato come servizio.
- `EC2Launch.exe` - eseguibile principale EC2launch
- `EC2LaunchAgentAttribution.txt` - attribuzione per il codice utilizzato in EC2 Launch

La directory `%ProgramData%\Amazon\EC2Launch` contiene le sottodirectory seguenti. Tutti i dati prodotti dal servizio, inclusi i log, la configurazione e lo stato, vengono memorizzati in questa directory.

- `config`— Configurazione

  Il file di configurazione del servizio è memorizzato in questa directory come `agent-config.yml`. Questo file può essere aggiornato per modificare, aggiungere o rimuovere le attività predefinite

eseguite dal servizio. L'autorizzazione per creare file in questa directory è limitata all'account di amministratore per evitare l'escalation dei privilegi.

- `log`— Registri delle istanze

  I log relativi al servizio (`agent.log`), alla console (), alle prestazioni (`console.log`), agli errori (`bench.log`) e alla telemetria (`err.log`) `telemetry.log` sono archiviati in questa directory. I file di log vengono aggiunti alle successive esecuzioni del servizio.

- `state`— Dati sullo stato del servizio

  Qui viene memorizzato lo stato utilizzato dal servizio per determinare quali attività devono essere eseguite. Esiste un file `.run-once` che indica se il servizio è già stato eseguito dopo Sysprep (quindi le attività con la frequenza di una volta vengono ignorate all'esecuzione successiva). Questa sottodirectory include `state.json` e `previous-state.json` per tenere traccia dello stato di ogni attività.

- `sysprep`— Sysprep

  Questa directory contiene i file utilizzati per determinare le operazioni eseguite da Sysprep quando crea un'AMI di Windows personalizzata che può essere riutilizzata.

- `wallpaper`— Carta da parati

  Queste immagini di sfondo sono memorizzate in questa cartella.

Configurare EC2Launch v2 tramite la CLI

Puoi utilizzare l'interfaccia a riga di comando (CLI) per configurare le impostazioni di EC2Launch e gestire il servizio. La sezione seguente contiene le descrizioni e le informazioni sull'utilizzo dei comandi CLI che puoi usare per gestire EC2Launch v2.

Comandi

- collect-logs
- get-agent-config
- list-volumes
- reset
- run
- status
- sysprep

- validate
- version
- wallpaper

collect-logs

Raccoglie i file di log per EC2launch, comprime i file e li inserisce in una directory specificata.

Esempio

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Utilizzo

`ec2launch collect-logs [flags]`

Flag

`-h, --help`

aiuto per `collect-logs`

`-o, --output string`

percorso dei file di log di output compressi

get-agent-config

Stampa `agent-config.yml` nel formato specificato (JSON o YAML). Se non viene specificato alcun formato, `agent-config.yml` viene stampato nel formato specificato in precedenza.

Esempio

```
ec2launch get-agent-config -f json
```

Esempio 2

I seguenti PowerShell comandi mostrano come modificare e salvare il `agent-config` file in formato JSON.

```
$config = & "$env:ProgramFiles/Amazon/EC2Launch/EC2Launch.exe" --format json |
 ConvertFrom-Json
$jumboFrame =@"
{
   "task": "enableJumboFrames"
}
"@
$config.config | %{if($_.stage -eq 'postReady'){$_.tasks += (ConvertFrom-Json -
InputObject $jumboFrame)}}
$config | ConvertTo-Json -Depth 6 | Out-File -encoding UTF8
$env:ProgramData/Amazon/EC2Launch/config/agent-config.yml
```

Utilizzo

`ec2launch get-agent-config [flags]`

Flag

`-h`, `--help`

aiuto per `get-agent-config`

`-f`, `--format string`

formato di output del file `agent-config`: `json`, `yaml`

list-volumes

Elenca tutti i volumi di archiviazione collegati all'istanza, inclusi i volumi temporanei ed EBS.

Esempio

```
ec2launch list-volumes
```

Utilizzo

`ec2launch list-volumes`

Flag

`-h`, `--help`

aiuto per `list-volumes`

reset

L'obiettivo principale di questa attività è reimpostare l'agente per la prossima esecuzione. A tale scopo, il comando reset elimina tutti i dati sullo stato dell'agente per EC2Launch v2 dalla directory `EC2Launch` locale (consultare Struttura della directory di EC2Launch v2). Il ripristino elimina facoltativamente i log di servizio e Sysprep.

Il comportamento degli script dipende dalla modalità in cui l'agente esegue gli script: in linea o distaccati.

In linea (impostazione predefinita)

L'agente EC2Launch v2 esegue gli script uno alla volta (`detach: false`). Si tratta dell'impostazione di default.

> **Note**
>
> Quando lo script in linea emette un comando reset o sysprep, viene eseguito immediatamente e reimposta l'agente. L'attività corrente termina, quindi l'agente si spegne senza eseguire altre attività.
> Ad esempio, se l'attività che emette il comando fosse stata seguita da un'attività `startSsm` (inclusa per impostazione predefinita dopo l'esecuzione dei dati utente), l'attività non viene eseguita e il servizio Systems Manager non viene mai avviato.

Distaccato

L'agente EC2Launch v2 esegue gli script contemporaneamente ad altre attività (`detach: true`).

> **Note**
>
> Quando lo script distaccato emette un comando reset o sysprep, tali comandi attendono che l'agente finisca prima di procedere all'esecuzione. Le attività successive all'ExecuteScript continueranno a essere eseguite.

Esempio

```
ec2launch reset -c
```

Utilizzo

`ec2launch reset [flags]`

Flag

`-c`, `--clean`

pulisce i log delle istanze prima di `reset`

`-h`, `--help`

aiuto per `reset`

run

Esecuzioni di EC2Launch v2

Esempio

```
ec2launch run
```

Utilizzo

`ec2launch run [flags]`

Flag

`-h`, `--help`

aiuto per `run`

status

Ottiene lo stato dell'agente EC2Launch v2. Blocca facoltativamente il processo fino al completamento dell'agente. Il codice di uscita del processo determina lo stato dell'agente:

- `0` — l'agente è stato eseguito e ha avuto successo.
- `1` — l'agente è stato eseguito e non è andato a buon fine.
- `2` — l'agente è ancora in esecuzione.
- `3` — l'agente si trova in uno stato sconosciuto. Lo stato dell'agente non è in esecuzione o è stato interrotto.

- 4 — si è verificato un errore nel tentativo di recuperare lo stato dell'agente.
- 5 — l'agente non è in esecuzione e lo stato dell'ultima esecuzione nota è sconosciuto. Ciò può significare che:
  - sia `state.json` che `previous-state.json` sono stati eliminati.
  - `previous-state.json` è danneggiato.

  Questo è lo stato dell'agente dopo l'esecuzione del comando `reset`.

Esempio:

```
ec2launch status -b
```

Utilizzo

`ec2launch status [flags]`

Flag

`-b,--block`

blocca il processo fino al termine dell'esecuzione del'aggente

`-h,--help`

aiuto per `status`

sysprep

L'obiettivo principale di questa attività è reimpostare l'agente per la prossima esecuzione. A tale scopo, il comando sysprep reimposta lo stato dell'agente, aggiorna il file `unattend.xml`, disabilita RDP ed esegue Sysprep.

Il comportamento degli script dipende dalla modalità in cui l'agente esegue gli script: in linea o distaccati.

In linea (impostazione predefinita)

L'agente EC2Launch v2 esegue gli script uno alla volta (`detach: false`). Si tratta dell'impostazione di default.

> **Note**
>
> Quando lo script in linea emette un comando reset o sysprep, viene eseguito immediatamente e reimposta l'agente. L'attività corrente termina, quindi l'agente si spegne senza eseguire altre attività.
> Ad esempio, se l'attività che emette il comando fosse stata seguita da un'attività `startSsm` (inclusa per impostazione predefinita dopo l'esecuzione dei dati utente), l'attività non viene eseguita e il servizio Systems Manager non viene mai avviato.

Distaccato

L'agente EC2Launch v2 esegue gli script contemporaneamente ad altre attività (`detach: true`).

> **Note**
>
> Quando lo script distaccato emette un comando reset o sysprep, tali comandi attendono che l'agente finisca prima di procedere all'esecuzione. Le attività successive all'ExecuteScript continueranno a essere eseguite.

Esempio:

```
ec2launch sysprep
```

Utilizzo

`ec2launch sysprep [flags]`

Flag

`-c,--clean`

pulisce i log delle istanze prima di `sysprep`

`-h,--help`

aiuto per Sysprep

`-s,--shutdown`

arresta l'istanza dopo `sysprep`

validate

Convalida il file `agent-config` `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml`.

Esempio

```
ec2launch validate
```

Utilizzo

`ec2launch validate [flags]`

Flag

-h , `--help`

aiuto per `validate`

version

Ottiene la versione eseguibile.

Esempio

```
ec2launch version
```

Utilizzo

`ec2launch version [flags]`

Flag

`-h`, `--help`

aiuto per `version`

wallpaper

Imposta il nuovo sfondo sul percorso dello sfondo fornito (file .jpg) e visualizza i dettagli dell'istanza selezionata.

Sintassi

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,instanceSize,availabilityZone,a
```

Input

Parametri

--allowed-tags [tag-name-1,] tag-name-n

(Facoltativo) Array JSON codificato in Base64 di nomi di tag delle istanze da visualizzare sullo sfondo. Puoi usare questo tag o `--all-tags`, ma non entrambi.

--attributes ***attributo-stringa-1***, ***attribute-string-n***

(Facoltativo) Un elenco separato da virgole di stringhe di attributi `wallpaper` per applicare le impostazioni allo sfondo.

[--path | -p] ***path-string***

(Obbligatorio) Specifica il percorso del file dell'immagine di sfondo `wallpaper`.

Flag

--all-tags

(Facoltativo) Visualizza tutti i tag delle istanze sullo sfondo. Puoi usare questo tag o `--allowed-tags`, ma non entrambi.

[--help | -h]

Visualizza l'assistenza per il comando wallpaper.

Configurazione dell'attività di EC2Launch v2

In questa sezione sono riportati lo schema, le attività, i dettagli e gli esempi di configurazione per `agent-config.yml` e i dati utente.

Attività ed esempi

- Schema: agent-config.yml
- Schema: dati utente
- Definizioni di processi

Schema: **`agent-config.yml`**

La struttura del file `agent-config.yml` è riportata di seguito. Nota che un'attività non può essere ripetuta nella stessa fase. Per le proprietà delle attività, consulta le descrizioni delle attività che seguono.

Struttura del documento: agent-config.yml

JSON

```
{
 "version": "1.0",
 "config": [
  {
   "stage": "string",
   "tasks": [
    {
     "task": "string",
     "inputs": {
      ...
     }
    },
    ...
   ]
  },
  ...
 ]
}
```

YAML

```
version: 1.0
config:
- stage: string
  tasks:
```

```
  - task: string
 inputs:
   ...
  ...
...
```

Esempio: **`agent-config.yml`**

Nell'esempio seguente vengono illustrate le impostazioni per il file di configurazione `agent-config.yml`.

```
version: 1.0
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
      - memory
      - network
```

```
- stage: postReady
  tasks:
  - task: startSsm
```

Schema: dati utente

Gli esempi JSON e YAML seguenti mostrano la struttura del documento per i dati utente. Amazon EC2 analizza ogni attività rinominata nell'array `tasks` specificato nel documento. Ogni attività ha il proprio set di proprietà e requisiti. Per informazioni dettagliate, consulta la Definizioni di processi.

> **Note**
>
> Un'attività deve essere visualizzata una sola volta nell'array di attività per i dati utente.

Struttura del documento: dati utente

JSON

```
{
 "version": "1.1",
 "tasks": [
  {
   "task": "string",
   "inputs": {
    ...
   },
  },
  ...
 ]
}
```

YAML

```
version: 1.1
tasks:
- task: string
  inputs:
    ...
...
```

Esempio: dati utente

Per ulteriori informazioni su questi dati utente, vedere In che modo Amazon EC2 gestisce i dati utente per le istanze Windows.

Il seguente esempio di documento YAML mostra uno PowerShell script che EC2Launch v2 esegue come dati utente per creare un file.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

È possibile utilizzare un formato XML per i dati utente compatibile con le versioni precedenti dell'agente di avvio. EC2Launch v2 esegue lo script come attività `executeScript` nella fase `UserData`. Per conformarsi al comportamento di EC2Launch v1 ed EC2Config, lo script dei dati utente viene eseguito come processo attaccato/in linea per impostazione predefinita.

Puoi aggiungere tag opzionali per personalizzare la modalità di esecuzione dello script. Ad esempio, per eseguire lo script dei dati utente al riavvio dell'istanza e una volta all'avvio dell'istanza, puoi utilizzare il seguente tag:

`<persist>true</persist>`

Esempio:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

È possibile specificare uno o più PowerShell argomenti con il tag. `<powershellArguments>` Se non viene passato alcun argomento, EC2Launch v2 aggiunge il seguente argomento per impostazione predefinita:. `-ExecutionPolicy Unrestricted`

Esempio:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Per eseguire uno script di dati utente XML come processo distaccato, aggiungi il seguente tag ai dati utente.

```
<detach>true</detach>
```

Esempio:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

> **Note**
>
> Il tag di distacco non è supportato nei precedenti agenti di avvio.

Log delle modifiche: dati utente

La tabella seguente elenca le modifiche apportate ai dati utente e le confronta con la versione dell'agente EC2Launch v2 applicabile.

Versione dei dati utente	Informazioni	Introdotta in
1.1	• Le attività relative ai dati utente vengono eseguite prima della fase `PostReady` nel file di configurazione dell'agente. • Esegue i dati utente prima di avviare l'agente Systems Manager (stesso comportamento di EC2Launch v1 ed EC2Config).*	EC2Launch v2 versione 2.0.1245

Versione dei dati utente	Informazioni	Introdotta in
1	• Diventerà obsoleta. • Le attività relative ai dati utente vengono eseguite dopo la fase `PostReady` nel file di configurazione dell'agente. Non è compatibile con EC2Launch v1 e versioni precedenti. • Influenzata da una race condition tra l'avvio dell'agente Systems Manager e le attività relative ai dati utente.	EC2Launch v2 versione 2.0.0

* Se utilizzato con il file `agent-config.yml` predefinito.

Definizioni di processi

Ogni attività ha il proprio set di proprietà e requisiti. Per informazioni dettagliate, consulta le singole attività da includere nel documento.

Attività

- activateWindows
- enableJumboFrames
- enableOpenSsh
- executeProgram
- executeScript
- extendRootPartition
- initializeVolume
- optimizeEna
- setAdminAccount
- setDnsSuffix
- setHostName
- setWallpaper
- startSsm
- sysprep

- writeFile

activateWindows

Attiva Windows su un set di server. AWS KMS L'attivazione viene ignorata se l'istanza viene rilevata come uso di licenze proprie (BYOL).

Frequency - una volta

AllowedStages — `[PreReady]`

Inputs —

`activation`: (mappa)

`type`: (stringa) tipo di attivazione da utilizzare, impostato su `amazon`

Esempio

```
task: activateWindows
inputs:
  activation:
    type: amazon
```

enableJumboFrames

Abilita i frame jumbo che aumentano l'unità di trasmissione massima (MTU) della scheda di rete. Per ulteriori informazioni, consulta Frame jumbo (9001 MTU).

Frequency - sempre

AllowedStages — `[PostReady, UserData]`

Inputs - nessuno

Esempio

```
task: enableJumboFrames
```

enableOpenSsh

Abilita Windows OpenSSH e aggiunge la chiave pubblica per l'istanza alla cartella delle chiavi autorizzate.

Frequency - una volta

AllowedStages — `[PreReady, UserData]`

Inputs - nessuno

Esempio

Nell'esempio seguente viene illustrato come abilitare OpenSSH su un'istanza e come aggiungere la chiave pubblica per l'istanza alla cartella delle chiavi autorizzate. Questa configurazione funziona solo su istanze che eseguono Windows Server 2019 e versioni successive.

```
task: enableOpenSsh
```

executeProgram

Esegue uno script con argomenti opzionali e una frequenza specificata.

Fasi: è possibile eseguire l'attività `executeProgram` durante le fasi`PreReady`, `PostReady` e `UserData`.

Frequenza: configurabile, vedere Input.

Input

Questa sezione contiene uno o più programmi per l'executeProgramoperazione da eseguire (input). Ogni input può includere le seguenti impostazioni configurabili:

frequenza (stringa)

(Obbligatorio) Specifica esattamente uno dei seguenti valori:

- `once`
- `always`

path (stringa)

(Obbligatorio) Il percorso del file per l'eseguibile da eseguire.

argomenti (elenco di stringhe)

(Facoltativo) Un elenco di argomenti separati da virgole da fornire al programma come input.

runAs (stringa)

(Obbligatorio) Deve essere impostato su `localSystem`

Output

Tutte le attività scrivono le voci del file di registro nel file `agent.log`. L'output aggiuntivo dell'attività `executeProgram` viene archiviato separatamente in una cartella denominata dinamicamente, come segue:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.tmp`*

Il percorso esatto dei file di output è incluso nel file `agent.log`, ad esempio:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

File di output per l'attività **`executeProgram`**

`ExecuteProgramInputs.tmp`

Contiene il percorso dell'eseguibile e tutti i parametri di input che l'attività `executeProgram` passa durante l'esecuzione.

`Output.tmp`

Contiene l'output di runtime del programma eseguito dall'attività `executeProgram`.

`Err.tmp`

Contiene messaggi di errore di runtime provenienti dal programma eseguito dall'attività `executeProgram`.

Esempi

Gli esempi seguenti mostrano come eseguire un file eseguibile da una directory locale su un'istanza con l'attività `executeProgram`.

Esempio 1: Configurazione dell'eseguibile con un argomento

Questo esempio mostra un'attività `executeProgram` che esegue un eseguibile di installazione in modalità silenziosa.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\Users\Administrator\Desktop\setup.exe
  arguments: ['-quiet']
```

Esempio 2: eseguibile VLC con due argomenti

Questo esempio mostra un'attività `executeProgram` che esegue un file eseguibile VLC con due argomenti passati come parametri di input.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\vlc-3.0.11-win64.exe
  arguments: ['/L=1033','/S']
  runAs: localSystem
```

executeScript

Esegue uno script con argomenti opzionali e una frequenza specificata. Il comportamento degli script dipende dalla modalità in cui l'agente esegue gli script: in linea o distaccati.

In linea (impostazione predefinita)

L'agente EC2Launch v2 esegue gli script uno alla volta (`detach: false`). Si tratta dell'impostazione di default.

> **Note**
>
> Quando lo script in linea emette un comando reset o sysprep, viene eseguito immediatamente e reimposta l'agente. L'attività corrente termina, quindi l'agente si spegne senza eseguire altre attività.
> Ad esempio, se l'attività che emette il comando fosse stata seguita da un'attività `startSsm` (inclusa per impostazione predefinita dopo l'esecuzione dei dati utente), l'attività non viene eseguita e il servizio Systems Manager non viene mai avviato.

Distaccato

L'agente EC2Launch v2 esegue gli script contemporaneamente ad altre attività (`detach: true`).

> **Note**
>
> Quando lo script distaccato emette un comando reset o sysprep, tali comandi attendono che l'agente finisca prima di procedere all'esecuzione. Le attività successive all'ExecuteScript continueranno a essere eseguite.

Fasi: è possibile eseguire l'attività `executeScript` durante le fasi`PreReady`, `PostReady` e `UserData`.

Frequenza: configurabile, vedere Input.

Input

Questa sezione contiene uno o più script per l'executeScriptoperazione da eseguire (input). Ogni input può includere le seguenti impostazioni configurabili:

frequenza (stringa)

(Obbligatorio) Specifica esattamente uno dei seguenti valori:

- `once`
- `always`

Tipo: stringa

(Obbligatorio) Specifica esattamente uno dei seguenti valori:

- `batch`
- `powershell`

argomenti (elenco di stringhe)

(Facoltativo) Un elenco di argomenti di stringa da passare all'interprete dei comandi. Questo parametro non è supportato per le attività eseguite su `type: batch`. Se non viene passato alcun argomento, EC2Launch v2 aggiunge il seguente argomento per impostazione predefinita:. `-ExecutionPolicy Unrestricted`

contenuto (stringa)

(Obbligatorio) Contenuto dello script.

runAs (stringa)

(Obbligatorio) Specificare esattamente uno dei seguenti valori:

- `admin`
- `localSystem`

staccare (booleano)

(Facoltativo) L'agente EC2Launch v2 esegue di default gli script uno alla volta (`detach: false`). Per eseguire lo script in concomitanza con altre attività, impostate il valore su`true` (`detach: true`).

> **Note**
>
> I codici di uscita dello script (tra cui `3010`) non hanno effetto quando `detach` è impostato su `true`.

Output

Tutte le attività scrivono le voci del file di registro nel file `agent.log`. L'output aggiuntivo dello script eseguito dall'attività `executeScript` viene archiviato separatamente in una cartella denominata dinamicamente, come segue:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.ext`*

Il percorso esatto dei file di output è incluso nel file `agent.log`, ad esempio:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

File di output per l'attività **`executeScript`**

`UserScript.`*`ext`*

Contiene lo script eseguito dall'attività `executeScript`. L'estensione del file dipende dal tipo di script specificato nel parametro `type` per l'attività `executeScript`, come segue:

- Se il tipo è`batch`, l'estensione del file è `.bat`.
- Se il tipo è`powershell`, l'estensione del file è `.ps1`.

`Output.tmp`

Contiene l'output di runtime dello script eseguito dall'attività `executeScript`.

`Err.tmp`

Contiene messaggi di errore di runtime provenienti dallo script eseguito dall'attività `executeScript`.

Esempi

Gli esempi seguenti mostrano come eseguire uno script in linea con l'attività `executeScript`.

Esempio 1: file di testo di output Ciao

Questo esempio mostra un'`executeScript`attività che esegue PowerShell uno script per creare un file di testo «Hello world» sull'unità. `C:`

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: admin
  content: |-
    New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
    Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Esempio 2: eseguire due script

Questo esempio mostra che l'attività `executeScript` può eseguire più di uno script e il tipo di script non deve necessariamente corrispondere.

Il primo script (`type: powershell`) scrive un riepilogo dei processi attualmente in esecuzione sull'istanza in un file di testo che si trova sull'unità `C:`.

Il secondo script (`batch`) scrive le informazioni di sistema nel file `Output.tmp`.

```
task: executeScript
```

```
inputs:
- frequency: always
  type: powershell
  content: |
    Get-Process | Out-File -FilePath C:\Process.txt
  runAs: localSystem
- frequency: always
  type: batch
  content: |
    systeminfo
```

Esempio 3: configurazione di sistema idempotente con riavvii

Questo esempio mostra un'attività `executeScript` che esegue uno script idempotente per eseguire la seguente configurazione di sistema con un riavvio tra ogni fase:

- Impostare il nome del computer.
- Aggiungere il computer al dominio
- Abilitare Telnet.

Lo script garantisce che ogni operazione venga eseguita una sola volta. Ciò impedisce un ciclo di riavvio e rende lo script idempotente.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: localSystem
  content: |-
    $name = $env:ComputerName
     if ($name -ne $desiredName) {
       Rename-Computer -NewName $desiredName
       exit 3010
     }
     $domain = Get-ADDomain
     if ($domain -ne $desiredDomain)
     {
       Add-Computer -DomainName $desiredDomain
       exit 3010
     }
    $telnet = Get-WindowsFeature -Name Telnet-Client
    if (-not $telnet.Installed)
```

```
    {
      Install-WindowsFeature -Name "Telnet-Client"
      exit 3010
    }
```

extendRootPartition

Estende il volume root per utilizzare tutto lo spazio disponibile sul disco.

Frequency - una volta

AllowedStages — `[Boot]`

Inputs - nessuno

Esempio

```
task: extendRootPartition
```

initializeVolume

Inizializza i volumi vuoti che sono collegati all'istanza in modo che vengano attivati e partizionati. L'agente di avvio salta l'inizializzazione se rileva che il volume non è vuoto. Un volume è considerato vuoto se i primi 4 KiB del volume sono vuoti o se non dispone di un layout di unità riconoscibile da Windows.

Il parametro di input `letter` viene sempre applicato quando viene eseguita questa attività, indipendentemente dal fatto che l'unità sia già inizializzata.

L'attività `initializeVolume` effettua le seguenti operazioni.

- Imposta gli attributi del disco `offline` e `readonly` su false.
- Creare una partizione. Se non è specificato alcun tipo di partizione nel parametro di input `partition`, si applicano le seguenti impostazioni predefinite:
  - Se la dimensione del disco è inferiore a 2 TB, imposta il tipo di partizione su `mbr`.
  - Se la dimensione del disco è pari o superiore a 2 TB, imposta il tipo di partizione su `.gpt`.
- Formatta il volume come NTFS.
- Imposta l'etichetta del volume, come indicato di seguito:

- Utilizza il valore del parametro di input `name`, se specificato.
- Se il volume è temporaneo e non è stato specificato alcun nome, imposta l'etichetta del volume su `Temporary Storage Z`.

- Se il volume è temporaneo (SSD o HDD, non Amazon EBS), crea un file `Important.txt` nel root del volume con il seguente contenuto:

```
This is an 'Instance Store' disk and is provided at no additional charge.

*This disk offers increased performance since it is local to the host
*The number of Instance Store disks available to an instance vary by instance type
*DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
 PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY

For more information, please refer to: Instance store Amazon EC2.
```

- Imposta la lettera dell'unità sul valore specificato nel parametro di input `letter`.

Fasi: è possibile eseguire l'attività `initializeVolume` durante le fasi `PostReady` e `UserData`.

Frequenza: sempre.

Input

È possibile configurare i parametri di runtime come segue:

dispositivi (elenco di mappe)

(Condizionale) Configurazione per ogni dispositivo inizializzato dall'agente di avvio. Questo parametro è obbligatorio quando il parametro di input `initialize` è impostato su `devices`.

- dispositivo (stringa, obbligatorio): identifica il dispositivo durante la creazione dell'istanza. Ad esempio, `xvdb`, `xvdf` o `\dev\nvme0n1`.
- lettera (stringa, facoltativo): un carattere. La lettera dell'unità da assegnare.
- nome (stringa, facoltativo): il nome del volume da assegnare.
- partizione (stringa, facoltativo): specifica uno dei seguenti valori per il tipo di partizione da creare o consenti all'agente di avvio di utilizzare le impostazioni predefinite in base alla dimensione del volume:
  - mbr
  - gpt

inizializza (stringa)

(Obbligatorio) Specificare esattamente uno dei seguenti valori:

- `all`
- `devices`

Esempi

Gli esempi seguenti mostrano esempi di configurazioni di input per l'attività `initializeVolume`.

Esempio 1: inizializzazione di due volumi su un'istanza

Questo esempio mostra un'attività `initializeVolume` che inizializza due volumi secondari su un'istanza. Il dispositivo denominato `DataVolume2` nell'esempio è effimero.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
  - device: xvdb
    name: DataVolume1
    letter: D
    partition: mbr
  - device: /dev/nvme0n1
    name: DataVolume2
    letter: E
    partition: gpt
```

Esempio 2: inizializzazione dei volumi EBS collegati a un'istanza

Questo esempio mostra un'attività `initializeVolume` che inizializza tutti i volumi EBS vuoti collegati all'istanza.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Ottimizza le impostazioni ENA in base al tipo di istanza corrente; l'istanza potrebbe essere riavviata.

Frequency - sempre

AllowedStages — `[PostReady, UserData]`

Inputs - nessuno

Esempio

```
task: optimizeEna
```

setAdminAccount

Imposta gli attributi per l'account amministratore predefinito creato nel computer locale.

Frequency - una volta

AllowedStages — `[PreReady]`

Inputs —

`name`: (stringa) nome dell'account amministratore

`password`: (mappa)

`type`: (stringa) strategia per impostare la password come `static`, `random` o `doNothing`

`data`: (stringa) archivia i dati se il campo `type` è statico

Esempio

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
    type: random
```

setDnsSuffix

Aggiunge suffissi DNS all'elenco dei suffissi di ricerca. All'elenco vengono aggiunti solo i suffissi che non esistono già. Per ulteriori informazioni su come gli agenti di avvio impostano i suffissi DNS, consulta. Configura il suffisso DNS per gli agenti di avvio di Windows

Frequency - sempre

AllowedStages — `[PreReady]`

Inputs —

`suffixes`: (elenco di stringhe) elenco di uno o più suffissi DNS validi, le variabili di sostituzione valide sono `$REGION` e `$AZ`

Esempio

```
task: setDnsSuffix
inputs:
  suffixes:
  - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Imposta il nome host del computer su una stringa personalizzata o, se `hostName` non è specificato, sull'indirizzo IPv4 privato.

Frequency - sempre

AllowedStages — `[PostReady, UserData]`

Inputs —

`hostName`: (stringa) nome host facoltativo, che deve essere formattato come segue.

- Deve essere uguale o inferiore a 15 caratteri
- Deve contenere solo caratteri alfanumerici (a-z, A-Z, 0-9) e trattino (-).
- Non deve essere costituito interamente da caratteri numerici.

`reboot`: (booleano) indica se è consentito un riavvio quando viene modificato il nome host

Esempio

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Crea il file di scorciatoia `setwallpaper.lnk` nella cartella di startup di ciascun utente esistente, eccetto `Default User`. Questo file di scorciatoia viene eseguito quando l'utente accede per la prima volta dopo l'avvio dell'istanza. Imposta l'istanza con uno sfondo personalizzato che visualizzi gli attributi dell'istanza.

Il percorso del file di scorciatoia è:

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/
Startup/setwallpaper.lnk
```

> **Note**
>
> La rimozione dell'attività `setWallpaper` non elimina questo file di scorciatoia. Per ulteriori informazioni, consulta Il processo `setWallpaper` non è abilitato ma lo sfondo viene ripristinato al riavvio.

Fasi: puoi configurare lo sfondo durante le fasi `PreReady` e `UserData`.

Frequenza: `always`

Configurazione dello sfondo

È possibile configurare lo sfondo con le seguenti impostazioni.

Input

Parametri di input che fornisci e attributi che puoi impostare per configurare lo sfondo:

attributi (elenco di stringhe)

(Facoltativo) Puoi aggiungere uno o più dei seguenti attributi allo sfondo:

- `architecture`
- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`

- `memory`
- `network`
- `privateIpAddress`
- `publicIpAddress`

instanceTags

(Facoltativo) Per questa impostazione puoi utilizzare esattamente una delle seguenti opzioni.

- AllTags(stringa) — Aggiungi tutti i tag di istanza allo sfondo.

```
instanceTags: AllTags
```

- instanceTags (elenco di stringhe): specifica un elenco di nomi di tag delle istanze da aggiungere allo sfondo. Per esempio:

```
instanceTags:
  - Tag 1
  - Tag 2
```

path (stringa)

(Obbligatorio) Il percorso del nome del file immagine in formato.jpg locale da utilizzare per l'immagine di sfondo.

Esempio

L'esempio seguente mostra gli input di configurazione dello sfondo che impostano il percorso del file per l'immagine di sfondo dello sfondo, insieme ai tag delle istanze denominati `Tag 1` e `Tag 2` e agli attributi che includono il nome dell'host, l'ID dell'istanza e gli indirizzi IP privati e pubblici dell'istanza.

```
task: setWallpaper
inputs:
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
  - hostName
  - instanceId
  - privateIpAddress
  - publicIpAddress
  instanceTags:
  - Tag 1
```

```
  - Tag 2
```

> **Note**
>
> È necessario abilitare i tag nei metadati per mostrare i tag sullo sfondo. Per ulteriori informazioni sui tag e metadati delle istanze, consulta Utilizzo dei tag dell'istanza nei metadati dell'istanza.

startSsm

Avvia il servizio Systems Manager (SSM) dopo Sysprep.

Frequency - sempre

AllowedStages — `[PostReady, UserData]`

Inputs - nessuno

Esempio

```
task: startSsm
```

sysprep

Reimposta lo stato del servizio, aggiorna `unattend.xml`, disabilita RDP ed esegue Sysprep. Questa attività viene eseguita solo dopo che tutte le altre attività sono state completate.

Frequency - una volta

AllowedStages — `[UserData]`

Inputs —

`clean`: (booleano) pulisce i log delle istanze prima di eseguire Sysprep

`shutdown`: (booleano) chiude l'istanza dopo l'esecuzione di Sysprep

Esempio

```
task: sysprep
```

```
inputs:
  clean: true
  shutdown: true
```

writeFile

Scrive un file in una destinazione.

Frequency - vedi Inputs

AllowedStages — `[PostReady, UserData]`

Inputs —

`frequency`: (stringa) `once` o `always`

`destination`: (stringa) percorso in cui scrivere il contenuto

`content`: (stringa) testo da scrivere nella destinazione

Esempio

```
task: writeFile
inputs:
- frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Codici di uscita e riavvii EC2Launch v2

È possibile utilizzare EC2Launch v2 per definire come i codici di uscita vengono gestiti dagli script. Per impostazione predefinita, il codice di uscita dell'ultimo comando eseguito in uno script viene segnalato come codice di uscita per l'intero script. Ad esempio, se uno script include tre comandi e il primo comando ha esito negativo ma quelli seguenti hanno esito positivo, lo stato di esecuzione viene segnalato come `success` perché il comando finale ha avuto esito positivo.

Se si desidera che uno script riavvii un'istanza, è necessario specificare `exit 3010` nello script, anche quando il riavvio è l'ultimo passo dello script. `exit 3010` indica a EC2Launch v2 di riavviare l'istanza e richiamare nuovamente lo script fino a quando non restituisce un codice di uscita che non è `3010` o fino a quando non viene raggiunto il numero massimo di riavvii. EC2Launch v2 consente

un massimo di 5 riavvii per attività. Se si tenta di riavviare un'istanza da uno script utilizzando un meccanismo diverso, ad esempio `Restart-Computer`, lo stato di esecuzione dello script non sarà coerente. Ad esempio, potrebbe rimanere bloccato in un ciclo di riavvio o non eseguire il riavvio.

Se utilizzi un formato di dati utente XML compatibile con agenti meno recenti, i dati utente potrebbero essere eseguiti più volte di quanto desideri. Per ulteriori informazioni, consulta Il servizio esegue i dati utente più di una volta nella sezione di risoluzione dei problemi.

EC2Launch v2 e Sysprep

Il servizio EC2Launch v2 esegue Sysprep, uno strumento Microsoft che ti permette di creare un'AMI di Windows personalizzata che può essere riutilizzata. Quando EC2Launch v2 chiama Sysprep, utilizza i file contenuti in `%ProgramData%\Amazon\EC2Launch` per determinare quali operazioni eseguire. Puoi modificare questi file indirettamente utilizzando la finestra di dialogo Impostazioni EC2Launch direttamente utilizzando un editor YAML o un editor di testo. Tuttavia esistono alcune impostazioni avanzate che non sono disponibili nella finestra di dialogoImpostazioni EC2Launch, quindi è necessario modificarle direttamente.

Se crei un'AMI da un'istanza dopo l'aggiornamento delle sue impostazioni, le nuove impostazioni vengono applicate a ogni istanza lanciata dalla nuova AMI. Per informazioni sulla creazione di un'AMI, consulta Crea un'AMI supportata da Amazon EBS.

Risoluzione dei problemi di EC2Launch v2

In questa sezione vengono illustrati scenari di risoluzione dei problemi comuni di EC2Launch v2 e informazioni sulla visualizzazione dei log di eventi di Windows, nonché l'output e i messaggi dei log della console.

Argomenti sulla risoluzione dei problemi

- Scenari per la risoluzione dei problemi comuni
- Log di eventi di Windows
- Output del log della console EC2Launch v2

Scenari per la risoluzione dei problemi comuni

In questa sezione vengono illustrati gli scenari di risoluzione dei problemi comuni e le fasi per la risoluzione dei problemi.

Scenari

Il servizio non riesce a impostare lo sfondo

Risoluzione

1. Controlla che `%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs \Startup\setwallpaper.lnk` esista.
2. Controlla `%ProgramData%\Amazon\EC2Launch\log\agent.log` per vedere se si sono verificati errori.

Il servizio non riesce a eseguire i dati utente

Possibile causa: il servizio potrebbe aver restituito l'esito negativo prima dell'esecuzione dei dati utente.

Risoluzione

1. Controlla `%ProgramData%\Amazon\EC2Launch\state\previous-state.json`.
2. Vedi se `boot`, `network`, `preReady` e `postReadyLocalData` sono stati tutti contrassegnati come completati.
3. Se una delle fasi non è riuscita, controlla `%ProgramData%\Amazon\EC2Launch\log \agent.log` per vedere se si sono verificati errori specifici.

Il servizio esegue un'attività una sola volta

Risoluzione

1. Controlla la frequenza dell'attività.
2. Se il servizio è già stato eseguito dopo Sysprep e la frequenza dell'attività è impostata su `once`, l'attività non verrà eseguita nuovamente.
3. Imposta la frequenza dell'attività su `always` se vuoi che venga eseguita ogni volta che viene eseguito EC2Launch v2.

Il servizio non riesce a eseguire un'attività

Risoluzione

1. Controlla le ultime voci in `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Se non si sono verificati errori, prova a eseguire manualmente il servizio da `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` per verificare se le attività hanno esito positivo.

Il servizio esegue i dati utente più di una volta

Risoluzione

I dati utente vengono gestiti in modo diverso tra EC2Launch v1 e EC2Launch v2. EC2Launch v1 esegue i dati utente come attività pianificata sull'istanza quando `persist` è impostato su `true`. Se `persist` è impostato su `false`, l'attività non viene pianificata anche quando esce con un riavvio o viene interrotta durante l'esecuzione.

EC2Launch v2 esegue i dati utente come attività agente e tiene traccia del relativo stato di esecuzione. Se i dati utente emettono un riavvio del computer o sono stati interrotti durante l'esecuzione, lo stato di esecuzione persiste come `pending` e i dati utente verranno eseguiti nuovamente al successivo avvio dell'istanza. Se si desidera impedire l'esecuzione dello script dei dati utente più di una volta, rendere lo script idempotente.

Lo script idempotente di esempio seguente imposta il nome del computer e si unisce a un dominio.

```
<powershell>
  $name = $env:computername
  if ($name -ne $desiredName) {
```

```
 Rename-Computer -NewName $desiredName
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
 Add-Computer -DomainName $desiredDomain
  }
  $telnet = Get-WindowsFeature -Name Telnet-Client
  if (-not $telnet.Installed)
  {
 Install-WindowsFeature -Name "Telnet-Client"
  }
</powershell>
<persist>false</persist>
```

Le attività pianificate da EC2Launch v1 non vengono eseguite dopo la migrazione a EC2Launch v2

Risoluzione

Lo strumento di migrazione non rileva alcuna attività pianificata collegata agli script EC2Launch v1, pertanto non imposta automaticamente tali attività in EC2Launch v2. Per configurare queste attività, modificare il file `agent-config.yml` o utilizzare la finestra di dialogo Impostazioni di EC2Launch v2. Ad esempio, se un'istanza dispone di un'attività pianificata che esegue `InitializeDisks.ps1`, dopo avere eseguito lo strumento di migrazione, è necessario specificare i volumi che si desidera inizializzare nella finestra di dialogo delle impostazioni di EC2Launch v2. Vedere il passaggio 6 della procedura per Modifica delle impostazioni utilizzando la finestra di dialogo delle impostazioni di EC2Launch v2.

Il servizio inizializza un volume EBS che non è vuoto

Risoluzione

Prima di inizializzare un volume, EC2Launch v2 tenta di rilevare se è vuoto. Se un volume non è vuoto, ignora l'inizializzazione. I volumi rilevati come non vuoti non vengono inizializzati. Un volume è considerato vuoto se i primi 4 KiB del volume sono vuoti o se non dispone di un layout di unità riconoscibile da Windows. Un volume che è stato inizializzato e formattato su un sistema Linux non dispone di un layout di unità riconoscibile da Windows, ad esempio MBR o GPT. Pertanto, sarà considerato vuoto e inizializzato. Se si desidera conservare questi dati, non fare affidamento sul rilevamento di unità EC2Launch v2 vuote. Specificare invece i volumi che si desidera inizializzare nella finestra di dialogo delle impostazioni di EC2Launch v2 (vedere il passaggio 6) o in `agent-config.yml`.

Il processo **`setWallpaper`** non è abilitato ma lo sfondo viene ripristinato al riavvio

Il processo `setWallpaper` crea il file di scorciatoia `setwallpaper.lnk` nella cartella di startup di ciascun utente esistente, eccetto `Default User`. Questo file di scorciatoia viene eseguito quando l'utente accede per la prima volta dopo l'avvio dell'istanza. Imposta l'istanza con uno sfondo personalizzato che visualizzi gli attributi dell'istanza. La rimozione del processo `setWallpaper` non elimina questo file di scorciatoia. È necessario eliminare questo file manualmente o con uno script.

Il percorso del file di scorciatoia è:

`$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk`

Risoluzione

Eliminare questo file manualmente o con uno script.

PowerShell Script di esempio per eliminare un file di collegamento

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
 $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup"
 if (Test-Path $startupPath)
 {
  $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
  if (Test-Path $wallpaperSetupPath)
  {
   Remove-Item $wallpaperSetupPath -Force -Confirm:$false
  }
 }
}
```

Servizio bloccato nello stato di esecuzione

Descrizione

EC2Launch v2 è bloccato con i messaggi di log (`agent.log`) simili ai seguenti:

```
2022-02-24 08:08:58 Info:
 ********************************************************************************
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
```

```
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Possibile causa

SAC è abilitato e utilizza la porta seriale. Per ulteriori informazioni, consulta Utilizzo di SAC per risolvere i problemi relativi all'istanza di Windows.

Risoluzione

Per risolvere il problema, prova a eseguire i seguenti passaggi:

- Disabilita il servizio che utilizza la porta seriale.
- Se desideri che il servizio continui a utilizzare la porta seriale, scrivi degli script personalizzati per eseguire le attività dell'agente di avvio e richiamarle come attività pianificate.

Un **`agent-config.yml`** non valido impedisce l'apertura della finestra di dialogo delle impostazioni di EC2Launch v2

Descrizione

Le impostazioni di EC2Launch v2 tentano di analizzare il file `agent-config.yml` prima dell'apertura della finestra di dialogo. Se il file di configurazione YAML non segue lo schema supportato, nella finestra di dialogo viene visualizzato il seguente errore:

```
Unable to parse configuration file agent-config.yml. Review configuration file. Exiting application.
```

Risoluzione

1. Verifica che il file di configurazione segua lo schema supportato.
2. Se vuoi iniziare da zero, copia il file di configurazione predefinito in `agent-config.yml`. Puoi utilizzare il plugin di `agent-config.yml` di esempio fornito nella sezione Task Configuration (Configurazione attività).
3. Puoi anche ricominciare da capo eliminando `agent-config.yml`. Le impostazioni di EC2Launch v2 generano un file di configurazione vuoto.

`task:executeScript should be unique and only invoked once`

Descrizione

Un'attività non può essere ripetuta nella stessa fase.

Risoluzione

Alcune attività devono essere inserite come array, ad esempio executeScript e executeProgram. Per un esempio di come scrivere lo script in forma di array, consulta l'argomento executeScript.

Log di eventi di Windows

EC2Launch v2 pubblica i log di eventi di Windows per gli eventi importanti, ad esempio per l'avvio del servizio, se Windows è pronto o sull'esito positivo o il fallimento delle attività. Gli identificatori di evento identificano in modo univoco un particolare evento. Ogni evento contiene informazioni su fasi, attività e livelli e una descrizione. Puoi impostare i trigger per eventi specifici utilizzando l'identificatore di evento.

Gli ID evento forniscono informazioni su un evento e identificano in modo univoco alcuni eventi. La cifra meno significativa di un ID evento indica la gravità di un evento.

Evento	Cifra meno significativa
`Success`	`. . .0`
`Informational`	`. . .1`
`Warning`	`. . .2`
`Error`	`. . .3`

Gli eventi relativi al servizio generati all'avvio o all'arresto del servizio includono un identificatore di evento a una cifra.

Evento	Identificatore a una cifra
`Success`	`0`
`Informational`	`1`

Evento	Identificatore a una cifra
`Warning`	2
`Error`	3

I messaggi di evento per gli eventi `EC2LaunchService.exe` iniziano con `Service:`. I messaggi di evento per gli eventi `EC2Launch.exe` non iniziano con `Service:`.

Gli ID evento a quattro cifre includono informazioni su stadio, attività e gravità di un evento.

Argomenti

- Formato ID evento
- Esempi di ID evento
- Schema dei log di eventi di Windows

Formato ID evento

Nella tabella seguente viene illustrato il formato di un identificatore di evento EC2Launch v2.

3	2 1	0
S	T	L

Le lettere e i numeri nella tabella rappresentano il tipo di evento e le definizioni seguenti.

Tipo di evento	Definizione
S (fase)	0 - Messaggio a livello di servizio 1 - Avvio 2 - Rete 3 - PreReady

Tipo di evento	Definizione
	5 - Windows è pronto 6 - PostReady 7 - Dati utente
T (attività)	Le attività rappresentate dai due valori corrispondenti sono diverse per ogni fase. Per visualizzare l'elenco completo degli eventi, consulta lo Schema dei log di eventi di Windows.
L (livello di evento)	0 - Operazione completata 1 - Messaggio informativo 2 - Avvertenza 3 - Errore

Esempi di ID evento

Di seguito sono riportati gli ID evento di esempio.

- `5000` - Windows è pronto per l'uso
- `3010`- L'attività di attivazione di Windows in PreReady fase è stata completata con successo
- `6013`- Si è verificato un errore nell'operazione Imposta sfondo nella fase PostReady Local Data

Schema dei log di eventi di Windows

MessageId/ID evento	Messaggio di evento
`. . .0`	`Success`
`. . .1`	`Informational`

MessageId/ID evento	Messaggio di evento
. . .2	Warning
. . .3	Error
x	EC2Launch service-level logs
0	EC2Launch service exited successfully
1	EC2Launch service informational logs
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition
2000	Network
2010	Network - add_routes
3000	PreReady

MessageId/ID evento	Messaggio di evento
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program

MessageId/ID evento	Messaggio di evento
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

Output del log della console EC2Launch v2

Questa sezione contiene un esempio di output del log della console per EC2Launch v2 ed elenca tutti i messaggi di errore del log della console EC2Launch v2 che consentono di risolvere i problemi. Per ulteriori informazioni sull'output della console di istanza e su come accedervi, consultathe section called “Output della console delle istanze”.

Output

- Output del log della console EC2Launch v2
- Messaggi di log della console EC2Launch v2

Output del log della console EC2Launch v2

Di seguito è riportato un esempio di output del log della console per EC2Launch v2.

```
2023/11/30 20:18:53Z: Windows sysprep configuration complete.
2023/11/30 20:18:57Z: Message: Waiting for access to metadata...
2023/11/30 20:18:57Z: Message: Meta-data is now available.
2023/11/30 20:18:57Z: AMI Origin Version: 2023.11.15
2023/11/30 20:18:57Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2023/11/30 20:18:58Z: OS: Microsoft Windows NT 10.0.20348
2023/11/30 20:18:58Z: OsVersion: 10.0
2023/11/30 20:18:58Z: OsProductName: Windows Server 2022 Datacenter
2023/11/30 20:18:58Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2023/11/30 20:18:58Z: OsCurrentBuild: 20348
2023/11/30 20:18:58Z: OsReleaseId: 2009
2023/11/30 20:18:58Z: Language: en-US
2023/11/30 20:18:58Z: TimeZone: UTC
2023/11/30 20:18:58Z: Offset: UTC +0000
2023/11/30 20:18:58Z: Launch: EC2 Launch v2.0.1643
2023/11/30 20:18:58Z: AMI-ID: ami-1234567890abcdef1
2023/11/30 20:18:58Z: Instance-ID: i-1234567890abcdef0
2023/11/30 20:18:58Z: Instance Type: c5.large
2023/11/30 20:19:00Z: Driver: AWS NVMe Driver v1.5.0.33
2023/11/30 20:19:00Z: SubComponent: AWS NVMe Driver v1.5.0.33;
 EnableSCSIPersistentReservations: 0
2023/11/30 20:19:00Z: Driver: AWS PV Driver Package v8.4.3
2023/11/30 20:19:01Z: Driver: Amazon Elastic Network Adapter v2.6.0.0
2023/11/30 20:19:01Z: RDPCERTIFICATE-SUBJECTNAME: EC2AMAZ-SO1T009
2023/11/30 20:19:01Z: RDPCERTIFICATE-THUMBPRINT:
 1234567890ABCDEF1234567890ABCDEF1234567890
2023/11/30 20:19:09Z: SSM: Amazon SSM Agent v3.2.1705.0
2023/11/30 20:19:13Z: Username: Administrator
2023/11/30 20:19:13Z: Password: <Password>
1234567890abcdef1EXAMPLEPASSWORD
</Password>
2023/11/30 20:19:14Z: User data format: no_user_data
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
2023/11/30 20:19:14Z: Message: Windows is Ready to use
```

Messaggi di log della console EC2Launch v2

Di seguito è riportato un elenco di tutti i messaggi di log della console EC2Launch v2.

```
Message: Error EC2Launch service is stopping. {error message}
```

```
 Error setting up EC2Launch agent folders
 See instance logs for detail
 Error stopping service
 Error initializing service
Message: Windows sysprep configuration complete
Message: Invalid administrator username: {invalid username}
Message: Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
Microsoft-Hyper-V is installed.
Unable to get service status for vmms
Microsoft-Hyper-V is {status}
SSM: Amazon SSM Agent {version}
AWS VSS Version: {version}
Message: Windows sysprep configuration complete
Message: Windows is being configured. SysprepState is {state}
Windows is still being configured. SysprepState is {state}
Message: Windows is Ready to use
Message: Waiting for meta-data accessibility...
Message: Meta-data is now available.
Message: Still waiting for meta-data accessibility...
Message: Failed to find primary network interface...retrying...
```

```
User data format: {format}
```

Cronologie delle versioni EC2Launch v2

Cronologie delle versioni

- Cronologia delle versioni di EC2Launch v2
- Cronologia delle versioni dello strumento di migrazione di EC2Launch v2

Cronologia delle versioni di EC2Launch v2

La tabella seguente descrive le versioni rilasciate di EC2Launch v2.

Versione	Dettagli	Data di rilascio
2.0,1924	• Aggiornata l'interfaccia utente delle impostazioni di EC2Launch. • Aggiornato il comando CLI dello sfondo. • Aggiornato il programma di installazione di EC2Launch.	10 giugno 2024
2,0,1914	• Aggiungi percorsi con indirizzi gateway non specificati (`0.0.0.0`per IPv4 o per IPv6). `::` • Aggiungi sempre sia i percorsi IPv4 che IPv6. • È stato risolto un problema per cui il nome `Administrator` utente veniva aggiunto al `agent-config.yml` file quando non era specificato. • Autorizzazioni EC2Launch v2 modificate.	5 giugno 2024
2,0,1881	• Aggiunta un'opzione di password crittografata all'operazione. `setAdminAccount` •	8 maggio 2024

Versione	Dettagli	Data di rilascio
	Aggiunto il comando CLI per crittografare la password statica in agent-config.yml. • È stato risolto un problema per cui i dati utente XML non PowerShell aggiungevano argomenti quando venivano eseguiti con le autorizzazioni di amministratore. Per ulteriori dettagli, consulta In che modo Amazon EC2 gestisce i dati utente per le istanze Windows. • PowerShell Argomenti modificati per gli script delle `executeScript` attività e dei dati utente quando vengono eseguiti con `LocalSystem` autorizzazioni. Quando gli argomenti sono vuoti, l'agente utilizza il seguente valore predefinito:. `-ExecutionPolicy Unrestricted` • Impedita la stampa di versioni duplicate dei driver nel registro della console.	
2,0,1815	• Modificata la gestione degli errori per evitare problemi critici di configurazione prima di sysprep. • È stato risolto un problema per cui le attività relative agli sfondi e ai nomi host potevano utilizzare un indirizzo IP errato nelle istanze con più indirizzi IP assegnati all'interfaccia di rete principale. • Le attività relative allo sfondo e al nome host sono state modificate per ottenere prima l'IP privato da IMDS, quindi restituirle a WMI se IMDS è disabilitato. • È stato risolto un problema relativo all'`initializeVolume` attività che impediva l'inizializzazione `sc1` dei volumi a causa di un errore temporaneo.	6 marzo 2024

Versione	Dettagli	Data di rilascio
2.0. 1739	• È stato risolto un problema che impediva l'acquisizione dei codici di uscita da `executeScript` attività eseguite come utente amministratore di Windows.	17 gennaio 2024
2,0,1702	• Autorizzazioni `Telemetry.log` limitate a `read-execute` solo per gli utenti standard. • Il servizio Windows EC2Launch è stato configurato per il riavvio in caso di errore di avvio. • Gli errori `add-routes` sono stati resi risolvibili registrando l'output `route.exe stderr`. • È stato risolto un problema che si verificava quando le metriche del percorso non rientravano nell'intervallo [1, 9999]. • È stato aggiunto il supporto per gli sfondi per numerosi nuovi tipi di istanze. • È stato risolto un problema causato dagli script di dati utente che venivano eseguiti come utente amministratore di Windows e inviavano l'output a `stderr`.	4 gennaio 2024

Versione	Dettagli	Data di rilascio
2,0,1643	• Lo strumento `ebsnvme-id.exe` è stato aggiornato alla versione 1.1.0.7. • È stato risolto un problema relativo alle impostazioni di dimensionamento lato ricezione (RSS) e della profondità della coda di ricezione sui tipi di istanze metal che iniziano con "metal-*", come metal-48x1. • È stato rimosso l'evento di telemetria che riporta i comandi userdata XML che bloccano l'agente. • È stata aggiornata l'attività `setDnsSuffix` per limitare la devoluzione del nome di dominio in base alla voce del registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • È stata aggiunta un'attività pubblica e una CLI che aggiunge percorsi di rete. • Nota: questa è l'ultima versione che supporta ufficialmente Windows Server 2012. • Nota: questa è l'ultima versione che supporta ufficialmente i sistemi operativi a 32 bit.	4 ottobre 2023
2.0,1580	• È stato modificato il modo in cui l'agente di avvio gestisce gli errori quando si modificano le autorizzazioni dei file di log. • È stato aggiunto un timeout per la connessione alla porta seriale. Il timeout consente all'agente di avvio di continuare a funzionare se la porta seriale è in uso.	5 settembre 2023

Versione	Dettagli	Data di rilascio

2.0,1521	• È stato dichiarato obsoleto il flag –`block` dei comandi reset e sysprep `EC2Launch.exe` .
	• È stato aggiornato diventando `EC2Launch.exe` per rilevare e gestire i comandi reset e sysprep utilizzati nelle attività in linea `executeScript` . Questi comandi causano l'interruzione dell'esecuzione dell'agente dopo l'esecuzione dell'operazione `executeScript` .
	• Gli script UserData XML sono stati aggiornati per l'esecuzione in linea per impostazione predefinita.
	• Consente di abilitare l'esecuzione degli script UserData XML in modo indipendente con il nuovo tag `detach`. Per ulteriori dettagli, consulta Script di dati utente.
	• Sono state apportate le seguenti modifiche al log dell'agente.
	  • Sono stati aggiornati i messaggi di log dell'agente.
	  • Sono stati rimossi i contenuti e output `executeScript` dal log dell'agente.
	  • Sono stati rimossi gli argomenti e output `executeProgram` dal log dell'agente.
	• Sono state apportate le seguenti modifiche al log della console.
	  • È stato aggiunto il valore `EnableSCSIPersistentReservations` al log della console.
		3 luglio 2023

Versione	Dettagli	Data di rilascio
2.0,1303	• Sono state aggiunte ulteriori righe di gestione degli errori e di log durante l'aggiunta di percorsi di rete. • Consentiti `executeScript` e `executeProgram` compiti in fase. PreReady • Attività `executeProgram` aggiornata per generare file di output simili all'output dell'attività executeScript. Per ulteriori informazioni, consulta executeProgram. • È stata aggiunta la telemetria per monitorare l'utilizzo dei comandi dell'agente di blocco nei dati utente XML.	3 maggio 2023
2.0.1245	• È stata migliorata la visibilità degli arresti anomali grazie alla registrazione in chiaro degli stack delle chiamate di arresto anomalo. • È stato aggiunto il EventLog servizio come dipendenza di avvio per correggere un arresto anomalo quando il servizio Amazon EC2Launch si avvia più velocemente del servizio. EventLog • I dati utente XML sono stati eseguiti prima della PostReady fase iniziale dal file di configurazione dell'agente (come EC2Launch v1 ed EC2Config). • È stata aggiunta la versione 1.1 dei dati utente YAML per far sì che i dati utente vengano eseguiti prima della PostReady fase dal file di configurazione dell'agente (la versione 1.0 dei dati utente YAML viene eseguita dopo la fase dal file di configurazione dell'agente). PostReady	8 marzo 2023

Versione	Dettagli	Data di rilascio
2.0.1173	• Aggiunge una funzionalità opzionale per visualizzare i tag delle istanze sullo sfondo. Per ulteriori informazioni, consulta setWallpaper . • Aggiunge la gestione degli errori quando il gruppo di sicurezza per Elastic Graphics non è impostato correttamente. • Corregge un timeout quando l'Instance Metadata Service non è abilitato.	6 febbraio 2023
2,0,1121	• Risolve un problema a causa del quale un errore 404 viene visualizzato sullo sfondo quando non viene assegnato alcun indirizzo IPv4 pubblico. • Risolve un problema a causa del quale il file system del volume è formattato come `RAW` invece di `NTFS` quando la lettera di unità del dispositivo è impostata su `D`. • Risolve un problema a causa del quale i volumi SSD NVMe vengono erroneamente identificati come volumi EBS. • Risolve un errore durante l'attivazione di Windows quando IMDS è disabilitato.	4 gennaio 2023

Versione	Dettagli	Data di rilascio
2,0,1082	• Risolve un problema per cui il campo `setWallpaper : privateIpAddress` è vuoto quando IMDS è disabilitato. • Risolve un problema relativo all'impostazione del nome host sull'indirizzo IPv4 privato quando IMDS è disabilitato. • Risolve un problema relativo all'inizializzazione dei volumi su Windows Server 2012. • Risolve un problema relativo all'impostazione dei frame jumbo. • Risolve un errore che si verifica quando non viene specificata alcuna chiave SSH all'avvio dell'istanza. • Risolve un errore in Windows Server 2012 quando Windows non dispone di una chiave di registro ". ReleaseId	7 dicembre 2022
2.0.1011	• Corregge la logica per la ricerca dell'adattatore di rete quando PnPDeviceID è vuoto.	11 novembre 2022
2.0,1009	• Utilizza le informazioni sui segmenti PCI per selezionare la porta della console.	8 novembre 2022

Versione	Dettagli	Data di rilascio
2.0,982	• Aggiunge la logica dei tentativi per ottenere informazioni su RDP. • Corregge gli errori durante l'inizializzazione dei volumi sulle istanze `d2.8xlarge` . • Risolve il problema per cui è possibile selezionare un adattatore di rete non corretto dopo un riavvio. • Rimuove il messaggio di errore di falso allarme quando ACPI SPCR non è disponibile.	31 ottobre 2022
2.0,863	• Aggiorna la logica di attesa IMDS per effettuare solo richieste IMDSv2. • Aggiunge la logica per l'assegnazione di una lettera di unità a volumi già inizializzati ma non montati. • Stampa un messaggio di errore più specifico quando il tipo di coppia di chiavi non è supportato. • Risolve bug del codice di riavvio 3010. • Aggiunge il controllo per dati utente con codifica base64 non validi.	6 luglio 2022
2.0,6988	• Corregge gli errori di battitura nell'output del log durante l'esecuzione di script.	30 gennaio 2022

Versione	Dettagli	Data di rilascio
2.0,6674	• La telemetria carica il controllo abilitato/disabilitato per la privacy. • Corregge i bug `index out of bounds`. • Rimuove le scorciatoie da sfondo durante `sysprep`.	15 novembre 2021
2.0,651	• Aggiunge la logica per disinstallare gli agenti legacy durante l'installazione di EC2Launch v2. • Risolve il problema `list-volume` della CLI quando il volume root non è elencato come volume 0.	7 ottobre 2021
2,0,592	• Corregge i bug per segnalare correttamente lo stato della fase. • Rimuove falsi messaggi di errore di allarme quando i file di log sono chiusi. • Aggiunge dati di telemetria.	31 agosto 2021
2.0,548	• Aggiunge zeri iniziali per il nome host IP esadecimale. • Risolve le autorizzazioni dei file per l'incarico `enableOpenSsh` . • Risolve il crash del comando sysprep.	4 agosto 2021

Versione	Dettagli	Data di rilascio
2.0,470	• Corregge il bug in fase di rete in attesa di DHCP per assegnare un IP all'istanza. • Corregge il bug con `setDnsSuffix` quando `SearchList` la chiave di registro non esiste. • Corregge il bug nella logica di devoluzione DNS in `setDnsSuffix` . • Aggiunge route di rete dopo i riavvii intermedi. • Consente a `initializeVolume` di ripetere la lettera dei volumi esistenti. • Rimuove informazioni aggiuntive dal sottocomando versione.	20 luglio 2021
2.0.285	• Aggiunge l'opzione per eseguire script utente in un processo scollegato. • I dati utente legacy (dati utente XML) vengono ora eseguiti in un processo scollegato, che è simile a quello dell'agente di avvio precedente. • Aggiunge il flag CLI ai comandi `sysprep` e `reset`, consenten done il blocco fino all'arresto del servizio. • Limita le autorizzazioni della cartella di configurazione.	8 marzo 2021

Versione	Dettagli	Data di rilascio
2.0.207	• Aggiunge il campo facoltativo `hostName` all'attività `setHostName` . • Corregge il bug di riavvio. Riavviare le attività `executeScript` e `executeProgram` verrà contrassegnato come in esecuzione. • Aggiunge altri codici di ritorno al comando di stato. • Aggiunge il servizio bootstrap per risolvere il problema di startup durante l'esecuzione sul tipo di istanza `t2.nano`. • Risolve i problemi legati alla modalità di installazione pulita per rimuovere i file non monitorati dal programma di installazione.	2 febbraio 2021
2.0.160	• Corregge il comando `validate` per rilevare il nome dello stadio non valido. • Aggiunge il comando `w32tm resync` nell'attività `addroutes` . • Risolve il problema con la modifica dell'ordine di ricerca del suffisso DNS. • Aggiunge condizioni di controllo per segnalare meglio i dati utente non validi.	4 dicembre 2020
2.0.153	Aggiunge la funzionalità Sysprep in. UserData	3 novembre 2020

Versione	Dettagli	Data di rilascio
2.0.146	• Risolve il problema relativo alle AMI non RootExtend in lingua inglese. • Concede ai gruppi di utenti l'autorizzazione di scrittura per i file del log • Crea partizione riservata MS per i volumi GPT. • Aggiunge il comando list-volumes e il menu a discesa del volume nelle impostazioni di Amazon EC2Launch. • Aggiunge get-agent-config il comando per la stampa del file agent-config.yml in formato yaml o json. • Cancella la password statica se non viene rilevata alcuna chiave pubblica.	6 ottobre 2020
2.0.124	• Aggiunge l'opzione per visualizzare la versione del sistema operativo sullo sfondo. • Inizializza volumi EBS crittografati. • Aggiunge route per i VPC senza un nome DNS locale.	10 settembre 2020
2.0.104	• Crea l'elenco di ricerca dei suffissi DNS se non esiste. • Ignora l'ibernazione se non richiesta.	12 agosto 2020
2.0.0	Versione iniziale.	30 giugno 2020

Cronologia delle versioni dello strumento di migrazione di EC2Launch v2

La tabella seguente descrive le versioni rilasciate dello strumento di migrazione EC2Launch v2.

Versione	Dettagli	Data di rilascio
1.0.396	• Aggiorna lo strumento di migrazione con l'ultima versione dell'agente EC2Launch v2:2.0.1924.	11 giugno 2024
1.0.394	• Aggiorna lo strumento di migrazione con l'ultima versione dell'agente EC2Launch v2:2.0.1914.	6 giugno 2024
1.0.384	• Aggiorna lo strumento di migrazione con l'ultima versione dell'agente EC2Launch v2:2.0.1881.	8 maggio 2024
1,0358	• Aggiorna lo strumento di migrazione con l'ultima versione dell'agente EC2Launch v2:2.0.1815.	8 marzo 2024
1.0.345	• Aggiorna lo strumento di migrazione con l'ultima versione dell'agente EC2Launch v2:2.0.1739.	18 gennaio 2024
1.0.342	• Aggiorna lo strumento di migrazione con l'ultima versione dell'agente EC2Launch v2:2.0.1702.	5 gennaio 2024
1.0.331	• Aggiornamento dello strumento di migrazione con la versione più recente dell'agente EC2Launch v2: 2.0.1643 • Risolvi un errore che si verifica durante l'esecuzione di `.Install.ps1 -DryRun` . • Risolvi un problema per cui la configurazione della password non viene impostata correttamente su `random` durante la migrazione da EC2Config. •	3 novembre 2023

Versione	Dettagli	Data di rilascio
	Risolvi un errore che si verifica se `setWallpaper` è impostato su `False` durante la migrazione da EC2Launch.	
1,0303	Aggiorna lo strumento di migrazione con la versione più recente dell'agente EC2Launch v2: 2.0.1580.	14 settembre 2023
1,0,286	Aggiorna lo strumento di migrazione con la versione più recente dell'agente EC2Launch v2: 2.0.1521.	14 luglio 2023
1,0272	Aggiorna lo strumento di migrazione con la versione più recente dell'agente EC2Launch v2: 2.0.1303.	3 maggio 2023
1,0,262	Aggiorna lo strumento di migrazione con la versione più recente dell'agente EC2Launch v2: 2.0.1245.	9 marzo 2023
1,0241	Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.1011.	7 dicembre 2022
1,0,218	• Convalida il valore della regione recuperato dai metadati dell'istanza. • Risolve il bug di errore di migrazione nei pacchetti di lingua. • Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.863.	3 settembre 2022
1,0,162	• Sposta la logica per rimuovere gli agenti legacy su EC2Launch v2 MSI. • Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.698.	18 marzo 2022
1,0,136	Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.651.	13 ottobre 2021
1,0,130	Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.548.	5 agosto 2021

Versione	Dettagli	Data di rilascio
1,0113	Utilizza IMDSv2 al posto di IMDSv1.	4 giugno 2021
1.0.101	Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.285.	12 marzo 2021
1.0.86	Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.207.	3 febbraio 2021
1.0.76	Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.160.	4 dicembre 2020
1.0.69	Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.153.	5 novembre 2020
1.0.65	Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.146.	9 ottobre 2020
1.0.60	Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.124.	10 settembre 2020
1.0.54	• Installa EC2Launch v2 se non sono installati agenti. • Incrementa il numero di versione dell'agente EC2Launch v2 a 2.0.104. • Disaccoppia SSM Agent.	12 agosto 2020
1.0.50	Rimuove NuGet la dipendenza.	10 agosto 2020
1.0.0	Versione iniziale.	30 giugno 2020

Configurazione dell'istanza Windows tramite EC2Launch

EC2Launch è un set di PowerShell script Windows che ha sostituito il servizio EC2Config sulle AMI Windows Server 2016 e 2019. Molte di queste AMI sono ancora disponibili. EC2Launch v2 è il più recente agente di avvio per tutte le versioni supportate di Windows Server che sostituisce sia EC2config che EC2Launch. Per ulteriori informazioni, consulta Configurare un'istanza Windows tramite EC2Launch v2.

> **Note**
>
> Per utilizzare EC2Launch con IMDSv2, la versione deve essere 1.3.2002730 o versione successiva.

Indice

Attività EC2Launch

EC2Launch esegue le seguenti operazioni per impostazione predefinita durante l'avvio dell'istanza iniziale:

- Imposta un nuovo sfondo che esegue il rendering delle informazioni riguardanti l'istanza.
- Imposta il nome del computer sull'indirizzo IPv4 privato dell'istanza.
- Invia le informazioni di istanza alla console Amazon EC2.
- Invia l'impronta del certificato RDP alla console EC2.
- Imposta una password casuale per l'account dell'amministratore.
- Aggiunge i suffissi DNS.

- Estende in modo dinamico la partizione del sistema operativo per includere qualsiasi spazio non partizionato.
- Esegue i dati utente (se specificato). Per ulteriori informazioni sulla specifica dei dati utente, consulta Utilizzo dei dati utente dell'istanza.
- Imposta percorsi statici persistenti per raggiungere il servizio di metadati e i server. AWS KMS

> **Important**
>
> Se da questa istanza viene creata un'AMI personalizzata, i routing vengono acquisiti come parte della configurazione del sistema operativo e qualsiasi nuova istanza avviata dall'AMI avrà gli stessi routing, indipendentemente dal posizionamento della sottorete. Per aggiornare i routing, vedi Aggiornamento di routing KMS/metadati per il Server 2016 o versione successiva quando si lancia un'AMI personalizzata.

Le seguenti attività contribuiscono a mantenere la retrocompatibilità con il servizio EC2Config. È anche possibile configurare EC2Launch in modo che esegua queste attività durante li startup:

- Inizializzare i volumi EBS secondari.
- Inviare i log di eventi di Windows ai log della console EC2.
- Inviare il messaggio Windows is ready to use (Windows è pronto per l'utilizzo) alla console EC2.

Per ulteriori informazioni su Windows Server 2019, consulta Confronta le funzionalità delle versioni di Windows Server su Microsoft.com.

Telemetria

La telemetria è un'informazione aggiuntiva che aiuta AWS a comprendere meglio i requisiti, diagnosticare i problemi e fornire funzionalità per migliorare l'esperienza con i servizi. AWS

EC2Launch versione `1.3.2003498` e successive raccolgono dati di telemetria, ad esempio parametri ed errori di utilizzo. Questi dati vengono raccolti dall'istanza Amazon EC2 su cui viene eseguito EC2Launch. Sono incluse tutte le AMI Windows di proprietà di. AWS

EC2Launch raccoglie i seguenti tipi di telemetria:

- Informazioni di utilizzo: comandi dell'agente, metodo di installazione e frequenza di esecuzione pianificata.

- Errori e informazioni diagnostiche: installazione dell'agente ed esecuzione dei codici di errore.

Esempi di dati raccolti:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

La telemetria è abilitata per impostazione predefinita. Puoi disabilitare la raccolta dati di telemetria in qualsiasi momento. Se la telemetria è abilitata, EC2Launch invia i dati di telemetria senza ulteriori notifiche ai clienti.

Viene registrata la scelta di abilitare o disabilitare la telemetria.

È possibile attivare o disattivare la raccolta di telemetria. La propria selezione per attivare o disattivare la telemetria viene raccolta per garantire l'adesione alla propria opzione di telemetria.

Visibilità della telemetria

Quando la telemetria è abilitata, viene visualizzata nell'output della console Amazon EC2 come segue:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Disabilitare la telemetria su un'istanza

Per disattivare la telemetria impostando una variabile di ambiente di sistema, esegui il comando seguente come amministratore:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Per disabilitare la telemetria durante l'installazione, eseguire `install.ps1` come riportato:

```
. .\install.ps1 -EnableTelemetry:$false
```

Installare la versione più recente di EC2Launch

Per scaricare e installare la versione più recente di EC2Launch sulle istanze, attenersi alla procedura seguente.

Scaricare e installare la versione più recente di EC2Launch

1. Se EC2Launch è già stato installato e configurato su un'istanza, eseguire un backup del file di configurazione di EC2Launch. Il processo di installazione non conserva le modifiche apportate a questo file. Per impostazione predefinita, il file si trova nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Scaricare EC2-Windows-Launch.zip in una directory dell'istanza.
3. Scaricare install.ps1 nella stessa directory in cui è stato scaricato `EC2-Windows-Launch.zip`.
4. Esegui `install.ps1`
5. Se è stato eseguito il backup del file di configurazione di EC2Launch, copiarlo nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Per scaricare e installare l'ultima versione di EC2Launch utilizzando PowerShell

Se EC2Launch è già stato installato e configurato su un'istanza, eseguire un backup del file di configurazione di EC2Launch. Il processo di installazione non conserva le modifiche apportate a questo file. Per impostazione predefinita, il file si trova nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Per installare l'ultima versione di EC2Launch utilizzando PowerShell, esegui i seguenti comandi da una finestra PowerShell

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-
Launch.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -
Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -
Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

> **Note**
>
> Se ricevi un errore durante il download del file e utilizzi Windows Server 2016, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il seguente comando e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Verifica l'installazione controllando `C:\ProgramData\Amazon\EC2-Windows\Launch`.

Verifica la versione EC2Launch

Usa il seguente PowerShell comando di Windows per verificare la versione installata di EC2Launch.

```
PS C:\> Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1" | Select Version
```

Struttura della directory di EC2Launch

Per impostazione predefinita, EC2Launch viene installato sulle AMI di Windows Server 2016 o versione successiva nella directory radice `C:\ProgramData\Amazon\EC2-Windows\Launch`.

> **Note**
>
> Per impostazione predefinita, Windows nasconde i file e le cartelle in `C:\ProgramData`. Per visualizzare le directory e i file di EC2Launch, è necessario digitare il percorso in Windows Explorer risorse o modificare le proprietà della cartella per visualizzare i file e le cartelle nascosti.

La directory `Launch` contiene le sottodirectory seguenti.

- `Scripts`— Contiene PowerShell gli script che compongono EC2Launch.
- `Module` - Contiene il modulo per la creazione di script relativi a Amazon EC2.
- `Config` - Contiene file di configurazione dello script che si possono personalizzare.
- `Sysprep` - Contiene risorse Sysprep.
- `Settings` - Contiene un'applicazione per l'interfaccia utente grafica di Sysprep.

- `Library`: contiene librerie condivise per gli agenti di avvio di EC2.
- `Logs` - Contiene i file di log generati dagli script.

Configurazione di EC2Launch

Dopo aver inizializzato l'istanza la prima volta, è possibile configurare EC2Launch in modo che venga eseguito nuovamente ed eseguire diverse attività di avvio.

Attività

- Configurare le attività di inizializzazione
- Pianificare EC2Launch in modo che venga eseguito a ogni avvio
- Inizializzazione delle unità e mappatura delle lettere di unità
- Inviare i log di eventi di Windows alla console EC2.
- Inviare il messaggio Windows is ready (Windows è pronto) dopo un avvio riuscito.

Configurare le attività di inizializzazione

Specificare le impostazioni nel file `LaunchConfig.json` per attivare o disattivare le seguenti attività di inizializzazione:

- Imposta il nome del computer sull'indirizzo IPv4 privato dell'istanza.
- Impostare il monitor in modo che rimanga sempre acceso.
- Impostare un nuovo sfondo.
- Aggiungere l'elenco di suffissi DNS.

> **Note**
>
> Ciò aggiunge una ricerca dei suffissi DNS per il seguente dominio e configura altri suffissi standard. Per ulteriori informazioni su come gli agenti di avvio impostano i suffissi DNS, consulta. Configura il suffisso DNS per gli agenti di avvio di Windows
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- Estendere la dimensione del volume di avvio.
- Impostare la password amministratore

Configurare le impostazioni di inizializzazione

1. Nell'istanza da configurare, aprire il seguente file in un editor di testo: `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json`.
2. Aggiornare le seguenti impostazioni come necessario e salvare le modifiche. Fornire una password in `adminPassword` solo se `adminPasswordtype` è `Specify`.

```
{
 "setComputerName": false,
 "setMonitorAlwaysOn": true,
 "setWallpaper": true,
 "addDnsSuffixList": true,
 "extendBootVolumeSize": true,
 "handleUserData": true,
 "adminPasswordType": "Random | Specify | DoNothing",
 "adminPassword": "password that adheres to your security policy (optional)"
}
```

   I tipi di password sono definiti come segue:

   `Random`

   EC2Launch genera una password e la crittografa utilizzando la chiave dell'utente. Il sistema disattiva questa impostazione dopo l'avvio dell'istanza in modo che questa password rimanga se l'istanza viene riavviata o arrestata e avviata.

   `Specify`

   EC2Launch utilizza la password specificata in `adminPassword`. Se la password non soddisfa i requisiti di sistema, EC2Launch genera invece una password casuale. La password viene memorizzata in `LaunchConfig.json` come testo non crittografato e viene cancellata dopo che Sysprep ha impostato la password amministratore. EC2Launch crittografa la password utilizzando la chiave dell'utente.

   `DoNothing`

   EC2Launch utilizza la password specificata nel file `unattend.xml`. Se non si indica una password in `unattend.xml`, l'account amministratore viene disattivato.
3. In Windows PowerShell, esegui il comando seguente per pianificare l'esecuzione dello script come operazione pianificata di Windows. Lo script viene eseguito una volta durante l'avvio successivo, poi disabilita la nuova esecuzione di queste attività.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Pianificare EC2Launch in modo che venga eseguito a ogni avvio

Puoi pianificare EC2Launch in modo che venga eseguito a ogni avvio invece che solo all'avvio iniziale.

Per abilitare EC2Launch in modo che venga eseguito a ogni avvio:

1. Apri Windows PowerShell ed esegui il seguente comando:

   ```
   PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
   SchedulePerBoot
   ```

2. Oppure, eseguire l'eseguibile con il seguente comando:

   ```
   PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
   ```

   Quindi selezionare `Run EC2Launch on every boot`. Puoi specificare che la tua istanza EC2 `Shutdown without Sysprep` o `Shutdown with Sysprep`.

> **Note**
>
> Quando abiliti EC2Launch in modo che sia eseguito a ogni avvio, al successivo avvio di EC2Launch si verifica quanto riportato di seguito:
>
> - Se `AdminPasswordType` è ancora impostato su `Random`, EC2Launch genererà una nuova password al prossimo avvio. Dopo l'avvio, `AdminPasswordType` viene impostato automaticamente su `DoNothing` per impedire a EC2Launch di generare nuove password agli avvii successivi. Per impedire a EC2Launch di generare una nuova password al primo avvio, imposta manualmente `AdminPasswordType` su `DoNothing` prima di riavviare.
> - `HandleUserData` verrà di nuovo impostato su `false` a meno che i dati utente non abbiano `persist` impostato su `true`. Per ulteriori informazioni, consulta the section called “Script di dati utente”.

Inizializzazione delle unità e mappatura delle lettere di unità

Specificare le impostazioni nel file `DriveLetterMappingConfig.json` per mappare le lettere di unità nei volumi dell'istanza EC2. Lo script inizializza le unità che non sono già inizializzate e partizionate. Per ulteriori informazioni su come ottenere i dettagli del volume in Windows, consulta la pagina Get-Volume nella documentazione di Microsoft.

Mappatura delle lettere di unità nei volumi

1. Apri il file `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` in un editor di testo.
2. Specificare le seguenti impostazioni di volume e salvare le modifiche:

```
{
 "driveLetterMapping": [
  {
   "volumeName": "sample volume",
   "driveLetter": "H"
  }
 ]
}
```

3. Apri Windows PowerShell e usa il seguente comando per eseguire lo script EC2Launch che inizializza i dischi:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

   Per inizializzare i dischi ogni volta che l'istanza si avvia, aggiungere il contrassegno `-Schedule` come segue:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

Inviare i log di eventi di Windows alla console EC2.

Specificare le impostazioni nel file `EventLogConfig.json` per inviare i log di eventi di Windows ai log della console EC2.

Configurazione delle impostazioni per inviare i log di eventi di Windows

1. Nell'istanza, aprire il file `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` in un editor di testo.
2. Configurare le seguenti impostazioni di log e salvare le modifiche:

```
{
 "events": [
  {
   "logName": "System",
   "source": "An event source (optional)",
   "level": "Error | Warning | Information",
   "numEntries": 3
  }
 ]
}
```

3. In Windows PowerShell, esegui il comando seguente in modo che il sistema pianifichi l'esecuzione dello script come attività pianificata di Windows ogni volta che l'istanza viene avviata.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -
Schedule
```

   Possono essere necessari tre minuti o più prima che i log compaiano nei log della console EC2.

Inviare il messaggio Windows is ready (Windows è pronto) dopo un avvio riuscito.

Il servizio EC2Config ha inviato il messaggio "Windows è pronto" alla console EC2 dopo ogni avvio. EC2Launch invia questo messaggio solo dopo l'avvio iniziale. Per la retrocompatibilità con il servizio EC2Config, è possibile programmare EC2Launch in modo che invii questo messaggio dopo ogni avvio. Nell'istanza, apri Windows PowerShell ed esegui il comando seguente. Il sistema programma l'esecuzione dello script come Windows Scheduled Task.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -
Schedule
```

Cronologia delle versioni di EC2Launch

Le AMI di Windows che iniziano con Windows Server 2016 includono una serie di script Windows Powershell chiamati EC2Launch. EC2Launch esegue le operazioni durante l'avvio dell'istanza iniziale. Per informazioni sulle versioni EC2Launch incluse nelle AMI AWS Windows, consulta Cronologia delle versioni di Windows AWS AMI.

Per scaricare e installare la versione più recente di EC2Launch, consultare Installare la versione più recente di EC2Launch.

La tabella seguente descrive le versioni rilasciate di EC2Launch. Il formato della versione è cambiato dopo la versione 1.3.610.

Versione	Dettagli	Data di rilascio
1.3.2004959	• Logica di installazione aggiornata per impedire installazioni non supportate su Windows Server 2025 o versioni successive.	2 luglio 2024
1,32004891	• È stato risolto un problema per cui non `HandleUserData` era impostato come previsto. `false` • È stata aggiunta un'opzione per `Encrypted` la password `aLaunchConfig.json` . • `Settings UI` Comportamento modificato per crittografare la password specificata dall'utente per impostazione predefinita. • `SetAdminPasswordConfig.ps1` Aggiunto per convertire l'opzione `Specify` password nell'opzione `Encrypted` password nel file di configurazione dell'agente.	31 maggio 2024
1,32004617	• È stato corretto un errore durante l'impostazione dello sfondo.	15 gennaio 2024
1,32004592	•	2 gennaio 2024

Versione	Dettagli	Data di rilascio
	Autorizzazioni di accesso aggiornate impostate da install.ps1 per `%ProgramData%\Amazon\EC2-Windows\Launch` . • Accesso limitato a cartelle/file EC2Launch in modalità di lettura-esecuzione solo per gli account utente standard. • L'agente è stato modificato in modo da non attendere più l'inizializzazione del servizio di metadati di istanza (IMDS) se IMDS non è abilitato per l'istanza. • È stato aggiunto un timeout di cinque minuti in attesa dell'inizializzazione dell'IMDS. • È stato modificato l'agente in modo che scrivesse la telemetria nel log della console dell'istanza prima del messaggio `Windows is Ready` anziché dopo. • È stato aggiunto il supporto per gli sfondi per numerosi nuovi tipi di istanze. Per ulteriori informazioni sui permessi di accesso e sui permessi degli account utente delle directory EC2Launch, consulta. the section called “Struttura della directory di EC2Launch”	
1.3.2004491	• È stata aggiunta la telemetria per monitorare l'utilizzo dell'opzione Specifica password dell'amministratore.	9 novembre 2023
1,32004462	• Aggiunto uno scarico dopo ogni scrittura sulla console seriale.	18 ottobre 2023

Versione	Dettagli	Data di rilascio
1,32004438	• Limita la devoluzione del nome di dominio in base alla voce del registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Le autorizzazioni `UserdataExecution.log` sono state limitate esclusivamente a `Administrators` . • Sono stati aggiunti messaggi di errore nel log eventi di Windows per i casi in cui l'inizializzazione del log non riesce.	4 ottobre 2023
1,32004256	• Valore `EnableSCSIPersistentReservations` aggiunto al log della console. • È stata aggiunta la funzionalità di riprova per Get-ConsolePort.	7 luglio 2023
1,32004052	• È stato risolto un errore che si verificava quando non veniva specificata alcuna chiave SSH all'avvio dell'istanza. • È stato aggiornato per riprovare ad avviare il servizio Windows AmazonSSMAgent in caso di errore. • Aggiornato per fallire SysprepInstance .ps1 se BeforeSysprep .cmd fallisce con un codice di uscita diverso da zero.	8 marzo 2023
1,32003975	• È stato risolto il problema relativo alle build AMI Packer in cui `SysprepInstance.ps1` restituiva un valore di `$LastErrorCode` pari a 1.	24 dicembre 2022

Versione	Dettagli	Data di rilascio
1,32003961	• È stato risolto il problema per cui le password amministratore specificate in modo esplicito venivano sovrascritte con una password casuale nelle istanze avviate rapidamente. • È stato risolto il problema a causa del quale l'agente SSM non si avviava su tipi di istanze più piccoli. • È stato risolto un problema a causa del quale il log della console dell'istanza conteneva `RDPCERTIFICATE-THUMBPRINT: 0000000000000000000000000` invece di un valore di impronta digitale del certificato RDP valido.	6 dicembre 2022
1,32003923	• Corregge la logica per la ricerca dell'adattatore di rete quando PnPDeviceID è vuoto.	9 novembre 2022
1,32003919	• Informazioni aggiornate sul segmento Get- ConsolePort to use PCI. • È stato risolto il problema per cui era possibile selezionare un adattatore di rete non corretto dopo un riavvio. • È stata corretta la logica di timeout start-SSM-Agent fissa. • Compatibilità con le versioni precedenti fissa per l'alias della AdminCredentials funzione Send-.	8 novembre 2022
1.3.2003857	• Assegna priorità agli adattatori con un gateway predefinito quando viene selezionato l'adattatore di rete principale. • Aggiunta la crittografia delle password in memoria.	3 ottobre 2022

Versione	Dettagli	Data di rilascio
1,32003824	• Errore risolto durante `setComputerName` . • Aggiunta una logica per ignorare l'attivazione di Windows quando viene rilevato un codice di fatturazione BYOL. • Aggiunta la crittografia delle password in memoria. • Errore risolto durante l'inizializzazione del volume su `m6id.4xlarge` .	30 agosto 2022
1,32003691	• La logica di attesa IMDS è stata aggiornata per effettuare solo richieste IMDSv2. • Corretto un bug che influisce sull'installazione di eGPU	21 giugno 2022
1,32003639	• Aggiunta la logica di attesa dell'adattatore di rete per impedire l'uso prima dell'inizializzazione. • Risolti problemi poco importanti.	10 maggio 2022
1,32003498	• Aggiunta della telemetria. • Aggiunto il collegamento all'interfaccia utente Impostazioni. • Script formattati. PowerShell • È stato risolto il problema relativo allo spegnimento che si verificava prima del completamento del file.cmd. BeforeSys prep	31 gennaio 2022
1.3.2003411	Modificata la logica di generazione delle password per escludere le password a bassa complessità.	4 agosto 2021
1,32003364	Installazione aggiornata: con supporto per EgpuManager iMDSv2.	7 giugno 2021

Versione	Dettagli	Data di rilascio
1.3.2003312	• Aggiunte righe di log prima e dopo l'impostazione di `setMonitorAlwaysOn` . • Aggiunta la versione del AWS pacchetto Nitro Enclaves al registro della console.	04 maggio 2021
1.3.2003284	Modello di autorizzazione migliorato tramite l'aggiornamento della posizione in cui archiviare i dati dell'utente in `LocalAppData` .	23 marzo 2021
1.3.2003236	• Metodo aggiornato per l'impostazione della password utente in `Set-AdminAccount` e `Randomize-LocalAdminPassword` . • Risolto `InitializeDisks` in modo che verifichi se il disco è impostato per la sola lettura prima di impostarlo su scrivibile.	11 febbraio 2021
1.3.2003210	Correzione della localizzazione per `install.ps1` .	7 gennaio 2021
1.3.2003205	Correzione della protezione `install.ps1` per aggiornare le autorizzazioni sulla directory `%ProgramData%AmazonEC2-WindowsLaunchModuleScripts` .	28 dicembre 2020
1.3.2003189	Aggiunta di `w32tm resync` dopo avere aggiunto gli instradamenti.	4 dicembre 2020
1.3.2003155	Informazioni aggiornate sul tipo di istanza.	25 agosto 2020
1.3.2003150	Aggiunta di `OsCurrentBuild` e `OsReleaseId` all'output della console.	22 aprile 2020
1.3.2003040	Corretta la logica di fallback IMDS versione 1.	7 aprile 2020
1.3.2002730	Aggiunto il supporto per IMDS V2.	3 marzo 2020

Versione	Dettagli	Data di rilascio
1.3.2002240	Risolti problemi poco importanti.	31 ottobre 2019
1.3.2001660	È stato risolto il problema di accesso automatico per gli utenti senza password dopo la prima esecuzione di Sysprep.	2 luglio 2019
1.3.2001360	Risolti problemi poco importanti.	27 marzo 2019
1.3.2001220	Tutti PowerShell gli script sono firmati.	28 febbraio 2019
1.3.2001200	È stato risolto il problema con InitializeDisks .ps1 a causa del quale l'esecuzione dello script su un nodo in un cluster di failover di Windows Server poteva formattare le unità su nodi remoti la cui lettera di unità corrispondeva alla lettera dell'unità locale.	27 febbraio 2019
1.3.2001160	Risolto problema sfondo mancante in Windows 2019.	22 febbraio 2019
1.3.2001040	• Plugin aggiunto per impostare il monitor in modo che non si spenga mai per risolvere i problemi di ACPI. • Edizione di SQL Server e versione scritta nella console.	21 gennaio 2019
1.3.2000930	Correzione l'aggiunta di routing ai metadati su ENI abilitate per ipv6.	2 gennaio 2019
1.3.2000760	• Aggiunta la configurazione predefinita per RSS e le impostazi oni Receive Queue per i dispositivi ENA. • Ibernazione disabilitata durante Sysprep.	5 dicembre 2018

Versione	Dettagli	Data di rilascio
1.3.2000630	• Aggiunto il percorso 169.254.169.253/32 per il server DNS. • Aggiunto il filtro dell'impostazione dell'utente Admin. • Migliorie apportate all'ibernazione delle istanze. • Aggiunta l'opzione per pianificare l'esecuzione di EC2Launch a ogni avvio.	9 novembre 2018
1.3.2000430.0	• Aggiunto il percorso 169.254.169.123/32 al servizio AMZN Time Service. • Aggiunto il percorso 169.254.169.249/32 al servizio GRID License Service. • Aggiunto un timeout di 25 secondi durante il tentativo di avviare Systems Manager.	19 settembre 2018
1.3.200039.0	• Risolto un problema di aggiunta di una lettera di unità non corretta per i volumi EBS NVME. • Aggiunta un'attività di logging per le versioni dei driver NVME.	15 agosto 2018
1.3.2000080	Risolti problemi poco importanti.	
1.3.610	Problema risolto con il reindirizzamento dell'output e degli errori ai file dai dati utente.	
1.3.590	• Tipi di istanze mancanti aggiunti allo sfondo. • È stato risolto un problema con la mappatura delle lettere dell'unità e l'installazione del disco.	
1.3.580	• Risolto `Get-Metadata` per utilizzare le impostazioni predefinite del proxy di sistema per le richieste Web. • Aggiunto un caso speciale per NVMe nell'inizializzazione del disco. • Risolti problemi poco importanti.	

Versione	Dettagli	Data di rilascio
1.3.550	Aggiunta un'opzione `-NoShutdown` per attivare Sysprep senza spegnimento.	
1.3.540	Risolti problemi poco importanti.	
1.3.530	Risolti problemi poco importanti.	
1.3.521	Risolti problemi poco importanti.	
1.3.0	• Corretto un problema di lunghezza esadecimale per la modifica del nome del computer. • Corretto un possibile ciclo di riavvio per la modifica del nome del computer. • Risolto un problema nella configurazione dello sfondo.	
1.2.0	• Aggiornamento per visualizzare le informazioni sul sistema operativo (SO) installato nel log di sistema EC2. • Aggiornamento per visualizzare la versione di EC2Launch e SSM Agent nel log di sistema di EC2. • Risolti problemi poco importanti.	

Versione	Dettagli	Data di rilascio
1.1.2	• Aggiornamento per visualizzare le informazioni del driver ENA nel log di sistema di EC2. • Aggiornamento per escludere Hyper-V dalla logica del filtro NIC primario. • AWS KMS Server e porta aggiunti alla chiave di registro per l'attivazione di KMS. • Impostazione dello sfondo migliorata per più utenti. • Aggiornamento per cancellare i percorsi da uno store persistente. • Aggiornamento per rimuovere la z dalla zona di disponibilità nell'elenco dei suffissi DNS. • Aggiornamento per risolvere un problema relativo al tag < runAsLocal System> nei dati utente.	
1.1.1	Versione iniziale.	

Configurare un'istanza di Windows utilizzando il servizio EC2Config (legacy)

> **Note**
>
> La documentazione di EC2Config viene fornita solo come riferimento storico. Le versioni del sistema operativo su cui viene eseguito non sono più supportate da Microsoft. Ti consigliamo vivamente di eseguire l'aggiornamento al servizio di avvio più recente.
> Il servizio di avvio più recente per Windows Server 2022 è EC2Launch v2, che sostituisce sia EC2config che EC2Launch.

Le AMI Windows per le versioni di Windows Server precedenti a Windows Server 2016 includono un servizio opzionale, il servizio EC2Config (). `EC2Config.exe` EC2Config comincia nel momento in cui l'istanza avvia ed esegue attività durante il startup iniziale dell'istanza e tutte le volte che questa viene arrestata o avviata. EC2Config può anche eseguire attività su richiesta. Alcune di queste attività sono abilitate automaticamente, mentre altre devono essere abilitate manualmente. Sebbene il servizio sia opzionale, fornisce accesso a caratteristiche avanzate che altrimenti non sarebbero disponibili. Questo servizio viene eseguito nell'account. LocalSystem

> **Note**
>
> EC2Launch ha sostituito il servizio EC2Config sulle AMI per Windows Server 2016 e 2019. Per ulteriori informazioni, consulta Configurazione dell'istanza Windows tramite EC2Launch. Il servizio di avvio più recente per tutte le versioni supportate di Windows Server è EC2Launch v2 che sostituisce sia EC2config che EC2Launch.

EC2Config utilizza i file di configurazione per controllare la sua operazione. È possibile aggiornare questi file di configurazione usando uno strumento grafico oppure modificando direttamente i file XML. I binari di servizio e dei file aggiuntivi sono contenuti nella directory `%ProgramFiles%\Amazon\EC2ConfigService`.

Indice

Attività di EC2Config

Quando l'istanza viene avviata per la prima volta, EC2Config esegue le attività relative al startup iniziale, quindi le disabilita. Per eseguire nuovamente queste attività, è necessario abilitarle in maniera esplicita prima di arrestare l'istanza o eseguire manualmente Sysprep. Si tratta delle seguenti attività:

- Impostare una password crittografata e casuale per l'account dell'amministratore.
- Generare e installare il certificato dell'host per la Connessione Desktop in remoto.
- Estendere in modo dinamico la partizione del sistema operativo per includere qualsiasi spazio non partizionato.
- Eseguire i dati dell'utente specifici (e il cloud-init, se installato). Per ulteriori informazioni sulla specifica dei dati utente, consulta Utilizzo dei dati utente dell'istanza.

EC2Config esegue le seguenti attività ogni volta che viene avviata l'istanza:

- Modifica il nome host per farlo corrispondere con l'indirizzo IP privato in un sistema esadecimale (questa attività è disabilitata automaticamente e deve essere abilitata per eseguirla all'avvio dell'istanza).
- Configura il server della gestione della chiave (AWS KMS), verifica lo stato di attivazione di Windows e attiva Windows quando necessario.
- Monta tutti i volumi di Amazon EBS e i volumi instance store; mappa i nomi del volume per le lettere di unità.
- Scrive voci di log dell'evento per la console al fine di aiutare nella risoluzione dei problemi (questa attività è disabilitata automaticamente e deve essere abilitata per eseguirla all'avvio dell'istanza).
- Scrive alla console quando Windows è pronto.
- Aggiungere un percorso personalizzato alla scheda di rete primaria in modo da abilitare i seguenti indirizzi IP quando vengono collegate una singola scheda NIC o più schede NIC: `169.254.169.250`, `169.254.169.251` e `169.254.169.254`. Questi indirizzi vengono utilizzati dall'attivazione di Windows e quando si accede ai metadati dell'istanza.

> **Note**
>
> Se il sistema operativo Windows è configurato per l'utilizzo di IPv4, è possibile utilizzare questi indirizzi locali di collegamento IPv4. Se il sistema operativo Windows ha lo stack del protocollo di rete IPv4 disabilitato e utilizza invece IPv6, aggiungere

`[fd00:ec2::240]` al posto di `169.254.169.250` e `169.254.169.251`. Quindi aggiungere `[fd00:ec2::254]` al posto di `169.254.169.254`.

EC2Config esegue le seguenti attività ogni volta che un utente effettua l'accesso:

- Mostra informazioni a schermo sullo sfondo del desktop.

Mentre l'istanza è in esecuzione, puoi richiedere che EC2Config esegua la seguente attività su richiesta:

- Esegue Sysprep e arresta l'istanza per poter creare un'AMI da questa attività. Per ulteriori informazioni, consulta Creare un'AMI con Windows Sysprep.

Installazione della versione più recente di EC2Config

Per impostazione predefinita, il servizio EC2Config è incluso nelle AMI da prima di Windows Server 2016. Quando il servizio EC2Config viene aggiornato, le nuove AMI Windows AWS includono la versione più recente del servizio. Tuttavia, è necessario aggiornare le tue AMI di Windows e le instante con la versione più recente di EC2Config.

> **Note**
>
> EC2Launch sostituisce il servizio EC2Config sulle AMI di Windows Server 2016 e 2019. Per ulteriori informazioni, consulta Configurazione dell'istanza Windows tramite EC2Launch. Il servizio di avvio più recente per tutte le versioni supportate di Windows Server è EC2Launch v2 che sostituisce sia EC2config che EC2Launch.

Per informazioni su come ricevere notifiche sugli aggiornamenti di EC2Config, consulta Iscrizione alle notifiche del servizio EC2Config. Per informazioni sulle variazioni di ogni versione, consulta Cronologia delle versioni di EC2Config.

Prima di iniziare

- Verifica di possedere la versione 3.5 SP1 o successiva di .NET framework.
- Per impostazione predefinita, l'opzione Setup sostituisce i tuoi file di configurazione con dei file di configurazione predefiniti durante l'installazione; inoltre riavvia il servizio EC2Config quando viene

completata l'installazione. Se hai modificato le impostazioni del servizio EC2Config, copia il file `config.xml` dalla directory `%Program Files%\Amazon\Ec2ConfigService\Settings`. Dopo aver aggiornato il servizio EC2Config, puoi ripristinare questo file per mantenere le modifiche della configurazione.

- Se possiedi una versione di EC2Config precedente alla 2.1.19 e stai installando la versione 2.2.12 o una versione precedente, devi eseguire prima l'installazione della versione 2.1.19. Per installare la versione 2.1.19, scarica il file EC2Install_2.1.19.zip, decomprimilo e quindi esegui `EC2Install.exe`.

> **Note**
>
> Se possiedi una versione di EC2Config precedente alla 2.1.19 e stai installando la versione 2.3.313 o successiva, puoi installarla direttamente senza eseguire prima l'installazione della versione 2.1.19.

Verificare la versione di EC2Config

Utilizza la procedura seguente per verificare la versione di EC2Config installata sulla tua istanza.

Per verificare la versione installata di EC2Config

1. Lancia un'istanza dall'AMI e connettila.
2. Sul pannello di controllo, seleziona Programs and Features (Programmi e caratteristiche).
3. Sulla lista dei programmi installati, cerca `Ec2ConfigService`. Il numero della versione viene mostrato nella colonna Version (Versione).

Aggiornamento di EC2Config

Per scaricare e installare la versione più recente di EC2Config sulle istanze, attenersi alla procedura seguente.

Scaricare e installare la versione più recente di EC2Config

1. Scarica e decomprimi il programma di installazione di EC2Config.
2. Esegui `EC2Install.exe`. Per un elenco completo delle opzioni, esegui `EC2Install` con l'opzione `/?`. Per impostazione predefinita, la configurazione mostra i prompt. Per eseguire il comando senza alcun prompt, utilizza l'opzione `/quiet`.

> **Important**
>
> Per mantenere le impostazioni personalizzate dal file `config.xml` che hai salvato, esegui `EC2Install` con l'opzione `/norestart`, ripristina le tue impostazioni e riavvia manualmente il servizio EC2Config.

3. Se stai eseguendo la versione 4.0 o successiva di EC2Config, sarà necessario riavviare SSM Agent sull'istanza dall'applicazione Microsoft Services.

> **Note**
>
> Le informazioni aggiornate sulla versione di EC2Config non verranno visualizzate nel Log di sistema o nel controllo di Trusted Advisor dell'istanza fino a che non viene riavviata o arrestata e avviata l'istanza.

Per scaricare e installare l'ultima versione di EC2Config utilizzando PowerShell

Per scaricare, decomprimere e installare l'ultima versione di EC2Config utilizzando PowerShell, esegui i seguenti comandi da una finestra: PowerShell

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.NameSpace($ExtractPath).CopyHere($ExtractFiles)
Start-Process $ExtractPath
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

> **Note**
>
> Se ricevi un errore durante il download del file e utilizzi Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il seguente comando e riprovare:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Verifica dell'installazione controllando `C:\Program Files\Amazon\` per la directory `Ec2ConfigService`.

Arresto, riavvio, eliminazione o disinstallazione di EC2Config

Puoi gestire il servizio EC2Config come qualsiasi altro servizio.

Per applicare le impostazioni aggiornate sull'istanza, puoi interrompere e riavviare il servizio. Se stai installando manualmente EC2Config, dovrai prima interrompere il servizio.

Per interrompere il servizio EC2Config

1. Avviare l'istanza Windows e connettersi a essa.
2. Nel menu Start (Avvio), vai su Administrative Tools (Strumenti amministratore), quindi fai clic su Services (Servizi).
3. Nell'elenco dei servizi, fai clic con il pulsante destro del mouse su EC2Config e seleziona Stop (Interrompi).

Per riavviare il servizio EC2Config

1. Avviare l'istanza Windows e connettersi a essa.
2. Nel menu Start (Avvio), vai su Administrative Tools (Strumenti amministratore), quindi fai clic su Services (Servizi).
3. Nell'elenco dei servizi, fai clic con il pulsante destro del mouse su EC2Config e seleziona Restart (Riavvia).

Se non devi aggiornare le impostazioni di configurazione, creare le tue AMI o utilizzare AWS Systems Manager, puoi eliminare e disinstallare il servizio. L'eliminazione di un servizio rimuove le sottochiavi del registro. La disinstallazione di un servizio rimuove i file, le sottochiavi del registro e tutti i tasti di scelta rapida del servizio.

Per cancellare il servizio EC2Config

1. Avvia una finestra del prompt dei comandi

2. Esegui il comando riportato qui di seguito:

```
sc delete ec2config
```

Per disinstallare EC2Config

1. Avviare l'istanza Windows e connettersi a essa.
2. Nel menu Start (Avvia), fare clic su Control Panel (Pannello di controllo).
3. Fare doppio clic su Programs and Features (Programmi e caratteristiche).
4. Nell'elenco dei programmi, seleziona EC2 e fai clic su ConfigService Disinstalla.

EC2Config e AWS Systems Manager

Il servizio EC2Config elabora le richieste Systems Manager sulle istanze create dalle AMI per le versioni di Windows Server precedenti a Windows Server 2016 che sono state pubblicate prima di novembre 2016.

Le istanze create dalle AMI, per le versioni di Windows Server precedenti a Windows Server 2016 che sono state pubblicate prima di novembre 2016, includono il servizio EC2Config e SSM Agent. EC2Config esegue tutte le attività descritte precedentemente, mentre SSM Agent elabora le richieste per le funzionalità di Systems Manager come Run Command e Gestione stato.

Puoi utilizzare Run Command per aggiornare le istanze esistenti al fine di utilizzare la versione recente del servizio EC2Config e di SSM Agent. Per ulteriori informazioni, consulta Aggiornamento di SSM Agent mediante Run Command nella Guida per l'utente di AWS Systems Manager .

EC2Config e Sysprep

Il servizio EC2Config esegue Sysprep, uno strumento Microsoft che ti permette di creare un'AMI di Windows personalizzato che può essere riutilizzato. Quando EC2Config chiama Sysprep, utilizza i file contenuti in `%ProgramFiles%\Amazon\EC2ConfigService\Settings` per determinare quali operazioni eseguire. Puoi modificare questi file in maniera indiretta tramite la finestra di dialogo Ec2 Service Properties (Proprietà del servizio Ec2) oppure direttamente utilizzando un editor di testo o XML. Tuttavia esistono alcune impostazioni avanzate che non sono disponibili nella finestra di dialogo Ec2 Service Properties (Proprietà del servizio Ec2), quindi è necessario modificare direttamente queste voci.

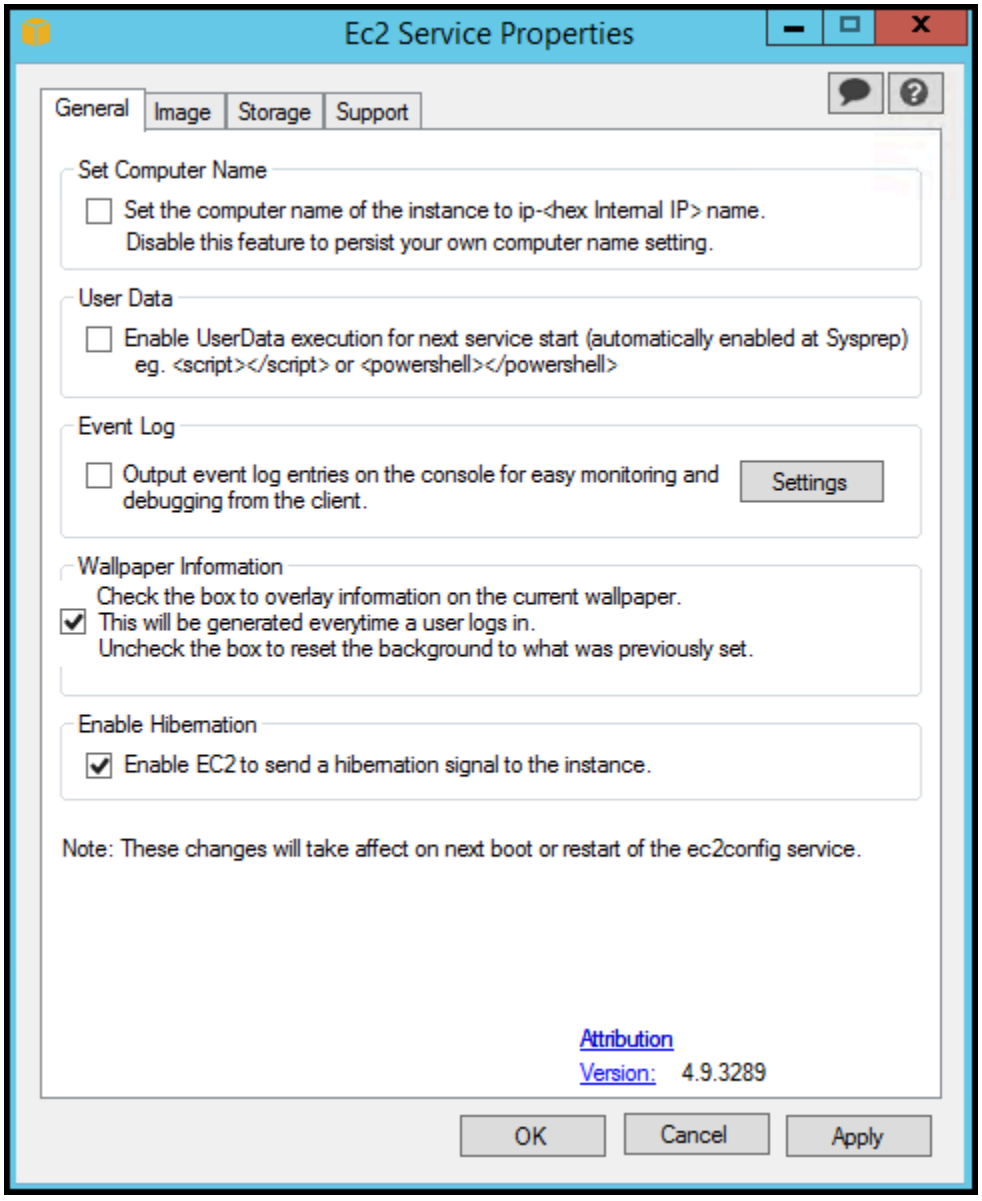
Se crei un'AMI da un'istanza dopo l'aggiornamento delle sue impostazioni, le nuove impostazioni vengono applicate a ogni istanza lanciata dalla nuova AMI. Per informazioni sulla creazione di un'AMI, consulta Crea un'AMI supportata da Amazon EBS.

Proprietà del servizio EC2

La procedura seguente descrive come utilizzare la finestra di dialogo Ec2 Service Properties (Proprietà del servizio Ec2) per abilitare o disabilitare le impostazioni.

Per cambiare le impostazioni tramite la finestra di dialogo Ec2 Service Properties (Proprietà del servizio Ec2)

1. Avviare l'istanza Windows e connettersi a essa.
2. Dal menu Start, fai clic su Tutti i programmi, quindi su Impostazioni EC2. ConfigService



3. Nella scheda General (Generali) della finestra di dialogo Ec2 Service Properties (Proprietà del servizio Ec2), è possibile abilitare o disabilitare le seguenti impostazioni.

   Set Computer Name (Imposta il nome del computer)

   Se questa impostazione è abilitata (è disabilitata per impostazione predefinita), il nome host viene confrontato con il corrente indirizzo IP interno a ogni avvio. Se il nome host e l'indirizzo IP interno non corrispondono, il nome host viene ripristinato per contenere l'indirizzo IP interno; quindi il sistema si riavvia per prendere il nuovo nome host. Per impostare il tuo nome host o per prevenire che il nome host esistente venga modificato, non abilitare questa opzione.

User Data (Dati utente)

L'esecuzione dei dati utente ti permette di specificare gli script nei metadati dell'istanza. Per impostazione predefinita, questi script vengono eseguiti durante il lancio iniziale. Inoltre, puoi configurare gli script per eseguirli al prossimo avvio e riavvio dell'istanza o ogni volta che avvii o riavvii l'istanza.

Se possiedi uno script di grandi dimensioni, ti raccomandiamo di utilizzare i dati utente per scaricare lo script per poi eseguirlo.

Per ulteriori informazioni, consulta Esecuzione dei dati utente.

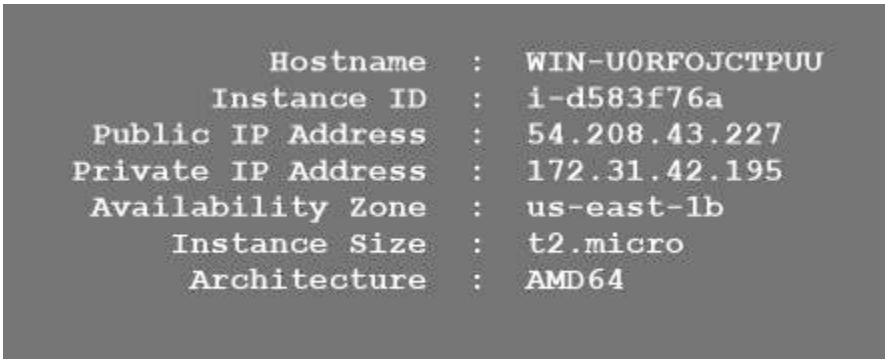
Event Log (Log eventi)

Utilizza questa impostazione per mostrare le voci dei log evento sulla console all'avvio, così da poter effettuare più facilmente il monitoraggio e il debug.

Fai clic su Settings (Impostazioni) per specificare i filtri per le voci di log inviate alla console. Il filtro predefinito invia le tre voci di errore più recenti dai log evento di sistema alla console.

Wallpaper Information (Informazioni sfondo)

Utilizza questa impostazione per mostrare le informazioni di sistema sullo sfondo del desktop. L'esempio seguente riguarda le informazioni mostrate sullo sfondo del desktop

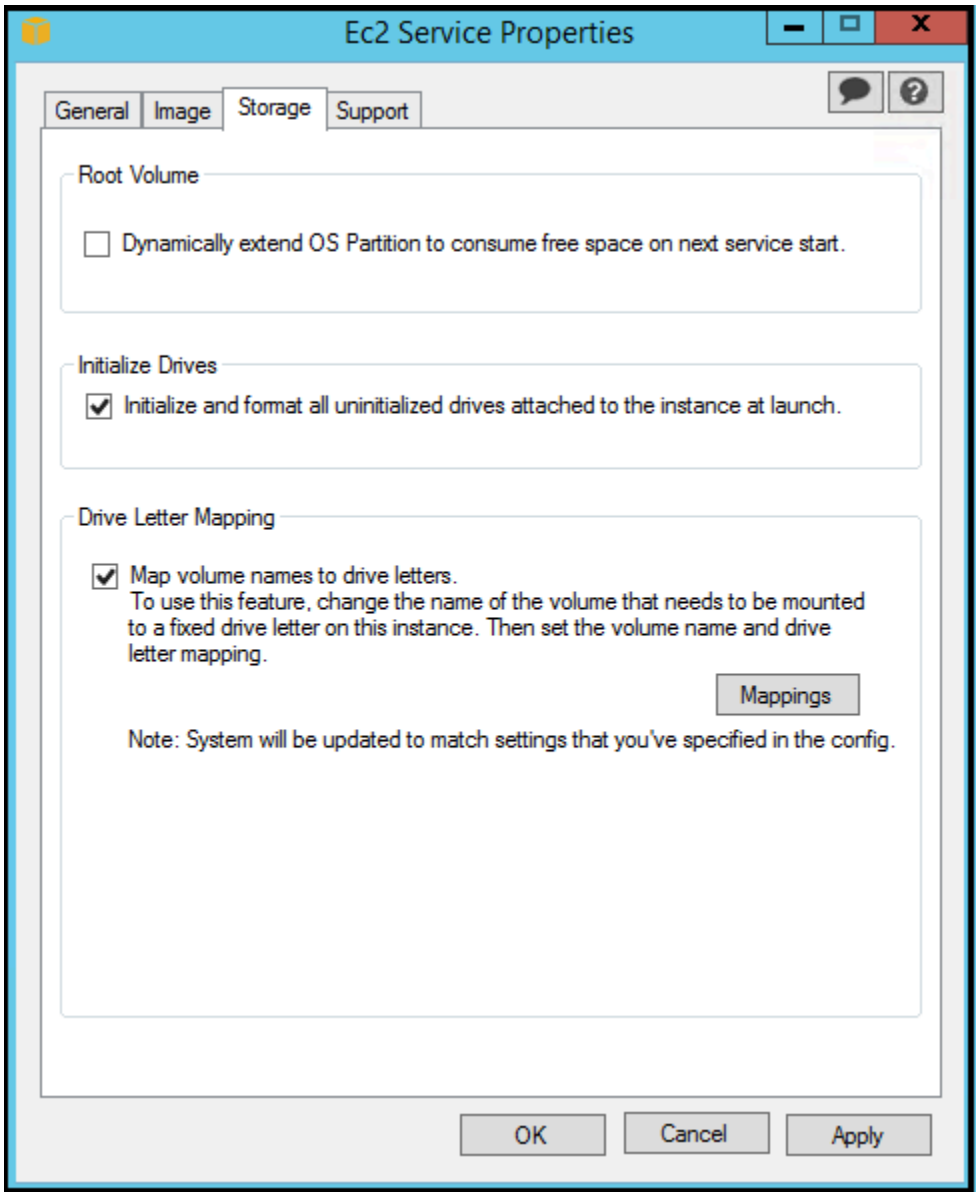


Le informazioni mostrate sullo sfondo del desktop sono controllate dal file delle impostazioni `EC2ConfigService\Settings\WallpaperSettings.xml`.

Abilitazione ibernazione

Utilizza questa impostazione affinché EC2 sia in grado di segnalare al sistema operativo di eseguire l'ibernazione.

4. Fare clic sulla scheda Storage (archiviazione). Puoi abilitare o disabilitare le seguenti impostazioni.



Root Volume (Volume root)

Questa impostazione estende in modo dinamico Disco 0/Volume 0 per includere qualsiasi spazio non partizionato. Ciò può essere utile quando l'istanza viene avviata da un volume dispositivo root di dimensioni personalizzate.

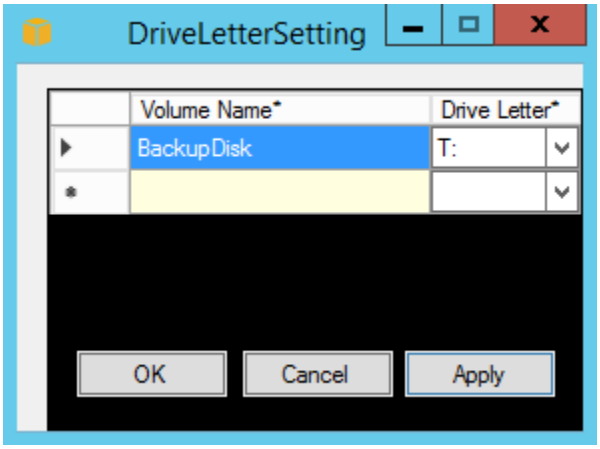
Initialize Drives (Inizializza unità)

Questa impostazione formatta e monta tutti i volumi collegati all'istanza durante l'avvio.

Drive Letter Mapping (Mappatura lettera unità)

Il sistema mappa i volumi collegati a un'istanza per le lettere di unità. Per i volumi Amazon EBS, l'impostazione predefinita assegna le lettere di unità che vanno dalla D: alla Z:. Ad esempio, i volumi di archiviazione, l'impostazione predefinita dipende dal driver. AWS I driver PV e i driver Citrix PV assegnano ai volumi di archiviazione delle istanze le lettere di unità che vanno da Z: a A:. I driver Red Hat assegnano, ai volumi instance store, lettere di unità che vanno dalla D: alla Z:.

Per scegliere le lettere di unità dei tuoi volumi, fai clic su Mappings (Mappature). Nella DriveLetterSettingfinestra di dialogo, specificate i valori Volume Name e Drive Letter per ogni volume, fate clic su Applica, quindi fate clic su OK. Ti raccomandiamo di selezionare lettere di unità che evitino conflitti con lettere di unità che potrebbero essere in uso, come le lettere di unità al centro dell'alfabeto.



Dopo aver specificato una mappatura della lettera di unità e collegato un volume con la stessa etichetta dei nomi volume specificati, EC2Config assegna automaticamente la lettera di unità specificata per quel volume. Tuttavia, se la lettera di unità è già in uso, la mappatura della lettera di unità avrà esito negativo. Nota che EC2Config, non modifica le lettere di unità dei volumi che sono già stati montati dopo aver specificato la mappatura della lettera di unità.

5. Per salvare le impostazioni e continuare a lavorarci in un secondo momento, fai clic su OK per chiudere la finestra di dialogo EC2 Service Properties (Proprietà del servizio EC2). Se hai terminato con la personalizzazione della tua istanza e desideri creare un'AMI da quella istanza, consulta Creare un'AMI con Windows Sysprep.

File delle impostazioni di EC2Config

I file di impostazione controllano l'operazione del servizio EC2Config. Questi file si trovano nella directory `C:\Program Files\Amazon\Ec2ConfigService\Settings`:

- `ActivationSettings.xml`: controlla l'attivazione del prodotto tramite un server di gestione della chiave (AWS KMS).
- `AWS.EC2.Windows.CloudWatch.json`—Controlla a quali contatori delle prestazioni inviare CloudWatch e quali registri inviare ai registri. CloudWatch
- `BundleConfig.xml` – Controlla in che modo EC2Config prepara un'istanza supportata dall'instance store per la creazione delle AMI.
- `Config.xml` – Controlla le impostazioni primarie.
- `DriveLetterConfig.xml` – Controlla le mappature delle lettere di unità.
- `EventLogConfig.xml` – Controlla le informazioni dei log evento mostrati sulla console all'avvio dell'istanza.
- `WallpaperSettings.xml` – Controlla le informazioni mostrate sullo sfondo del desktop.

ActivationSettings.xml

Questo file contiene le impostazioni che controllano l'attivazione del prodotto. All'avvio di Windows, il servizio EC2Config verifica se Windows è già stato attivato. Se Windows non è stato ancora attivato, il servizio prova ad attivarlo cercando lo specifico server AWS KMS .

- `SetAutodiscover`: indica se un AWS KMS verrà rilevato automaticamente.
- `TargetKMSServer`—Memorizza l'indirizzo IP privato di un. AWS KMS Il AWS KMS deve trovarsi nella stessa regione della tua istanza.
- `DiscoverFromZone`—Rileva il AWS KMS server dalla zona DNS specificata.
- `ReadFromUserData`—Recupera il server da. AWS KMS UserData
- `LegacySearchZones`—Rileva il AWS KMS server dalla zona DNS specificata.
- `DoActivate` – Tenta l'attivazione tramite le impostazioni specificate nella sezione. Questo valore può essere `true` o `false`.
- `LogResultToConsole` – Mostra i risultati sulla console.

BundleConfig.xml

Questo file contiene le impostazioni che controllano in che modo EC2Config prepara un'istanza per la creazione di AMI.

- `AutoSysprep` – Indica la possibilità di utilizzare Sysprep in modo automatico. Modifica il valore su `Yes` per utilizzare Sysprep.
- `SetRDPCertificate` – Imposta un certificato autofirmato per il server del desktop remoto. Questa operazione ti permette di utilizzare l'RDP in modo sicuro nell'istanza. Modifica il valore su `Yes` se la nuova istanza possiede il certificato.

  Questa impostazione non viene utilizzata per le istanze con versioni del sistema operativo precedenti a Windows Server 2016, poiché possono generare i propri certificati.
- `SetPasswordAfterSysprep` – Imposta una password casuale in un'istanza appena avviata, la crittografa con la chiave di lancio dell'utente e invia la password crittografata alla console. Modifica il valore di questa impostazione su `No` se le nuove istanze non sono impostate per creare una password criptata casuale.

Config.xml

Plug-ins (Plug-in)

- `Ec2SetPassword` – Genera una password criptata casuale ogni volta che avvii un'istanza. Questa caratteristica si disattiva per impostazione predefinita dopo il primo lancio, affinché il riavvio di questa istanza non modifichi una password impostata dall'utente. Modifica questa impostazione su `Enabled` per continuare a generare password ogni volta che lanci un'istanza.

  Questa impostazione è importante se si desidera creare un'AMI dalla propria istanza.
- `Ec2SetComputerName` – Imposta il nome host dell'istanza come nome univoco basato sull'indirizzo IP dell'istanza e la riavvia. Per impostare il tuo nome host o per prevenire che il nome host esistente venga modificato, è necessario disabilitare questa impostazione.
- `Ec2InitializeDrives` – Inizializza e formatta tutti i volumi durante il startup. Questa caratteristica viene attivata per impostazione predefinita.
- `Ec2EventLog` – Mostra le voci di log evento nella console. Per impostazione predefinita, vengono mostrate le tre voci di errore più recenti dai log evento del sistema. Per specificare quali voci di log evento mostrare, modifica il file `EventLogConfig.xml` che si trova nella directory

`EC2ConfigService\Settings`. Per informazioni riguardanti le impostazioni in questo file, consulta la pagina relativa alla Chiave Eventlog nella libreria di MSDN.

- `Ec2ConfigureRDP` – Imposta un certificato autofirmato sull'istanza, così che gli utenti possano accedere in modo sicuro all'istanza tramite il desktop remoto. Questa impostazione non viene utilizzata per le istanze con versioni del sistema operativo precedenti a Windows Server 2016, poiché possono generare i propri certificati.
- `Ec2OutputRDPCert` – Mostra le informazioni del certificato del desktop remoto sulla console, così che l'utente possa verificarlo con quello dell'identificazione personale.
- `Ec2SetDriveLetter` – Imposta le lettere di unità dei volumi montati secondo le impostazioni definite dall'utente. Per impostazione predefinita, quando un volume Amazon EBS viene collegato a un'istanza, questa non può essere montata tramite la lettera di unità nell'istanza. Per specificare le mappature della lettera di unità, modifica il file `DriveLetterConfig.xml` che si trova nella directory `EC2ConfigService\Settings`.
- `Ec2WindowsActivate` – Il plug-in gestisce l'attivazione di Windows. Esegue una verifica per controllare se Windows è stato attivato. In caso contrario, aggiorna le impostazioni AWS KMS del client e quindi attiva Windows.

  Per modificare le AWS KMS impostazioni, modifica il `ActivationSettings.xml` file che si trova nella `EC2ConfigService\Settings` directory.
- `Ec2DynamicBootVolumeSize` – Estende Disco 0/Volume 0 per includere qualsiasi spazio non partizionato.
- `Ec2HandleUserData` — Crea ed esegue gli script creati dall'utente al momento del primo avvio di un'istanza, dopo che Sysprep viene eseguito. I comandi racchiusi nei tag di script vengono salvati in un file batch e i comandi racchiusi nei PowerShell tag vengono salvati in un file.ps1 (corrisponde alla casella di controllo Dati utente nella finestra di dialogo Proprietà del servizio Ec2).
- `Ec2ElasticGpuSetup` – Installa il pacchetto software delle GPU Elastiche, se l'istanza è associata a una GPU elastica.
- `Ec2FeatureLogging` – Invia a Windows l'installazione della funzionalità e il corrispondente stato dei servizi alla console. Supportato solo per la funzionalità Microsoft Hyper-V e il corrispondente servizio vmms.

Impostazioni generali

- `ManageShutdown` – Assicura che le istanze lanciate dalle AMI supportate da instance store non terminino durante l'esecuzione di Sysprep.

- `SetDnsSuffixList` – Abilita il suffisso DNS della scheda di rete per Amazon EC2. Questa operazione consente la risoluzione DNS dei server in esecuzione su Amazon EC2 senza fornire il nome di dominio completo.

  > **Note**
  >
  > Ciò aggiunge una ricerca dei suffissi DNS per il seguente dominio e configura altri suffissi standard. Per ulteriori informazioni su come gli agenti di avvio impostano i suffissi DNS, consulta. Configura il suffisso DNS per gli agenti di avvio di Windows
  >
  > ```
  > region.ec2-utilities.amazonaws.com
  > ```

- `WaitForMetaDataAvailable` – Assicura che il servizio EC2Config attenderà che i metadati siano accessibili e che la rete sia disponibile prima di proseguire con l'avvio. Questa verifica assicura che EC2Config riesca a ottenere informazioni dai metadati per l'attivazione e per gli altri plug-in.
- `ShouldAddRoutes` – Aggiunge un percorso personalizzato per la scheda di rete primaria in modo da abilitare i seguenti indirizzi IP quando vengono collegate più schede NIC: 169.254.169.250, 169.254.169.251 e 169.254.169.254. Questi indirizzi vengono utilizzati dall'attivazione di Windows e quando si accede ai metadati dell'istanza.
- `RemoveCredentialsfromSyspreponStartup`—Rimuove la password dell'amministratore da `Sysprep.xml` al successivo avvio del servizio. Per essere sicuro che questa password persista, modifica questa impostazione.

DriveLetterConfig.xml

Questo file contiene le impostazioni che controllano le mappature della lettera di unità. Per impostazione predefinita, un volume può essere mappato su qualsiasi lettera di unità disponibile. È possibile montare un volume su una determinata lettera di unità come segue.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
  <Mapping>
```

```
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- `VolumeName` – L'etichetta del volume. Ad esempio, *`My Volume`*. Per specificare una mappatura per un volume dello archiviazione dell'istanza, utilizzare l'etichetta `Temporary Storage X`, dove `X` è un numero compreso tra 0 e 25.
- `DriveLetter`—La lettera dell'unità. Ad esempio, *`M:`*. Se la lettera di unità è già in uso, la mappatura avrà esito negativo.

EventLogConfig.xml

Questo file contiene le impostazioni che controllano le informazioni dei log evento mostrati sulla console all'avvio dell'istanza. Per impostazione predefinita, vengono mostrate le tre voci di errore più recenti dai log evento di sistema.

- `Category` – La chiave del log evento da monitorare.
- `ErrorType` – Il tipo di evento, ad esempio `Error`, `Warning`, `Information`.
- `NumEntries` – Il numero di eventi archiviati per questa categoria.
- `LastMessageTime` – Per evitare che lo stesso messaggio venga inviato ripetutamente, il servizio aggiorna questo valore ogni volta che viene inviato un messaggio.
- `AppName` – L'origine o l'applicazione dell'evento che lo ha registrato.

WallpaperSettings.xml

Questo file contiene le impostazioni che controllano le informazioni mostrate sullo sfondo del desktop. Le seguenti informazioni sono mostrate per impostazione predefinita.

- `Hostname` – Mostra il nome del computer.
- `Instance ID` – Mostra l'ID dell'istanza.
- `Public IP Address` – Mostra l'indirizzo IP pubblico dell'istanza.
- `Private IP Address` – Mostra l'indirizzo IP privato dell'istanza.
- `Availability Zone` – Mostra la zona di disponibilità in cui viene eseguita l'istanza.
- `Instance Size` – Mostra il tipo di istanza.

- `Architecture` – Mostra l'impostazione della variabile ambiente `PROCESSOR_ARCHITECTURE`.

Cancellando la voce di una qualsiasi informazione mostrata come predefinita, è possibile rimuoverla. Puoi aggiungere ulteriori metadati dell'istanza affinché vengano mostrati come di seguito.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

Puoi aggiungere ulteriori variabili ambiente del sistema affinché vengano mostrate come di seguito.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Questo file contiene le impostazioni che controllano in che modo EC2Config inizializza i drive.

Per impostazione predefinita, EC2Config inizializza i drive che non sono stati messi online dal sistema operativo. Puoi personalizzare il plug-in come di seguito.

```
<InitializeDrivesSettings>
    <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Utilizza un gruppo di impostazioni per specificare in che modo desideri inizializzare i drive:

FormatWithTAGLIARE

Abilita il comando TRIM al momento della formattazione dei drive. Dopo che un drive è stato formattato e inizializzato, il sistema ripristina la configurazione TRIM.

A partire dalla versione 3.18 di EC2Config, il comando TRIM viene disabilitato per impostazione predefinita durante l'operazione di formato disco. Tutto ciò migliora il tempo di formattazione. Utilizza questa impostazione per abilitare il comando TRIM durante l'operazione di formato disco, per le versioni 3.18 e successive di EC2Config.

FormatWithoutRIFINIRE

Disabilita il comando TRIM quando si formattano i drive e migliora i tempi di formattazione su Windows. Dopo che un drive è stato formattato e inizializzato, il sistema ripristina la configurazione TRIM.

DisableInitializeDrives

Disabilita la formattazione per i nuovi drive. Utilizza questa impostazione per inizializzare manualmente i drive.

Configurazione delle impostazioni proxy per il servizio EC2Config

È possibile configurare il servizio EC2Config per comunicare tramite un proxy utilizzando uno dei seguenti metodi: l'SDK for AWS .NET, l'`system.net`elemento o Microsoft Group Policy e Internet Explorer. L'utilizzo dell' AWS SDK for .NET è il metodo preferito perché è possibile specificare le credenziali di accesso.

Metodi

- Configura le impostazioni del proxy utilizzando (Preferito AWS SDK for .NET)
- Configurazione delle impostazioni proxy utilizzando l'elemento system.net
- Configurazione delle impostazioni proxy con la policy del gruppo Microsoft e con Microsoft Internet Explorer

Configura le impostazioni del proxy utilizzando (Preferito AWS SDK for .NET)

Puoi configurare le impostazioni del proxy per il servizio EC2Config specificando l'elemento `proxy` nel file `Ec2Config.exe.config`. Per ulteriori informazioni, consulta Configuration Files Reference for AWS SDK for .NET.

Per specificare l'elemento proxy su Ec2Config.exe.config

1. Modifica il file `Ec2Config.exe.config` sull'istanza dove desideri che il servizio EC2Config comunichi attraverso un proxy. Per impostazione predefinita, il file si trova nella directory seguente: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Aggiungi il seguente elemento `aws` sulla `configSections`. Non aggiungerlo per nessun `sectionGroups` esistente.

   Per la versione 3.17 di EC2Config o precedente

```
<configSections>
   <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
</configSections>
```

Per la versione 3.18 di EC2Config o successiva

```
<configSections>
     <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
</configSections>
```

3. Aggiungi il seguente elemento `aws` per il file `Ec2Config.exe.config`.

```
<aws>
   <proxy
     host="string value"
     port="string value"
     username="string value"
     password="string value" />
</aws>
```

4. Salva le modifiche.

Configurazione delle impostazioni proxy utilizzando l'elemento system.net

Puoi specificare le impostazioni del proxy in un elemento `system.net` sul file `Ec2Config.exe.config`. Per ulteriori informazioni, consulta l'articolo relativo all'elemento defaultProxy (Impostazioni di rete) su MSDN.

Per specificare l'elemento system.net su Ec2Config.exe.config

1. Modifica il file `Ec2Config.exe.config` sull'istanza dove desideri che il servizio EC2Config comunichi attraverso un proxy. Per impostazione predefinita, il file si trova nella directory seguente: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Aggiungi una voce `defaultProxy` per `system.net`. Per ulteriori informazioni, consulta l'articolo relativo all'elemento defaultProxy (Impostazioni di rete) su MSDN.

   La seguente configurazione, ad esempio, instrada tutto il traffico per consentire l'uso del proxy attualmente configurato per Internet Explorer, fatta eccezione per il traffico dei metadati e della licenza, che ignoreranno il proxy.

```
<defaultProxy>
    <proxy usesystemdefault="true" />
    <bypasslist>
        <add address="169.254.169.250" />
        <add address="169.254.169.251" />
        <add address="169.254.169.254" />
        <add address="[fd00:ec2::250]" />
        <add address="[fd00:ec2::254]" />
    </bypasslist>
</defaultProxy>
```

3. Salva le modifiche.

Configurazione delle impostazioni proxy con la policy del gruppo Microsoft e con Microsoft Internet Explorer

Il servizio EC2Config esegue l'account utente nel LocalSystem. Dopo aver modificato le impostazioni della policy del gruppo sull'istanza, puoi specificare le impostazioni del proxy di tutte le istanze per l'account su Internet Explorer.

Per configurare le impostazioni del proxy con la policy del gruppo e Internet Explorer

1. Sull'istanza dove desideri che il servizio EC2Config comunichi attraverso un proxy, apri un prompt Command (Comando) come amministratore, digita **`gpedit.msc`** e premi Invio.
2. Nell'editor della policy del gruppo locale, su Local Computer Policy (Policy computer locale), scegli Computer Configuration (Configurazione del computer), Administrative Templates (Modelli amministrativi), Windows Components (Componenti di Windows), Internet Explorer.
3. Nel riquadro a destra, scegli Make proxy settings per-machine (rather than per-user) (Attiva impostazioni proxy per la macchina, anziché per l'utente), quindi scegli Edit policy setting (Modifica impostazione proxy).
4. Seleziona Enabled (Abilitato), quindi Apply (Applica).
5. Apri Internet Explorer e scegli il pulsante Tools (Strumenti).
6. Seleziona Internet Option (Opzioni internet), quindi scegli la scheda Connections (Connessioni).
7. Seleziona LAN settings (Impostazioni LAN).
8. Sotto Proxy server (Server proxy), scegliere l'opzione Use a proxy server for your LAN (Usa un server proxy per la LAN).
9. Specifica le informazioni della porta e dell'indirizzo e scegli OK.

Cronologia delle versioni di EC2Config

Le AMI di Windows precedenti a Windows Server 2016 includono un servizio opzionale chiamato EC2 Config (`EC2Config.exe`). EC2Config comincia nel momento in cui l'istanza avvia ed esegue attività durante il startup iniziale dell'istanza e tutte le volte che questa viene arrestata o avviata.

Puoi ricevere notifiche quando vengono rilasciate nuove versioni del servizio EC2Config. Per ulteriori informazioni, consulta Iscrizione alle notifiche del servizio EC2Config.

La tabella seguente descrive le versioni rilasciate di EC2Config. Per ulteriori informazioni sugli aggiornamenti per SSM Agent, consulta l'articolo relativo alle note di rilascio di SSM Agent Systems Manager.

Versione	Dettagli	Data di rilascio
4.9.5777	• Problema risolto per cui la configurazione RSS era impostata in modo errato per alcuni tipi di istanze. • Nuova versione di SSM Agent `3.3.484.0` .	17 giugno 2024
4.9.554	• Limita la devoluzione del nome di dominio in base alla voce del registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Nuova versione di SSM Agent `3.2.1630.0` .	4 ottobre 2023
4,9,5467	• È stata aggiunta la funzionalità di riprova per scoprire la porta della console. • Nuova versione di SSM Agent `3.1.2282.0` .	1° agosto 2023
4,9,5288	• SDK del core di AWS aggiornato alla versione `3.7.103.23` . •	8 marzo 2023

Versione	Dettagli	Data di rilascio
	È stato risolto il problema a causa del quale il documento SSM `AWS-UpdateEC2Config` non aggiornava `EC2Config` nelle istanze abilitate solo con IMDSv2. • Nuova versione di SSM Agent `3.1.2144.0` .	
4,9,5231	• Nuova versione di SSM Agent 3.1.1927.0.	14 febbraio 2023
4,9,5103	• È stato risolto un problema a causa del quale i volumi effimeri venivano erroneamente identificati nelle famiglie di istanze r5d e i4i. • Nuova versione di SSM Agent 3.1.1856.0.	5 dicembre 2022
4,9,5064	• È stato effettuato un aggiornamento per utilizzare le informazioni sui segmenti PCI per selezionare la porta della console. • PowerShell Script firmati e intestazioni di copyright aggiunte. • Logica di selezione dell'adattatore di rete primario fisso. • Nuova versione di SSM Agent 3.1.1732.0.	16 novembre 2022
4.9.4588	• La logica di attesa IMDS è stata aggiornata per effettuare solo richieste IMDSv2. • È stata aggiunta la libreria condivisa dell'agente di avvio libec2launch.dll. • Nuova versione di SSM Agent 3.1.1188.0.	31 maggio 2022

Versione	Dettagli	Data di rilascio
4,9,4556	• Aggiunta la logica di attesa per garantire l'inizializzazione completa della scheda NIC prima dell'uso. • La nuova versione di Log4Net 2.0.14.0 include la patch di sicurezza. • La nuova versione di SSM Agent 3.1.1045.0 include la patch di sicurezza.	1 marzo 2022
4,9,4536	• Risolto il problema di arresto anomalo di userdata quando manca la cartella Temp. • Nuova versione di SSM Agent 3.1.804.0.	31 gennaio 2022
4,9,4508	• Risolto il problema per calcolare correttamente il percorso dello script diskpart. • Nuova versione di SSM Agent 3.1.338.0.	6 ottobre 2021
4,9,4500	• `Install-EgpuManagerConfig` aggiornato con il supporto di IMDS v2. • Link Web aggiornati per utilizzare https. • Nuova versione di SSM Agent (3.1.282.0)	7 settembre 2021
4,9,4419	• Corretta la logica di fallback IMDS versione 1 • È stato aggiornato l'intero utilizzo della directory temporanea di Windows alla directory temporanea EC2config • Nuova versione dell'SSM Agent (3.0.1124.0)	2 giugno 2021

Versione	Dettagli	Data di rilascio
4.9.4381	• Aggiunto il supporto per lo schema di documento SSM versione 2.2 in EC2 ConfigUpdater • Aggiunta la versione del AWS pacchetto Nitro Enclaves al registro della console • Nuova versione dell'SSM Agent (3.0.529.0)	4 maggio 2021
4.9.4326	• Rimossi tutti i collegamenti nell'interfaccia utente delle impostazioni • Questa è l'ultima versione di EC2config che supporta Windows Server 2008.	3 marzo 2021
4.9.4279	• Risolto il problema di protezione relativo all'attività pianificata `Ec2ConfigMonitor` • Risolto il problema della mappatura delle lettere di unità e il conteggio dei dischi temporanei • Aggiunta di `OsCurrentBuild` e `OsReleaseId` all'output della console • Nuova versione dell'SSM Agent 2.3.871.0	11 dicembre 2020
4.9.4222	• Corretta la logica di fallback IMDS versione 1 • Nuova versione dell'SSM Agent 2.3.842.0	7 aprile 2020
4.9.4122	• Aggiunto il supporto per IMDS V2. • Nuova versione dell'SSM Agent 2.3.814.0	4 marzo 2020
4.9.3865	• Corretto errore di individuazione della porta COM per Windows Server 2008 R2 su istanze metal • Nuova versione dell'SSM Agent (2.3.722.0)	31 ottobre 2019
4.9.3519	• Nuova versione dell'SSM Agent 2.3.634.0	18 giugno 2019

Versione	Dettagli	Data di rilascio
4.9.3429	• Nuova versione dell'SSM Agent (2.3.542.0)	25 aprile 2019
4.9.3289	• Nuova versione dell'SSM Agent 2.3.444.0	11 febbraio 2019
4.9.3270	• Plugin aggiunto per impostare il monitor in modo che non si spenga mai per risolvere i problemi di ACPI • Edizione di SQL Server e versione scritta nella console • Nuova versione dell'SSM Agent 2.3.415.0	22 gennaio 2019
4.9.3230	• La descrizione Drive Letter Mapping è stata aggiornata per essere maggiormente in linea con la funzionalità • Nuova versione dell'SSM Agent 2.3.372.0	10 gennaio 2019
4.9.3160	• Tempo di attesa aumentate per il filtro NIC primario • Aggiunta la configurazione predefinita per RSS e le impostazi oni Receive Queue per i dispositivi ENA • Ibernazione disabilitata durante Sysprep • Nuova versione dell'SSM Agent 2.3.344.0 • SDK aggiornato alla versione 3.3.29.13 AWS	15 dicembre 2018
4.9.3067	• Migliorie apportate all'ibernazione delle istanze • Nuova versione dell'SSM Agent 2.3.235.0	8 Novembre 2018
4.9.3034	• Aggiunto il percorso 169.254.169.253/32 per il server DNS • Nuova versione dell'SSM Agent 2.3.193.0	24 ottobre 2018
4.9.2986	• Aggiunta la firma per tutti i binari correlati EC2Config • Nuova versione dell'SSM Agent 2.3.136.0	11 ottobre 2018
4.9.2953	Nuova versione dell'SSM Agent (2.3.117.0)	2 ottobre 2018

Versione	Dettagli	Data di rilascio
4.9.2926	Nuova versione dell'SSM Agent (2.3.68.0)	18 settembre 2018
4.9.2905	• Nuova versione dell'SSM Agent (2.3.50.0) • Aggiunto il percorso 169.254.169.123/32 al servizio AMZN Time Service • Aggiunto il percorso 169.254.169.249/32 al servizio GRID License Service • Risolto un problema per cui i volumi EBS NVMe venivano contrassegnati come temporanei	17 settembre 2018
4.9.2854	Nuova versione dell'SSM Agent (2.3.13.0)	17 agosto 2018
4.9.2831	Nuova versione dell'SSM Agent (2.2.916.0)	7 agosto 2018
4.9.2818	Nuova versione dell'SSM Agent (2.2.902.0)	31 luglio 2018
4.9.2756	Nuova versione dell'SSM Agent (2.2.800.0)	27 giugno 2018
4.9.2688	Nuova versione dell'SSM Agent (2.2.607.0)	25 maggio 2018
4.9.2660	Nuova versione dell'SSM Agent (2.2.546.0)	11 maggio 2018
4.9.2644	Nuova versione dell'SSM Agent (2.2.493.0)	26 aprile 2018
4.9.2586	Nuova versione dell'SSM Agent (2.2.392.0)	28 marzo 2018

Versione	Dettagli	Data di rilascio
4.9.2565	• Nuova versione dell'SSM Agent (2.2.355.0) • Corretto un problema sulle istanze M5 e C5 (impossibile trovare i driver PV) • Aggiunta registrazione della console per tipo di istanza, driver PV più recenti e driver NVMe	13 marzo 2018
4.9.2549	Nuova versione dell'SSM Agent (2.2.325.0)	8 marzo 2018
4.9.2461	Nuova versione dell'SSM Agent (2.2.257.0)	15 febbraio 2018
4.9.2439	Nuova versione dell'SSM Agent (2.2.191.0)	6 febbraio 2018
4.9.2400	Nuova versione dell'SSM Agent (2.2.160.0)	16 gennaio 2018
4.9.2327	• Nuova versione dell'SSM Agent (2.2.120.0) • Aggiunta individuazione porta COM sulle istanze bare metal di Amazon EC2 • Aggiunto stato registrazione Hyper-V sulle istanze bare metal di Amazon EC2	2 gennaio 2018
4.9.2294	Nuova versione dell'SSM Agent (2.2.103.0)	4 dicembre 2017
4.9.2262	Nuova versione dell'SSM Agent (2.2.93.0)	15 novembre 2017
4.9.2246	Nuova versione dell'SSM Agent (2.2.82.0)	11 novembre 2017

Versione	Dettagli	Data di rilascio
4.9.2218	Nuova versione dell'SSM Agent (2.2.64.0)	29 ottobre 2017
4.9.2212	Nuova versione dell'SSM Agent (2.2.58.0)	23 ottobre 2017
4.9.2203	Nuova versione dell'SSM Agent (2.2.45.0)	19 ottobre 2017
4.9.2188	Nuova versione dell'SSM Agent (2.2.30.0)	10 ottobre 2017
4.9.2180	• Nuova versione dell'SSM Agent (2.2.24.0) • Aggiunto plug-in GPU elastico per istanze GPU	5 ottobre 2017
4.9.2143	Nuova versione dell'SSM Agent (2.2.16.0)	1 ottobre 2017
4.9.2140	Nuova versione dell'SSM Agent (2.1.10.0)	
4.9.2130	Nuova versione dell'SSM Agent (2.1.4.0)	
4.9.2106	Nuova versione dell'SSM Agent (2.0.952.0)	
4.9.2061	Nuova versione dell'SSM Agent (2.0.922.0)	
4.9.2047	Nuova versione dell'SSM Agent (2.0.913.0)	
4.9.2031	Nuova versione dell'SSM Agent (2.0.902.0)	
4.9.2016	• Nuova versione dell'SSM Agent (2.0.879.0) • È stato corretto il percorso della directory CloudWatch Logs per Windows Server 2003	

Versione	Dettagli	Data di rilascio
4.9.1981	• Nuova versione dell'SSM Agent (2.0.847.0) • Corretto il problema relativo a `important.txt` che è stato generato sui volumi EBS.	
4.9.1964	Nuova versione dell'SSM Agent (2.0.842.0)	
4.9.1951	• Nuova versione dell'SSM Agent (2.0.834.0) • Corretto un problema relativo alla lettera di unità, la quale non veniva mappata a partire dalla Z per le unità temporanee.	
4.9.1925	• Nuova versione dell'SSM Agent (2.0.822.0) • [Bug] Questa versione non è una destinazione di aggiornam ento valida per l'SSM Agent v4.9.1775.	
4.9.1900	Nuova versione dell'SSM Agent (2.0.805.0)	
4.9.1876	• Nuova versione dell'SSM Agent (2.0.796.0) • Corretto un problema relativo al reindirizzamento dell'output e degli errori per l'esecuzione dati utente dell'amministratore.	
4.9.1863	• Nuova versione dell'SSM Agent (2.0.790.0) • Corretto un problema relativo al collegamento di più volumi EBS su un'istanza Amazon EC2. • È stato migliorato CloudWatch il percorso di configurazione, mantenendo la compatibilità con le versioni precedenti.	
4.9.1791	Nuova versione dell'SSM Agent (2.0.767.0)	

Versione	Dettagli	Data di rilascio
4.9.1775	Nuova versione dell'SSM Agent (2.0.761.0)	
4.9.1752	Nuova versione dell'SSM Agent (2.0.755.0)	
4.9.1711	Nuova versione dell'SSM Agent (2.0.730.0)	
4.8.1676	Nuova versione dell'SSM Agent (2.0.716.0)	
4.7.1631	Nuova versione dell'SSM Agent (2.0.682.0)	
4.6.1579	• Nuova versione dell'SSM Agent (2.0.672.0) • Corretto il problema dell'aggiornamento dell'agente per v4.3, v4.4 e v4.5	
4.5.1534	Nuova versione dell'SSM Agent (2.0.645.1)	
4.4.1503	Nuova versione dell'SSM Agent (2.0.633.0)	
4.3.1472	Nuova versione dell'SSM Agent (2.0.617.1)	
4.2.1442	Nuova versione dell'SSM Agent (2.0.599.0)	
4.1.1378	Nuova versione dell'SSM Agent (2.0.558.0)	

Versione	Dettagli	Data di rilascio
4.0.1343	• Il supporto per Run Command, State Manager, l' CloudWatch agente e il supporto per l'aggiunta al dominio sono stati spostati in un altro agente chiamato SSM Agent. SSM Agent verrà installato come parte dell'aggiornamento EC2Config. Per ulteriori informazioni, consulta EC2Config e AWS Systems Manager. • Se disponi di una configurazione del proxy su EC2Config, sarà necessario aggiornare le impostazioni proxy dell'SSM Agent prima dell'aggiornamento. Se non aggiorni le impostazioni del proxy, non potrai utilizzare il comando di esecuzione per gestire le tue istanze. Per evitarlo, prima di eseguire l'aggiornamento alla versione più recente, consulta Installazione e configurazione dell'SSM Agent sulle istanze Windows nella Guida per l'utente di AWS Systems Manager . • Se in precedenza hai abilitato CloudWatch l'integrazione sulle tue istanze utilizzando un file di configurazione locale (`AWS.EC2.Windows.CloudWatch.json`), dovrai configurare il file per funzionare con SSM Agent.	
3.19.1153	• Plugin di attivazione riabilitato per istanze con configurazione precedente. AWS KMS Salta l'attivazione per gli utenti BYOL. • Modifica il comportamento TRIM predefinito in modo che sia disabilitato durante l'operazione di formattazione del disco e aggiunto FormatWith TRIM per InitializeDisks sovrascrivere il plug-in con i dati utente.	

Versione	Dettagli	Data di rilascio
3.18.1118	• Introdotta una correzione per aggiungere instradamenti in modo affidabile all'adattatore di rete primario. • Aggiornamenti per migliorare il supporto per i servizi. AWS	
3.17.1032	• Apportate correzioni ai log di sistema duplicati, i quali vengono visualizzati quando i filtri impostano la stessa categoria. • Introdotte correzioni per evitare blocchi durante l'inizial izzazione del disco.	
3.16.930	Aggiunto il supporto per registrare l'evento "Window is Ready to use" (Windows pronto all'uso) all'avvio del log di eventi di Windows.	
3.15.880	Apportata una correzione per permettere il caricamento dell'outp ut di Run Command per Systems Manager in nomi di bucket S3 con un carattere "." (punto).	
3.14.786	Aggiunto il supporto per sovrascrivere le impostazioni del Initializ eDisks plugin. Ad esempio, per velocizzare l'inizializzazione del disco SSD, puoi disattivare temporaneamente TRIM specifica ndo nei dati utente come segue: < InitializeDrivesSettings >< > TRIM</ SettingsGroup ></ FormatWithout SettingsGroup InitializeDrivesSettings	
3.13.727	Run Command di Systems Manager – Apportate correzioni per elaborare in modo affidabile i comandi dopo il riavvio della finestra.	

Versione	Dettagli	Data di rilascio
3.12.649	• Introdotta una correzione per gestire correttamente il riavvio durante l'esecuzione di comandi e script. • Apportata una correzione per cancellare in modo affidabile l'esecuzione dei comandi. • Aggiunto il supporto per il caricamento (facoltativo) dei log MSI su S3, durante l'installazione di applicazioni tramite Run Command di Systems Manager.	
3.11.521	• Correzioni per abilitare la generazione dell'impronta RDP per Windows Server 2003. • Correzioni per includere l'offset UTC e timezone nelle linee log di EC2Config. • Supporto di Systems Manager per eseguire comandi Run Command in parallelo. • Roll back della modifica precedente per trasferire online i dischi partizionati.	
3.10.442	• Corretti gli errori di configurazione di Systems Manager durante l'installazione di applicazioni MSI. • Apportata una correzione per trasferire in modo affidabile online i dischi archiviazione. • Aggiornamenti per migliorare il supporto per i servizi. AWS	

Versione	Dettagli	Data di rilascio
3.9.359	• Introdotta una correzione nello script post Sysprep per lasciare la configurazione dell'aggiornamento di Windows nello stato predefinito. • Corretto il plug-in per la generazione della password per migliorare l'affidabilità delle impostazioni della policy per la password GPO. • Introdotta limitazione per l'autorizzazione al gruppo degli amministratori locali per la cartella log EC2Config/SSM. • Aggiornamenti per migliorare il supporto per AWS i servizi.	
3.8.294	• È stato risolto un problema CloudWatch che impediva il caricamento dei log quando non si trovavano sull'unità principale. • Migliorato il processo di inizializzazione del disco tramite l'aggiunta della logica di ripetizione. • È stata aggiunta una migliore gestione degli errori quando il SetPassword plug-in occasionalmente falliva durante la creazione dell'AMI. • Aggiornamenti per migliorare il supporto per AWS i servizi.	

Versione	Dettagli	Data di rilascio
3.7.308	• Apportate migliorie all'utilità ec2config-cli per i test config e per la risoluzione dei problemi di un'istanza. • Evita di aggiungere percorsi statici AWS KMS e servizi di metadati su un adattatore OpenVPN. • Risolto un problema a causa del quale l'esecuzione dei dati utente non stavano onorando il tag "persist". • Migliorata la gestione degli errori quando l'accesso alla console EC2 non è disponibile. • Aggiornamenti per migliorare il supporto per i servizi. AWS	
3.6.269	• Corretta l'affidabilità dell'attivazione di Windows affinché si utilizzi prima l'indirizzo locale del collegamento, ovvero 169.254.0.250/251, per l'attivazione di Windows tramite AWS KMS • Migliorata la gestione del proxy per Systems Manager, l'attivaz ione di Windows e gli scenari del collegamento del dominio • Corretto un problema secondo il quale doppie linee degli account utente non venivano aggiunte al file di risposta Sysprep	
3.5.228	• Risolto uno scenario in cui il CloudWatch plug-in poteva consumare CPU e memoria eccessive durante la lettura dei registri degli eventi di Windows • È stato aggiunto un collegamento alla documentazione di CloudWatch configurazione nell'interfaccia utente delle impostazioni di EC2Config	

Versione	Dettagli	Data di rilascio
3.4.212	• Aggiunte correzioni per l'utilizzo di EC2Config con VM Import. • Risolto il problema di denominazione del servizio sul programma d'installazione WiX.	
3.3.174	• Migliorata la gestione dell'eccezione per Systems Manager e gli errori di aggiunta del dominio • Apportata modifica per supportare la funzione Versioni multiple dello schema SSM di Systems Manager • Corretta la formattazione di dischi temporanei su Win2K3. • Apportata modifica per supportare la configurazione delle dimensioni del disco maggiori di 2TB. • Ridotto l'utilizzo della memoria virtuale attraverso l'imposta zione della modalità GC su predefinita. • Supporto per scaricare gli artefatti dal percorso UNC sui plug-in `aws:psModule` e `aws:application` . • Migliorato l'accesso per i plug-in dell'attivazione di Windows.	

Versione	Dettagli	Data di rilascio
3.2.97	• Apportati dei miglioramenti alle prestazioni tramite il ritardo del caricamento delle assembly SSM per Systems Manager. • Migliorata la gestione dell'eccezione per sysprep2008.xml difettoso. • Introdotto il supporto della riga di comando per la configura zione "Apply" di Systems Manager. • Apportata una modifica per supportare l'aggiunta del dominio nel caso in cui ci fosse una denominazione del computer in attesa. • Introdotto un supporto per parametri opzionali sul plug-in `aws:applications` . • Introdotto un supporto per la matrice di comando nel plug-in `aws:psModule` .	
3.0.54	• Abilitazione del supporto per Systems Manager. • Aggiunte automaticamente al dominio le istanze Windows di EC2 a una directory AWS tramite Systems Manager. • Configura e carica CloudWatch log/metriche tramite Systems Manager. • Installa PowerShell i moduli tramite Systems Manager. • Installazione di applicazioni MSI tramite Systems Manager.	

Versione	Dettagli	Data di rilascio
2.4.233	• Aggiunta attività programmata per ripristinare EC2Config dagli errori relativi ail startup del servizio. • Apportate migliorie ai messaggi di errore del log della console. • Aggiornamenti per migliorare il supporto per AWS i servizi.	
2.3.313	• È stato risolto un problema relativo all'elevato consumo di memoria in alcuni casi quando la funzionalità CloudWatch Registri è abilitata. • Corretto un bug relativo all'aggiornamento, così che le versioni di EC2Config precedenti alla 2.1.19 possono essere aggiornat e alle più recenti ora. • Aggiornata l'eccezione dell'apertura del porto COM affinché sia più facile da usare e utile sui log. • L'configServiceSettings interfaccia utente di Ec2 ha disabilitato il ridimensionamento e ha corretto l'attribuzione e il posiziona mento della visualizzazione della versione nell'interfaccia utente.	
2.2.12	• Gestito NullPointerException durante l'interrogazione di una chiave di registro per determinare lo stato di Windows Sysprep, che occasionalmente restituiva un valore nullo. • Liberate le risorse non gestite nel blocco finally.	
2.2.11	È stato risolto un problema nel CloudWatch plugin per la gestione delle righe di registro vuote.	

Versione	Dettagli	Data di rilascio
2.2.10	• Rimossa la configurazione delle impostazioni CloudWatch dei registri tramite l'interfaccia utente. • Consenti agli utenti di definire le impostazioni CloudWatch dei log nel `%ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` file per consentire miglioramenti futuri.	
2.2.9	Corretta l'eccezione non gestita e aggiunto il logging.	
2.2.8	• Corretta la verifica della versione del sistema operativo Windows sul programma di installazione di EC2Config per il supporto di Windows Server 2003 SP1 e versioni successive. • Corretta la gestione del valore nullo al momento della lettura di chiavi di registro, le quali erano correlate all'aggiornamento dei file config di Sysprep.	
2.2.7	• Aggiunto un supporto per EC2Config da eseguire durante l'esecuzione di Sysprep per Windows 2008 e versioni successive. • Migliorata la gestione e il logging dell'eccezione per una migliore diagnostica	
2.2.6	• È stato ridotto il carico sull'istanza e sui CloudWatch registri durante il caricamento degli eventi di registro. • Risolto un problema di aggiornamento a causa del quale il plug-in CloudWatch Logs non rimaneva sempre abilitato	

Versione	Dettagli	Data di rilascio
2.2.5	• È stato aggiunto il supporto per caricare i log su CloudWatch Log Service. • Risolto un problema di race condition sul plug-in Ec2Output RDPCert • Opzione di ripristino del servizio EC2Config modificata da cui riavviare TakeNoAction • Aggiunte maggiori informazioni di eccezione quando EC2Config si arresta in modo anomalo	
2.2.4	• È stato corretto un errore di battitura in .cmd PostSysprep • Corretto un bug per il quale EC2Config non si bloccava sul menu di avvio per OS2012+	

Versione	Dettagli	Data di rilascio
2.2.3	• Aggiunta l'opzione per installare EC2Config senza che il servizio cominci subito dopo l'installazione. Per utilizzarlo, avvia 'Ec2Install.exe start=false' dal prompt dei comandi • Aggiunto un parametro sul plug-in dello sfondo per controlla re l'aggiunta/rimozione dello sfondo. Per utilizzarlo, esegui 'Ec2 WallpaperInfo .exe set' o 'Ec2 .exe revert' dal prompt dei comandi WallpaperInfo • Aggiunto il controllo della chiave, restituisce le impostazi oni errate RealTimeIsUniversal della chiave di registro alla console RealTimeIsUniveral • Rimossa la dipendenza di EC2Config sulla cartella temp di Windows • Rimossa la dipendenza dall' UserData esecuzione su.Net 3.5	
2.2.2	• Aggiunta verifica per i comportamenti di blocco del servizio, al fine di controllare che le risorse siano state rilasciate • Risolto un problema legato a lunghi tempi di esecuzione al momento dell'aggiunta al dominio	

Versione	Dettagli	Data di rilascio
2.2.1	• Aggiornato il programma di esecuzione per permettere gli aggiornamenti delle versioni più datate • Risolto il WallpaperInfo bug Ec2 solo nell'ambiente.Net4.5 • Risolto un bug di rilevamento intermittente dei driver • Aggiunta un'opzione di installazione in modalità silenzios a. Esecuzione del file Ec2Install.exe con l'opzione "-q", ad esempio "Ec2Install.exe -q"	
2.2.0	• Aggiunto un supporto solo nell'ambiente di .Net4 e .Net4.5 • Aggiornato il programma di installazione	
2.1.19	• Aggiunto il supporto per l'etichettatura del disco temporane o quando si utilizza il driver di rete Intel (ad esempio tipo di istanza C3). Per ulteriori informazioni, consulta Rete avanzata su Amazon EC2. • Aggiunti supporti Nome origine AMI e Versione origine AMI all'output della console • Effettuate modifiche all'output della console per un'analisi e una formattazione coerenti • Aggiornato file di aiuto	

Versione	Dettagli	Data di rilascio
2.1.18	• Aggiunto l'oggetto WMI EC2Config per la notifica di completamento (-Namespace root\ Amazon -Class EC2_) ConfigService • Le prestazioni della query WMI al startup con un ampio utilizzo di log eventi, potrebbe causare un'attività elevata e prolungata della CPU durante l'esecuzione iniziale	
2.1.17	• È stato risolto UserData il problema di esecuzione con il riempimento del buffer Standard Output e Standard Error • Risolto un problema relativo all'impronta RDP errata che a volte compariva nell'output della console per >= Sistema operativo w2k8 • Console Output ora contiene 'RDPCERTIFICATE-Su bjectName: 'per Windows 2008+, che contiene il valore del nome del computer • Aggiunto D:\ nell'elenco a cascata della mappatura della lettera di unità • Spostato il pulsante Aiuto in alto a destra e modificate aspetto e sensazione • Aggiunto un collegamento del sondaggio sul feedback in alto a destra	

Versione	Dettagli	Data di rilascio
2.1.16	• La scheda Generali contiene un collegamento alla pagina per scaricare le versioni più recenti di EC2Config • La sovrapposizione dello sfondo del desktop ora è memorizza ta nella cartella Users Local Appdata anziché nella cartella My Documents per supportare il reindirizzamento MyDoc • Nome di MSSQLServer sincronizzato con il sistema sullo script Post-Sysprep (2008+) • Riordinata la cartella dell'applicazione (spostati i file sulla directory Plug-in e rimossi i file duplicati) • Modificato l'output del log di sistema (console): • *Modificati i formati di valore, nome e data per un'analisi più semplice (Inizia a migrare le dipendenze nel nuovo formato) • *Aggiunto lo stato del plugin «Ec2» SetPassword • *Aggiunta l'ora di inizio e di fine di Sysprep • Risolto un problema per il quale i dischi temporanei non venivano etichettati come 'Storage Temporary (Archiviazione temporanea)' per i sistemi operativi non in lingua inglese • Risolti errori relativi alla disinstallazione di EC2Config dopo aver eseguito Sysprep	

Versione	Dettagli	Data di rilascio
2.1.15	• Ottimizzate le richieste per il servizio di metadati • I metadati ora bypassano le impostazioni Proxy • I dischi temporanei etichettati come 'Temporary Storage (Archiviazione temporanea)' e Important.txt posti sul volume se trovati (solo driver Citrix PV). Per ulteriori informazioni, consulta Aggiornamento dei driver PV sulle istanze Windows. • I dischi temporanei assegnavano lettere di unità dalla Z alla A (solo driver Citrix PV) – questo incarico può essere sovrascri tto tramite il plug-in della mappatura della lettera di unità con le etichette del volume 'Temporary Storage X (Archiviazione temporanea X)', dove x è un numero compreso tra 0 e 25. • UserData ora viene eseguito immediatamente dopo «Windows is Ready»	
2.1.14	Risolti problemi relativi allo sfondo del desktop	
2.1.13	• Lo sfondo del desktop mostrerà l'hostname per impostazione predefinita • Rimossa dipendenza sul servizio Windows Time • Aggiunta route per i casi in cui più IP venivano assegnati a una singola interfaccia	

Versione	Dettagli	Data di rilascio
2.1.11	• Apportate modifiche al plug-in Ec2Activation • - Verifica lo stato di attivazione ogni 30 giorni • - Se mancano 90 giorni alla scadenza del periodo di grazia (su 180 giorni), riprova l'attivazione	
2.1.10	• La sovrapposizione dello sfondo del desktop non persiste più con Sysprep o con l'arresto senza Sysprep • L'opzione Userdata da eseguire su ogni servizio inizia con <persist>true</persist> • Posizione e nome modificati di/.cmd in /Scripts/ DisableWi nUpdate .cmd PostSysprep • La password dell'amministratore è impostata per non scadere per impostazione predefinita in /Scripts/ .cmd PostSysprep • La disinstallazione rimuoverà lo script EC2Config da c: \windows\setup\script\ .cmd PostSysprep CommandComplete • Aggiunta una route che supporta i parametri dell'interfaccia personalizzata	
2.1.9	UserData L'esecuzione non è più limitata a 3851 caratteri	

Versione	Dettagli	Data di rilascio
2.1.7	• La versione del sistema operativo e l'identificatore della lingua sono scritti nella console • La versione di EC2Config è scritta nella console • La versione del driver PV è scritta nella console • Rilevamento della verifica dei bug e dell'output per la console al prossimo riavvio, se riscontrati • Aggiunta opzione su config.xml così che le credenziali di Sysprep persistano • Aggiunta logica di ripetizione dei tentativi route nel caso in cui ENI non sia disponibile all'avvio • Il PID di esecuzione dei dati utente è scritto nella console • La lunghezza minima della password generata viene recuperata dal GPO • Impostato l'avvio del servizio affinché compia 3 tentativi • Aggiunti esempi di file.ps1 e DownloadFile S3_Upload file.ps1 nella cartella /Scripts	

Versione	Dettagli	Data di rilascio
2.1.6	• Informazioni della versione aggiunte sulla scheda Generali • Rinominata la scheda Bundle in Immagine • Semplificato il processo di specificazione della password; spostata la password dell'interfaccia utente dalla scheda Generali alla scheda Immagine • Rinominata la scheda Impostazioni disco in archiviazione • Aggiunta una scheda Supporto con strumenti comuni per la risoluzione di problemi • Impostato `sysprep.ini` di Windows Server 2003 per estendere la partizione del sistema operativo per impostazi one predefinita • Aggiunto l'indirizzo IP privato allo sfondo • Indirizzo IP privato mostrato sullo sfondo • Aggiunta logica di ripetizione dei tentativi per l'output della console • Risolto un problema relativo all'eccezione della porta Com per l'accessibilità dei metadati – che causava l'interruzione di EC2Config prima che venisse mostrato l'output della console • Introdotte verifiche dello stato di attivazione per ogni avvio – si attiva se necessario • Risolto un problema dei percorsi relativi – riscontrato all'esecu zione manuale della scelta rapida dello sfondo dalla cartella di startup; diretto a Administrator/logs	

Versione	Dettagli	Data di rilascio
	• Corretto il colore dello sfondo predefinito per l'utente di Windows Server 2003 (oltre che per l'amministratore)	

Versione	Dettagli	Data di rilascio
2.1.2	• Time stamp della console su UTC (Zulù) • Rimosso l'aspetto del collegamento ipertestuale sulla scheda Sysprep • Aggiunta la caratteristica che permette di espandere in maniera dinamica il Volume root al primo avvio su Windows 2008+ • Quando l'opzione per l'impostazione della password è abilitata , anche EC2Config ora viene abilitato per impostare la password • EC2Config verifica lo stato di attivazione prima di eseguire Sysprep (vengono mostrati avvisi se questo non è attivato) • Per impostazione predefinita, `Sysprep.xml` su Windows Server 2003 ora imposta il fuso orario su UTC anziché sul fuso orario del Pacifico • Randomizzati i server di attivazione • Rinominata la scheda Mappatura del drive su Impostazioni disco • Spostati gli elementi dell'interfaccia utente per inizializzare i drive dalla scheda Generali a Impostazioni disco • Il pulsante Aiuto indirizza ora al file di aiuto HTML • Aggiornato il file di aiuto HTML con modifiche • Aggiornato il testo 'Note' per le mappature della lettera di unità •	

Versione	Dettagli	Data di rilascio
	È stato aggiunto InstallUpdates .ps1 alla cartella /Scripts per automatizzare le patch e la pulizia prima di Sysprep	
2.1.0	• Lo sfondo del desktop mostra le informazioni dell'istanza per impostazione predefinita al primo accesso (senza disconnettersi e riconnettersi) • PowerShell può essere eseguito dai dati utente racchiudendo il codice con<powershell></powershell>	

Iscrizione alle notifiche del servizio EC2Config

Amazon SNS può avvisarti in caso di pubblicazione di nuove versioni del servizio EC2Config. Utilizza la procedura seguente per effettuare l'iscrizione a queste notifiche.

Per effettuare l'iscrizione alle notifiche EC2Config

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. Devi selezionare questa regione perché le notifiche SNS per le quali hai effettuato l'iscrizione sono state create in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Create subscription (Crea sottoscrizione) segui questi passaggi:
   a. Per ARN argomento, usa il seguente nome della risorsa Amazon (ARN):

      ```
      arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
      ```

   b. In Protocol (Protocollo), scegli `Email`.
   c. In Endpoint digita l'indirizzo e-mail utilizzabile per ricevere le notifiche.
   d. Scegli Create Subscription (Crea sottoscrizione).

6. Riceverai un'e-mail in cui ti verrà chiesto di confermare l'iscrizione. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

Quando viene rilasciata una nuova versione del servizio EC2Config, inviamo notifiche ai sottoscrittori. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Per annullare l'iscrizione alle notifiche di EC2Config

1. Aprire la console Amazon SNS.
2. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
3. Selezionare l'iscrizione, quindi scegliere Actions (Operazioni), Delete subscriptions (Cancella iscrizioni). Quando viene richiesta la conferma, selezionare Delete (Cancella).

Risoluzione dei problemi relativi al servizio EC2Config

Le informazioni seguenti possono essere utili per risolvere i problemi con il servizio EC2Config

Aggiornamento di EC2Config su un'istanza irraggiungibile

Utilizza la procedura seguente per aggiornare il servizio EC2Config su un'istanza Windows Server inaccessibile tramite desktop remoto.

Per aggiornare EC2Config su un'istanza Windows supportata da Amazon EBS alla quale non riesci a connetterti

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Individua l'istanza interessata. Selezionare l'istanza e scegliere Instance state (Stato istanza), quindi Stop (Arresta).

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

4. Scegli Launch instances (Avvia le istanze) e crea un'istanza temporanea `t2.micro` nella stessa Zona di disponibilità dell'istanza interessata. Utilizza un'AMI differente rispetto a quella utilizzata per lanciare l'istanza interessata.

   > **Important**
   >
   > Se non crei l'istanza nella stessa Zona di disponibilità dell'istanza interessata, non potrai collegare il volume root dell'istanza interessata sulla nuova istanza.

5. Nella console EC2, scegliere Volumes (Volumi).
6. Individua il volume root dell'istanza interessata. Scollega il volume e collega il volume all'istanza temporanea creata in precedenza. Collegala con il nome del dispositivo predefinito (xvdf).
7. Utilizzare Desktop remoto per collegarsi all'istanza temporanea, quindi usare l'utilità Disk Management (Gestione disco) per rendere il volume disponibile per l'uso.
8. Scaricare la versione più recente del servizio EC2Config. Estrarre i file dal file `.zip` nella directory `Temp` sull'unità collegata.
9. Nell'istanza temporanea, aprire la finestra di dialogo Run (Esegui), digitare **`regedit`** e premere Invio.
10. Scegli `HKEY_LOCAL_MACHINE`. Dal menu File scegliere Load Hive (Carica Hive). Scegli il drive, quindi individua e apri il file seguente: `Windows\System32\config\SOFTWARE`. Quando richiesto, specifica un nome chiave.
11. Selezionare la chiave appena caricata e passare a `Microsoft\Windows\CurrentVersion`. Scegli la chiave `RunOnce`. Se questa chiave non esiste, scegliere `CurrentVersion` dal menu contestuale (pulsante destro del mouse), quindi New (Nuovo) e selezionare Key (Chiave). Rinomina la chiave `RunOnce`.
12. Dal menu contestuale (pulsante destro del mouse) scegliere la chiave `RunOnce`, quindi New (Nuovo) e selezionare String Value (Valore stringa). Immettere il nome `Ec2Install` e i dati `C:\Temp\Ec2Install.exe /quiet`.
13. Scegli la chiave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`. Dal menu contestuale (pulsante destro del mouse) scegliere New (Nuovo), quindi selezionare String Value (Valore stringa). Immettere **`AutoAdminLogon`** come nome e **`1`** come dati valore.
14. Scegli la chiave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon>`. Dal menu contestuale (pulsante destro del mouse) scegliere

New (Nuovo), quindi selezionare String Value (Valore stringa). Immettere **`DefaultUserName`** come nome e **`Administrator`** come dati valore.

15. Scegli la chiave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`. Dal menu contestuale (pulsante destro del mouse) scegliere New (Nuovo), quindi selezionare String Value (Valore stringa). Digitare **`DefaultPassword`** come nome e inserire una password nei dati valore.
16. Nel riquadro di navigazione del Registry editor, scegli la chiave temporanea che hai creato alla prima apertura del Registry Editor.
17. Dal menu File, scegliere Unload Hive (Scarica Hive).
18. Nell'utilità Disk Management (Gestione disco), scegliere l'unità collegata in precedenza, aprire il menu contestuale (pulsante destro del mouse) e scegliere Offline.
19. Nella console Amazon EC2 distaccare il volume interessato dall'istanza temporanea e ricollegalo all'istanza con il nome del dispositivo console, `/dev/sda1`. Devi specificare questo nome del dispositivo per indicare il volume come volume root.
20. Arresta e avvia le istanze Amazon EC2 l'istanza.
21. All'avvio dell'istanza, verificare il log di sistema e accertarsi di visualizzare il messaggio Windows is ready to use (Windows è pronto per l'utilizzo).
22. Apri il Registry Editor e scegli `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. Elimina le chiavi String Value che hai creato in precedenza: AutoAdminLogon, DefaultUserName, e DefaultPassword.
23. Cancella o interrompi l'istanza temporanea creata durante questa procedura.

Usa EC2 Fast Launch per le tue istanze Windows

Ogni istanza Windows Amazon EC2 deve superare i passaggi di avvio standard del sistema operativo Windows (OS), che includono diversi riavvii e spesso richiedono 15 minuti o più per essere completati. Le AMI Windows Server di Amazon EC2 con la funzionalità EC2 Fast Launch abilitata completano alcuni di questi passaggi e si riavviano in anticipo per ridurre il tempo necessario per avviare un'istanza.

Quando configuri un'AMI Windows Server per EC2 Fast Launch, Amazon EC2 crea un set di snapshot preconfigurati da utilizzare per un avvio più rapido, come segue.

1. Amazon EC2 avvia una serie di istanze t3 temporanee, in base alle tue impostazioni.

2. Quando ogni istanza temporanea completa i passaggi di avvio standard, Amazon EC2 crea uno snapshot con pre-provisioning dell'istanza. Archivia lo snapshot nel tuo bucket Amazon S3.
3. Quando lo snapshot è pronto, Amazon EC2 termina l'istanza t3 associata per mantenere i costi delle risorse il più bassi possibile.
4. La prossima volta che Amazon EC2 avvia un'istanza dall'AMI abilitata per EC2 Fast Launch, utilizza una delle istantanee per ridurre significativamente il tempo necessario per l'avvio.

Amazon EC2 ripristina automaticamente le istantanee disponibili in quanto le utilizza per avviare istanze dall'AMI EC2 Fast Launch abilitata.

Qualsiasi account che abbia accesso a un'AMI con EC2 Fast Launch abilitato può beneficiare di tempi di avvio ridotti. Quando il proprietario dell'AMI concede l'accesso all'avvio delle istanze, gli snapshot pre-assegnati provengono dall'account del proprietario dell'AMI.

Se un'AMI che supporta EC2 Fast Launch è condivisa con te, puoi abilitare o disabilitare tu stesso l'avvio più rapido sull'AMI condivisa. Se abiliti un'AMI condivisa per EC2 Fast Launch, Amazon EC2 crea gli snapshot preimpostati direttamente nel tuo account. Se esaurisci gli snapshot nel tuo account, puoi comunque utilizzare gli snapshot dall'account del proprietario dell'AMI.

> **Note**
>
> EC2 Fast Launch elimina le istantanee pre-assegnate non appena vengono utilizzate da un lancio per ridurre al minimo i costi di archiviazione e impedirne il riutilizzo. Tuttavia, se gli snapshot eliminati soddisfano una regola di conservazione, il Cestino li conserva automaticamente. Ti consigliamo di esaminare l'ambito delle regole di conservazione del Cestino in modo che ciò non accada. Per ulteriori informazioni, consulta Considerazioni. Questa funzionalità è diversa dal ripristino rapido degli snapshot EBS. Devi abilitare esplicitamente il ripristino rapido degli snapshot EBS per ogni snapshot, ciò prevede costi associati.

Il video seguente mostra come configurare l'AMI Windows per un avvio più rapido con una rapida panoramica dei termini chiave correlati e delle relative definizioni: Avvio delle istanze EC2 Windows fino al 65% più velocemente. AWS

Costi delle risorse

Non sono previsti costi di servizio per configurare le AMI Windows per EC2 Fast Launch. Tuttavia, i prezzi standard si applicano a tutte le AWS risorse sottostanti utilizzate da Amazon EC2. Per ulteriori informazioni sui costi delle risorse associate e su come gestirli, consulta Gestisci i costi delle risorse con EC2 Fast Launch.

Indice

Termini chiave

La funzionalità EC2 Fast Launch utilizza i seguenti termini chiave:

Snapshot con pre-provisioning

Un'istantanea di un'istanza che è stata avviata da un'AMI Windows con EC2 Fast Launch abilitato e che ha completato i seguenti passaggi di avvio di Windows, riavviando se necessario.

- Specializzazione di Sysprep
- Windows Out of Box Experience (OOBE)

Una volta completati questi passaggi, EC2 Fast Launch arresta l'istanza e crea un'istantanea che viene successivamente utilizzata per un avvio più rapido dall'AMI, in base alla configurazione.

Frequenza di avvio

Controlla il numero di snapshot con pre-provisioning che Amazon EC2 può avviare entro il periodo di tempo specificato. Quando abiliti EC2 Fast Launch per la tua AMI, Amazon EC2 crea il set iniziale di snapshot preconfigurati in background. Ad esempio, se la frequenza di avvio è impostata su cinque lanci all'ora, che è l'impostazione predefinita, EC2 Fast Launch crea un set iniziale di cinque snapshot preconfigurati.

Quando Amazon EC2 avvia un'istanza da un'AMI con EC2 Fast Launch abilitato, utilizza una delle istantanee predisposte per ridurre i tempi di avvio. Man mano che gli snapshot vengono utilizzati, vengono automaticamente riforniti, fino al numero specificato dalla frequenza di lancio.

Se è previsto un picco del numero di istanze avviate dall'AMI, ad esempio durante un evento speciale, è possibile aumentare la frequenza di lancio in anticipo per coprire le istanze aggiuntive necessarie. Quando la frequenza di avvio torna alla normalità, è possibile regolarla nuovamente.

Quando avviene un numero di avvii superiore al previsto, potresti utilizzare tutti gli snapshot con pre-povisioning disponibili. Ciò non causa il fallimento di alcun avvio. Tuttavia, può comportare che alcune istanze passino attraverso il processo di avvio standard, fino a quando non è possibile reintegrare gli snapshot.

Numero di risorse di destinazione

Il numero di snapshot preconfigurati da tenere a portata di mano per un'AMI Amazon EC2 Windows Server con EC2 Fast Launch abilitato.

Numero massimo di avvi paralleli

Controlla quante istanze Amazon EC2 può avviare contemporaneamente per creare gli snapshot preimpostati per EC2 Fast Launch. Se il numero di risorse di destinazione è superiore al numero massimo di avvii paralleli configurato, Amazon EC2 avvia il numero di istanze specificato dall'impostazione Numero massimo di avvii paralleli per la creazione degli snapshot. Quando queste istanze completano il processo, Amazon EC2 acquisisce lo snapshot e arresta l'istanza. Quindi continua ad avviare altre istanze fino a quando il numero totale di snapshot disponibili non raggiunge il numero di risorse di destinazione. Il valore in Numero massimo di avvi paralleli deve essere pari o superiore a 6.

Prerequisiti per EC2 Fast Launch

Prima di configurare EC2 Fast Launch, verifica di aver soddisfatto i seguenti prerequisiti necessari per creare istantanee per le AMI del tuo computer: Account AWS

- Se non utilizzi un modello di avvio per configurare le impostazioni, assicurati che sia configurato un VPC predefinito per la regione in cui utilizzi EC2 Fast Launch.

> **Note**
>
> Se elimini accidentalmente il tuo VPC predefinito nella regione in cui intendi configurare EC2 Fast Launch, puoi creare un nuovo VPC predefinito in quella regione. Per ulteriori

informazioni, consulta Creazione di un VPC predefinito nella Guida per l'utente di Amazon VPC.

- Per specificare un VPC non predefinito, devi utilizzare un modello di avvio quando configuri l'avvio rapido di Windows. Per ulteriori informazioni, consulta Utilizza un modello di lancio quando configuri EC2 Fast Launch.
- Se il tuo account include una policy che applica IMDSv2 per istanze Amazon EC2, devi creare un modello di avvio che specifichi la configurazione dei metadati per applicare IMDSv2.
- Le AMI EC2 Fast Launch private devono supportare l'esecuzione di script di dati utente.
- Per configurare EC2 Fast Launch per un'AMI, è necessario creare l'AMI utilizzando l'Sysprepopzione shutdown. La funzionalità EC2 Fast Launch attualmente non supporta le AMI create da un'istanza in esecuzione.

  Per creare un'AMI tramite Sysprep, consultare Creare un'AMI con Windows Sysprep.
- La quota predefinita per il Numero massimo di avvi paralleli su tutte le AMI in un Account AWS è di 40 per regione. Puoi richiedere un aumento delle Service Quotas per il tuo account, come indicato di seguito.

  1. Accedere AWS Management Console e aprire la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/.
  2. Nel riquadro di navigazione, scegli Servizi AWS.
  3. Nella barra di ricerca, inserisci `EC2 Fast Launch` e seleziona il risultato.
  4. Seleziona il link per `Parallel instance launches`. Viene visualizzata la pagina dei dettagli della quota di servizio Avvii di istanze parallele.
  5. Scegliere Request quota increase (Richiedi aumento di quota).

  Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente di Service Quotas.

Configura le impostazioni EC2 Fast Launch per la tua AMI Amazon EC2 Windows Server

Puoi configurare le AMI EC2 Fast Launch for Windows di cui sei proprietario o le AMI condivise con te dall'API AWS Management Console, dagli SDK o (). CloudFormation AWS Command Line Interface AWS CLI Prima di configurare EC2 Fast Launch, verifica che l'AMI soddisfi tutti i prerequisiti

necessari per creare le istantanee predisposte. Per ulteriori informazioni, consulta Prerequisiti per EC2 Fast Launch.

Quando abiliti EC2 Fast Launch, Amazon EC2 verifica che tu disponga delle autorizzazioni necessarie per avviare le istanze dall'AMI e dal modello di avvio specificati (se forniti), incluse le autorizzazioni per le AMI crittografate. Per evitare errori durante il processo di avvio dell'istanza, il servizio convalida le autorizzazioni prima che EC2 Fast Launch sia abilitato. Se non disponi delle autorizzazioni richieste, il servizio restituisce un errore e non abilita EC2 Fast Launch.

Le seguenti sezioni illustrano i passaggi di configurazione per la console Amazon EC2 e. AWS CLI

Abilita EC2 Fast Launch

Per abilitare EC2 Fast Launch, scegli la scheda che corrisponde al tuo ambiente e segui i passaggi.

> **Note**
>
> Prima di modificare queste impostazioni, assicurati che l'AMI e la regione in cui è eseguita soddisfino tutti Prerequisiti per EC2 Fast Launch.

Console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di spostamento, in Images (Immagini), scegliere AMI.
3. Selezionare l'AMI da aggiornare selezionando la casella di controllo accanto al Name (Nome).
4. Dal menu Operazioni sopra l'elenco delle AMI, scegli Configura avvio rapido. Si apre la pagina Configure fast launch, in cui puoi configurare le impostazioni per EC2 Fast Launch.
5. Per iniziare a utilizzare snapshot con pre-provisioning per avviare più rapidamente le istanze dall'AMI Windows, seleziona la casella di controllo Abilita avvio rapido di Windows.
6. Dall'elenco a discesa Set anticipated launch frequency (Imposta la frequenza di lancio prevista), scegliere un valore per specificare il numero di snapshot creati e mantenuti per coprire il volume di avvio dell'istanza previsto.
7. Una volta completate le modifiche, scegliere Save (Salva).

> **Note**
>
> Se occorre utilizzare un modello di avvio per specificare un VPC non predefinito o per configurare impostazioni di metadati per IMDSv2, consulta Utilizza un modello di lancio quando configuri EC2 Fast Launch.

AWS CLI

Il enable-fast-launch comando richiama l'operazione dell'EnableFastLaunchAPI Amazon EC2.

Sintassi:

```
aws ec2 enable-fast-launch \
  --image-id <value> \
  --resource-type <value> \ (optional)
  --snapshot-configuration <value> \ (optional)
  --launch-template <value> \ (optional)
  --max-parallel-launches <value> \ (optional)
  --dry-run | --no-dry-run \  (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Esempio:

L'enable-fast-launchesempio seguente abilita EC2 Fast Launch per l'AMI specificata, avviando sei istanze parallele per il pre-provisioning. `ResourceType` è impostato su `snapshot`, che è il valore di default.

```
aws ec2 enable-fast-launch \
         --image-id ami-01234567890abcedf  \
         --max-parallel-launches 6 \
         --resource-type snapshot
```

Output:

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {
```

```
            "TargetResourceCount": 10
        },
        "LaunchTemplate": {},
        "MaxParallelLaunches": 6,
        "OwnerId": "0123456789123",
        "State": "enabling",
        "StateTransitionReason": "Client.UserInitiated",
        "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
    }
```

PowerShell

Il Enable-EC2FastLaunch cmdlet richiama l'operazione dell'API Amazon EnableFastLaunchEC2 per abilitare EC2 Fast Launch sull'AMI Windows.

Sintassi:

```
Enable-EC2FastLaunch
      -ImageId <String>
      -LaunchTemplate_LaunchTemplateId <String>
      -LaunchTemplate_LaunchTemplateName <String>
      -MaxParallelLaunch <Int32>
      -ResourceType <String>
      -SnapshotConfiguration_TargetResourceCount <Int32>
      -LaunchTemplate_Version <String>
      -Select <String>
      -PassThru <SwitchParameter>
      -Force <SwitchParameter>
```

Esempio:

L'Enable-EC2FastLaunchesempio seguente abilita EC2 Fast Launch per l'AMI specificata, avviando sei istanze parallele per il pre-provisioning. `ResourceType` è impostato su `snapshot`, che è il valore di default.

```
Enable-EC2FastLaunch `
 -ImageId ami-01234567890abcedf `
 -MaxParallelLaunch 6 `
 -Region us-west-2 `
 -ResourceType snapshot
```

Output:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
State                 : enabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:24:11 PM
```

Disattiva EC2 Fast Launch

Per disabilitare EC2 Fast Launch, scegli la scheda che corrisponde al tuo ambiente e segui i passaggi.

> **Note**
>
> Prima di modificare queste impostazioni, assicurati che l'AMI e la regione in cui è eseguita soddisfino tutti Prerequisiti per EC2 Fast Launch.

Console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di spostamento, in Images (Immagini), scegliere AMI.
3. Selezionare l'AMI da aggiornare selezionando la casella di controllo accanto al Name (Nome).
4. Dal menu Operazioni sopra l'elenco delle AMI, scegli Configura avvio rapido. Si apre la pagina Configure fast launch, in cui puoi configurare le impostazioni per EC2 Fast Launch.
5. Deseleziona la casella di controllo Abilita avvio rapido per Windows per disabilitare EC2 Fast Launch e rimuovere le istantanee preimpostate. Ciò comporta d'ora in poi che AMI utilizzi il processo di lancio standard per ogni istanza.

> **Note**
>
> Quando disabiliti l'ottimizzazione delle immagini di Windows, tutti gli snapshot con pre-provisioning esistenti vengono eliminati automaticamente. Questo passaggio deve essere completato prima di poter ricominciare a utilizzare la funzione.

6. Una volta completate le modifiche, scegliere Save (Salva).

AWS CLI

Il disable-fast-launch comando richiama l'operazione dell'DisableFastLaunchAPI Amazon EC2.

Sintassi:

```
aws ec2 disable-fast-launch \
  --image-id <value> \
  --force | --no-force \ (optional)
  --dry-run | --no-dry-run \ (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Esempio:

L'disable-fast-launchesempio seguente disabilita EC2 Fast Launch sull'AMI specificata e pulisce le istantanee preconfigurate esistenti.

```
aws ec2 disable-fast-launch \
         --image-id ami-01234567890abcedf
```

Output:

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {},
     "LaunchTemplate": {
         "LaunchTemplateId": "lt-01234567890abcedf",
         "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
```

```
        "Version": "1"
    },
    "MaxParallelLaunches": 6,
    "OwnerId": "0123456789123",
    "State": "disabling",
    "StateTransitionReason": "Client.UserInitiated",
    "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
}
```

PowerShell

Il Disable-EC2FastLaunch cmdlet richiama l'operazione dell'API Amazon DisableFastLaunchEC2.

Sintassi:

```
Disable-EC2FastLaunch
      -ImageId <String>
      -ForceStop <Boolean>
      -Select <String>
      -PassThru <SwitchParameter>
      -Force <SwitchParameter>
```

Esempio:

L'Disable-EC2FastLaunchesempio seguente disabilita EC2 Fast Launch sull'AMI specificata e pulisce le istantanee preconfigurate esistenti.

```
Disable-EC2FastLaunch -ImageId ami-01234567890abcedf
```

Output:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : disabling
StateTransitionReason : Client.UserInitiated
```

```
StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Utilizza un modello di lancio quando configuri EC2 Fast Launch

Con un modello di avvio puoi configurare una serie di parametri di avvio che Amazon EC2 utilizza ogni volta che avvia un'istanza da tale modello. Puoi specificare elementi come un'AMI da utilizzare per l'immagine di base, tipi di istanza, storage, impostazioni di rete e altro.

I modelli di avvio sono facoltativi, tranne nei casi specifici seguenti, in cui devi utilizzare un modello di avvio per l'AMI Windows quando configuri un avvio più rapido:

- È necessario utilizzare un modello di avvio per specificare un VPC non predefinito per l'AMI Windows.
- Se il tuo account include una policy che applica IMDSv2 per istanze Amazon EC2, devi creare un modello di avvio che specifichi la configurazione dei metadati per applicare IMDSv2.

  Utilizza il modello di avvio che include la configurazione dei metadati dalla console EC2 o quando esegui il enable-fast-launchcomando o richiami AWS CLI l'EnableFastLaunchazione API.

Amazon EC2 EC2 Fast Launch non supporta la seguente configurazione quando utilizzi un modello di lancio. Se utilizzi un modello di lancio per EC2 Fast Launch, non devi specificare nessuno dei seguenti elementi:

- Script di dati utente
- Termination protection (Protezione da cessazione)
- Metadati disabilitati
- Opzione Spot
- Comportamento di spegnimento che chiude l'istanza
- Tag di risorse per interfacce di rete, grafica elastica o richieste di istanze Spot

Specifica un VPC non predefinito

Fase 1: creazione di un modello di avvio

Crea un modello di avvio che specifica i seguenti dettagli per le tue istanze di Windows:

- La sottorete VPC.

- Un tipo di istanza di `t3.xlarge`.

Per ulteriori informazioni, consulta Creazione di un modello di avvio.

Fase 2: Specificate il modello di lancio per la vostra AMI EC2 Fast Launch

Scegli la scheda che corrisponde al tuo processo:

Console

Per specificare il modello di lancio per EC2 Fast Launch da AWS Management Console, segui questi passaggi:

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di spostamento, in Images (Immagini), scegliere AMI.
3. Selezionare l'AMI da aggiornare selezionando la casella di controllo accanto al Name (Nome).
4. Dal menu Operazioni sopra l'elenco delle AMI, scegli Configura avvio rapido. Si apre la pagina Configure fast launch, in cui è possibile configurare le impostazioni per EC2 Fast Launch.
5. La casella Modello di avvio esegue una ricerca filtrata che trova modelli di avvio nel tuo account nella regione corrente che corrispondono al testo che hai inserito. Specifica parte o tutto il nome o l'ID del modello di avvio nella casella per visualizzare un elenco di modelli di avvio corrispondenti. Ad esempio, se inserisci `fast` nella casella, Amazon EC2 trova tutti i modelli di avvio nel tuo account nella regione corrente che includono "fast" nel nome.

   Per creare un nuovo modello di avvio, puoi scegliere Crea modello di avvio.
6. Quando selezioni un modello di avvio, Amazon EC2 mostra la versione predefinita per tale modello nella casella Versione modello origine. Per specificare una versione diversa, evidenzia quella predefinita per sostituirla e inserisci il numero di versione desiderato nella casella.
7. Una volta completate le modifiche, scegliere Save (Salva).

AWS CLI, API

Per specificare il modello di avvio per EC2 Fast Launch da AWS CLI, specifica il nome o l'ID del modello di avvio nel `--launch-template` parametro quando esegui il enable-fast-launchcomando in. AWS CLI

Per specificare il modello di avvio per EC2 Fast Launch in una richiesta API, specifica il nome o l'ID del modello di lancio nel `LaunchTemplate` parametro quando richiami l'azione EnableFastLaunchAPI.

Per ulteriori informazioni sui modelli di avvio EC2, consulta Avvio di un'istanza da un modello di avvio.

Crea un'immagine personalizzata con EC2 Fast Launch abilitato

Amazon EC2 EC2 Fast Launch si integra con EC2 Image Builder per aiutarti a creare immagini personalizzate con EC2 Fast Launch abilitato. Per ulteriori informazioni, consulta Creazione di impostazioni di distribuzione per un'AMI Windows con EC2 Fast Launch abilitato (AWS CLI)nella Guida per l'utente di EC2 Image Builder.

Visualizza le AMI con EC2 Fast Launch abilitato

È possibile utilizzare il describe-fast-launch-imagescomando nel cmdlet o il AWS CLIGet-EC2FastLaunchImageTools for PowerShell Cmdlet per ottenere dettagli sulle AMI che hanno EC2 Fast Launch abilitato.

Amazon EC2 fornisce i seguenti dettagli per ogni AMI Windows restituita nei risultati:

- L'ID immagine per un'AMI con EC2 Fast Launch abilitato.
- Il tipo di risorsa utilizzato per il pre-provisioning dell'AMI associata di Windows. Valore supportato: `snapshot`.
- Configurazione snapshot, ovvero un gruppo di parametri per la configurazione del pre-provisioning dell'AMI di Windows associata utilizzando gli snapshot.
- Avviare le informazioni sul modello, inclusi l'ID, il nome e la versione del modello di avvio utilizzato dall'AMI associata quando avvia le istanze Window da snapshot pre-provisioning.
- Il numero massimo di istanze che possono essere avviate contemporaneamente per la creazione di risorse.
- L'ID proprietario per l'AMI associata. Questo campo non è compilato per le AMI condivise con te.

- Lo stato attuale di EC2 Fast Launch per l'AMI associata. I valori supportati includono: `enabling | enabling-failed | enabled | enabled-failed | disabling | disabling-failed`.

> **Note**
>
> Puoi anche controllare lo stato corrente visualizzato nella pagina Gestisci ottimizzazione immagini nella console EC2, come Stato ottimizzazione immagine.

- Il motivo per cui EC2 Fast Launch per l'AMI associata è passato allo stato attuale.
- L'ora in cui EC2 Fast Launch per l'AMI associata è passato allo stato corrente.

Scegliere la scheda che corrisponde all'ambiente della riga di comando:

AWS CLI

Il describe-fast-launch-images comando richiama l'operazione dell'DescribeFastLaunchImagesAPI Amazon EC2.

Sintassi:

```
aws ec2 describe-fast-launch-images \
 --image-ids <value> \ (optional)
 --filters <value> \ (optional)
 --dry-run | --no-dry-run \ (optional)
 --cli-input-json <value> \ (optional)
 --starting-token <value> \ (optional)
 --page-size <value> \ (optional)
 --max-items <value> \ (optional)
 --generate-cli-skeleton <value> \ (optional)
```

Esempio:

L'describe-fast-launch-imagesesempio seguente descrive i dettagli di ciascuna delle AMI dell'account configurate per EC2 Fast Launch. In questo esempio, solo un'AMI nell'account è configurata per EC2 Fast Launch.

```
aws ec2 describe-fast-launch-images
```

Output:

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
            "SnapshotConfiguration": {},
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-01234567890abcedf",
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

Tools for PowerShell

Il Get-EC2FastLaunchImage cmdlet richiama l'operazione dell'API Amazon DescribeFastLaunchImagesEC2.

Sintassi:

```
Get-EC2FastLaunchImage
-Filter <Filter[]>
-ImageId <String[]>
-MaxResult <Int32>
-NextToken <String>
-Select <String>
-NoAutoIteration <SwitchParameter>
```

Esempio:

L'Get-EC2FastLaunchImageesempio seguente descrive i dettagli per ciascuna delle AMI dell'account configurate per EC2 Fast Launch. In questo esempio, solo un'AMI nell'account è configurata per EC2 Fast Launch.

```
Get-EC2FastLaunchImage -ImageId ami-01234567890abcedf
```

Output:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : enabled
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:54:43 PM
```

Gestisci i costi delle risorse con EC2 Fast Launch

Non sono previsti costi di servizio per configurare le AMI Windows per EC2 Fast Launch. Tuttavia, quando abiliti EC2 Fast Launch per un'AMI Windows Amazon EC2, si applicano i prezzi standard per le risorse AWS sottostanti utilizzate da Amazon EC2 per preparare e archiviare gli snapshot preimpostati. Puoi configurare i tag di allocazione dei costi per monitorare e gestire i costi associati alle risorse EC2 Fast Launch. Per ulteriori informazioni su come configurare i tag per l'allocazione dei costi, consulta Tieni traccia dei costi di EC2 Fast Launch sulla tua bolletta.

L'esempio seguente mostra come potrebbero essere allocati i costi associati alle istantanee di EC2 Fast Launch.

Scenario di esempio: l'azienda AtoZ Example dispone di un'AMI Windows con un volume root EBS di 50 GiB. Abilitano EC2 Fast Launch per le loro AMI e impostano il numero di risorse target su cinque. Nel corso di un mese, l'utilizzo di EC2 Fast Launch per le loro AMI costa loro circa $5,00 e la ripartizione dei costi è la seguente:

1. Quando AtoZ Example abilita EC2 Fast Launch, Amazon EC2 lancia cinque piccole istanze. Ogni istanza viene eseguita attraverso le fasi di avvio di Sysprep e OOBE di Windows, riavviando secondo necessità. Ciò richiede diversi minuti per ogni istanza (il tempo può variare, in base a quanto è occupata la regione o la zona di disponibilità (AZ) e alle dimensioni dell'AMI).

Costi

- Costi di runtime dell'istanza (o runtime minimo, se applicabile): cinque istanze
- Costi dei volumi: cinque volumi root EBS

2. Al termine del processo di pre-provisioning, Amazon EC2 acquisisce uno snapshot dell'istanza, archiviata in Amazon S3. Gli snapshot generalmente vengono archiviati per 4-8 ore prima di essere utilizzati da un avvio. In questo caso, il costo è di circa 0,02-0,05 USD per snapshot.

   Costi

   - Archiviazione degli snapshot (Amazon S3): cinque snapshot

3. Dopo che Amazon EC2 ha acquisito lo snapshot, interrompe l'istanza. A quel punto, l'istanza non accumula più costi. Tuttavia, i costi del volume EBS continuano ad accumularsi.

   Costi

   - Volumi EBS: i costi continuano per i volumi root EBS associati.

> **Note**
>
> I costi qui riportati sono solo a scopo dimostrativo. I costi variano a seconda del piano tariffario e della configurazione AMI.

Tieni traccia dei costi di EC2 Fast Launch sulla tua bolletta

I tag di allocazione dei costi possono aiutarti a organizzare la AWS fattura in modo da rispecchiare i costi associati a EC2 Fast Launch. Puoi utilizzare il seguente tag che Amazon EC2 aggiunge alle risorse che crea quando prepara e archivia gli snapshot preimpostati per EC2 Fast Launch:

Chiave di tag: `CreatedBy`, Valore: `EC2 Fast Launch`

Dopo aver attivato il tag nella console Gestione costi e fatturazione e aver impostato un report di fatturazione dettagliato, la colonna `user:CreatedBy` viene visualizzata nel report. La colonna include i valori di tutti i servizi. Tuttavia, se scarichi il file CSV, puoi importare i dati in un foglio di calcolo e filtrare per `EC2 Fast Launch` nel valore. Queste informazioni vengono visualizzate anche nel momento in cui il AWS Cost and Usage Report tag viene attivato.

Fase 1: attivazione dei tag di allocazione dei costi definiti dall'utente

Per includere i tag delle risorse nei report sui costi, devi prima attivare i tag nella console Gestione costi e fatturazione. Per ulteriori informazioni, consulta la sezione relativa all'attivazione dei tag per l'allocazione dei costi definiti dall'utente nella Guida per l'utente di AWS Billing and Cost Management .

> **Note**
>
> L'attivazione può richiedere fino a 24 ore.

Fase 2: impostazione di un report sui costi

Se hai già impostato un report sui costi, una colonna per il tag viene visualizzata la volta successiva che il report viene eseguito dopo il completamento dell'attivazione. Per impostare i report sui costi per la prima volta, scegli una delle opzioni seguenti.

- Consulta Impostazione di un report di allocazione dei costi mensili nella Guida per l'utente di AWS Billing and Cost Management .
- Consulta Creazione di report su costi e utilizzo nella Guida per l'utente di AWS Cost and Usage Report .

> **Note**
>
> Possono essere necessarie fino a 24 ore prima che inizi AWS a inviare report al tuo bucket S3.

Puoi configurare le AMI EC2 Fast Launch for Windows di tua proprietà o le AMI condivise con te dalla console Amazon EC2, dall'API, dagli SDK o dai comandi di. CloudFormationec2 AWS CLI Le seguenti sezioni illustrano i passaggi di configurazione per la console Amazon EC2 e. AWS CLI

Puoi anche creare AMI Windows personalizzate configurate per EC2 Fast Launch con EC2 Image Builder. Per ulteriori informazioni, consulta Creare impostazioni di distribuzione per un'AMI Windows con EC2 Fast Launch abilitato (AWS CLI).

Monitora l'avvio rapido di EC2

Questa sezione spiega come monitorare le AMI Windows Server di Amazon EC2 nel tuo account con EC2 Fast Launch abilitato.

Monitora le modifiche allo stato di EC2 Fast Launch con EventBridge

Quando lo stato cambia per un'AMI Windows con EC2 Fast Launch abilitato, Amazon EC2 genera un `EC2 Fast Launch State-change Notification` evento. Quindi Amazon EC2 invia l'evento di modifica dello stato ad Amazon EventBridge (precedentemente noto come Amazon Events). CloudWatch

Puoi creare EventBridge regole che attivano una o più azioni in risposta all'evento di cambio di stato. Ad esempio, puoi creare una EventBridge regola che rileva quando EC2 Fast Launch è abilitato ed esegue le seguenti azioni:

- Invia un messaggio a un argomento Amazon SNS per avvisare i propri abbonati.
- Richiama una funzione Lambda che esegue una determinata operazione.
- Invia i dati relativi alle modifiche di stato ad Amazon Data Firehose per l'analisi.

Per ulteriori informazioni, consulta la sezione Creazione di EventBridge regole Amazon che reagiscono agli eventi nella Amazon EventBridge User Guide.

Eventi di modifica dello stato

La funzionalità Fast Launch di EC2 emette eventi di modifica dello stato in formato JSON nel miglior modo possibile. Amazon EC2 invia gli eventi quasi EventBridge in tempo reale. Questa sezione descrive i campi dell'evento e mostra un esempio del relativo formato.

`EC2 Fast Launch State-change Notification`

imageId

Identifica l'AMI con la modifica dello stato di EC2 Fast Launch.

resourceType

Il tipo di risorsa da utilizzare per il pre-provisioning. Valore supportato: `snapshot`. Il valore predefinito è `snapshot`.

stato

Lo stato attuale della funzionalità EC2 Fast Launch per l'AMI specificata. I valori validi includono i seguenti:

- attivazione: hai abilitato la funzionalità EC2 Fast Launch per l'AMI e Amazon EC2 ha iniziato a creare snapshot per il processo di pre-provisioning.

- enabling-failed: si è verificato un errore che ha causato il fallimento del processo di pre-provisioning la prima volta che hai abilitato EC2 Fast Launch per un'AMI. Questo può accadere in qualsiasi momento durante il processo di pre-provisioning.
- abilitata — La funzione EC2 Fast Launch è abilitata. Lo stato cambia non `enabled` appena Amazon EC2 crea la prima snapshot pre-configurata per un'AMI EC2 Fast Launch appena abilitata. Se l'AMI era già abilitata e viene nuovamente sottoposta al pre-provisioning, la modifica dello stato avviene immediatamente.
- enabled-failed: questo stato si applica solo se non è la prima volta che l'AMI EC2 Fast Launch viene sottoposta al processo di pre-provisioning. Ciò può accadere se la funzionalità EC2 Fast Launch è disabilitata e successivamente riattivata, oppure se si verifica una modifica della configurazione o un altro errore dopo il completamento del pre-provisioning per la prima volta.
- disabilitazione: il proprietario dell'AMI ha disattivato la funzionalità EC2 Fast Launch per l'AMI e Amazon EC2 ha avviato il processo di pulizia.
- disabilitata — La funzionalità EC2 Fast Launch è disabilitata. Lo stato diventa `disabled` non appena Amazon EC2 completa il processo di pulizia.
- disabling-failed: il processo di pulizia ha avuto esito negativo a causa di un errore. Ciò significa che alcuni snapshot sottoposti a pre-provisioning potrebbero ancora essere presenti nell'account.

stateTransitionReason

Il motivo per cui lo stato è cambiato per l'AMI EC2 Fast Launch.

> **Note**
>
> Tutti i campi di questo messaggio di evento sono obbligatori.

L'esempio seguente mostra un'AMI EC2 Fast Launch appena abilitata che ha lanciato la prima istanza per avviare il processo di pre-provisioning. A questo punto, lo stato è `enabling`. Dopo che Amazon EC2 ha creato il primo snapshot sottoposto a pre-provisioning, lo stato cambia in `enabled`.

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "EC2 Fast Launch State-change Notification",
 "source": "aws.ec2",
```

```
 "account": "123456789012",
 "time": "2022-08-31T20:30:12Z",
 "region": "us-east-1",
 "resources": [
  "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
 ],
 "detail": {
  "imageId": "ami-123456789012",
  "resourceType": "snapshot",
  "state": "enabling",
  "stateTransitionReason": "Client.UserInitiated"
 }
}
```

Monitora le metriche di EC2 Fast Launch con CloudWatch

Le AMI Amazon EC2 con EC2 Fast Launch abilitato inviano metriche ad Amazon. CloudWatch Puoi utilizzare il AWS Management Console AWS CLI, il o un'API per elencare le metriche inviate da EC2 Fast Launch. CloudWatch Il `AWS/EC2` namespace include le seguenti metriche di EC2 Fast Launch:

Parametro	Descrizione
NumberOfAvailableFastLaunchSnapshots	Il numero di istantanee preconfigurate disponibili per ogni AMI abilitata per EC2 Fast Launch.
NumberOfInstancesFastLaunched	Il numero di istanze per ogni AMI abilitata a EC2 Fast Launch che sono state lanciate da istantanee pre-assegnate.
NumberOfInstancesNotFastLaunched	Il numero di istanze per ogni AMI abilitata a EC2 Fast Launch ha comportato un avvio a freddo a causa della mancanza di istantanee preconfigurate disponibili al momento del lancio.
FastLaunchSnapshotUsedToRefillStartTime	Il timestamp in cui Amazon EC2 ha lanciato una nuova immagine da un Fast Launch EC2 ha consentito all'AMI di creare un'altra istantanea dopo l'utilizzo di una snapshot esistente.

Parametro	Descrizione
FastLaunchSnapshotCreationTime	Misura il tempo impiegato da Amazon EC2 per avviare un'istanza e creare uno snapshot per un'AMI compatibile con EC2 Fast Launch.

Ruolo collegato ai servizi per EC2 Fast Launch

Amazon EC2 utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri Servizi AWS per tuo conto. Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a un. Servizio AWS I ruoli collegati ai servizi forniscono un modo sicuro per delegare le autorizzazioni Servizi AWS perché solo il servizio collegato può assumere un ruolo collegato al servizio. Per ulteriori informazioni sull'utilizzo dei ruoli IAM da parte di Amazon EC2, consultare Ruoli IAM per Amazon EC2.

Amazon EC2 utilizza il ruolo collegato ai servizi denominato `AWSServiceRoleForEC2FastLaunch` per creare e gestire una serie di snapshot pre-provisioning che riducono il tempo necessario all'avvio delle istanze dall'AMI di Windows.

Non è necessario creare manualmente questo ruolo collegato ai servizi. Quando inizi a utilizzare EC2 Fast Launch per la tua AMI, Amazon EC2 crea il ruolo collegato al servizio per te, se non esiste già.

> **Note**
>
> Se il ruolo collegato al servizio viene eliminato dal tuo account, puoi abilitare EC2 Fast Launch per un'altra AMI Windows per ricreare il ruolo nel tuo account. In alternativa, puoi disabilitare EC2 Fast Launch per l'AMI corrente e riattivarlo. Tuttavia, la disabilitazione della funzionalità comporta l'AMI del processo di avvio standard per tutte le nuove istanze mentre Amazon EC2 rimuove tutti gli snapshot con pre-provisioning. Dopo che tutte le istantanee pre-assegnate sono state eliminate, puoi abilitare nuovamente l'utilizzo di EC2 Fast Launch per la tua AMI.

Amazon EC2 non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForEC2FastLaunch`. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché potrebbero farvi riferimento varie entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo avere eliminato le risorse correlate. Ciò protegge le risorse Amazon EC2 associate alla tua AMI Amazon EC2 Windows Server con EC2 Fast Launch abilitato, perché non puoi rimuovere inavvertitamente l'autorizzazione di accesso alle risorse.

Amazon EC2 supporta il ruolo collegato al servizio EC2 Fast Launch in tutte le regioni in cui è disponibile il servizio Amazon EC2. Per ulteriori informazioni, consulta Regioni.

Autorizzazioni concesse da **`AWSServiceRoleForEC2FastLaunch`**

Amazon EC2 utilizza la policy gestita `EC2FastLaunchServiceRolePolicy` per completare le operazioni seguenti:

- `cloudwatch:PutMetricData`— Pubblica i dati metrici associati a EC2 Fast Launch nello spazio dei nomi Amazon EC2.
- `ec2:CreateLaunchTemplate`— Crea un modello di lancio per la tua AMI Amazon EC2 Windows Server con EC2 Fast Launch abilitato.
- `ec2:CreateSnapshot`— Crea istantanee preconfigurate per la tua AMI Windows Server Amazon EC2 con EC2 Fast Launch abilitato.
- `ec2:CreateTags`— Crea tag per le risorse associate all'avvio e al pre-provisioning di istanze Windows per la tua AMI Windows Server Amazon EC2 con EC2 Fast Launch abilitato.
- `ec2:DeleteSnapshots`— Elimina tutte le istantanee pre-assegnate associate se EC2 Fast Launch è disattivato per un'AMI precedentemente abilitata.
- `ec2:DescribeImages`— Descrivere le immagini per tutte le risorse.
- `ec2:DescribeInstanceAttribute`— Descrivere gli attributi di istanza per tutte le risorse.
- `ec2:DescribeInstanceStatus`— Descrivere gli stati di istanza per tutte le risorse.
- `ec2:DescribeInstances`— Descrivere le istanze per tutte le risorse.
- `ec2:DescribeInstanceTypeOfferings`— Descrivere le offerte di tipo di istanza per tutte le risorse.
- `ec2:DescribeLaunchTemplates`— Descrivere i modelli di avvio per tutte le risorse.
- `ec2:DescribeLaunchTemplateVersions`— Descrivere le versioni dei modelli di avvio per tutte le risorse.
- `ec2:DescribeSnapshots`— Descrivere le risorse degli snapshot per tutte le risorse.
- `ec2:DescribeSubnets`— Descrivere le sottoreti per tutte le risorse.
- `ec2:RunInstances`— Avvia istanze da un'AMI Amazon EC2 Windows Server con EC2 Fast Launch abilitato, per eseguire le fasi di provisioning.

- `ec2:StopInstances`— Interrompi le istanze lanciate da un'AMI Windows Server di Amazon EC2 con EC2 Fast Launch abilitato, per creare snapshot preimpostati.
- `ec2:TerminateInstances`— Termina un'istanza che è stata lanciata da un'AMI Amazon EC2 Windows Server con EC2 Fast Launch abilitato, dopo aver creato lo snapshot preconfigurato da essa.
- `iam:PassRole`— Consentire al ruolo collegato al servizio `AWSServiceRoleForEC2FastLaunch` di avviare istanze utilizzando il profilo di istanza dal modello di avvio.

Per ulteriori informazioni sulle policy gestite in Amazon EC2, consultare AWS politiche gestite per Amazon EC2.

Accesso alle chiavi gestite dal cliente per l'uso con le AMI crittografate e gli snapshot EBS

Prerequisito

- Per consentire ad Amazon EC2 di accedere a un'AMI crittografata, è necessario disporre dell'autorizzazione per l'operazione `createGrant` nella chiave gestita dal cliente.

Quando abiliti EC2 Fast Launch per un'AMI crittografata, Amazon EC2 garantisce che venga concessa l'autorizzazione al ruolo per utilizzare `AWSServiceRoleForEC2FastLaunch` la chiave gestita dal cliente per accedere all'AMI. Questa autorizzazione è necessaria per avviare istanze e creare snapshot pre-provisioning.

Usa gli acceleratori Amazon Elastic Graphics su istanze Windows

> **Important**
>
> Amazon Elastic Graphics ha raggiunto la fine del ciclo di vita l'8 gennaio 2024. Per carichi di lavoro che richiedono l'accelerazione grafica, ti consigliamo di utilizzare istanze Amazon EC2 G4ad, G4dn o G5.

Amazon Elastic Graphics offre un'accelerazione grafica flessibile, a basso costo e ad alte prestazioni per le istanze Windows. Gli acceleratori Elastic Graphics sono disponibili in diverse dimensioni e rappresentano un'alternativa a basso costo all'utilizzo di tipi di istanze grafiche GPU (come G3). Hai la flessibilità di scegliere un tipo di istanza che soddisfa le esigenze di calcolo, memoria e

archiviazione dell'applicazione. In seguito, scegli l'acceleratore per l'istanza che soddisfa i requisiti grafici del carico di lavoro.

Grafica elastica è adatta per applicazioni che richiedono una quantità piccola o intermittente di accelerazione grafica aggiuntiva e che utilizzano il supporto grafico OpenGL. Se è necessario accedere a GPU complete e direttamente collegate e utilizzare in parallelo i framework di elaborazione DirectX, CUDA o Open Computing Language (OpenCL), utilizzare invece un tipo di istanza di elaborazione accelerata.

Indice

Nozioni di base su Grafica elastica

Per utilizzare Elastic Graphics, avvia un'istanza Windows e specifica un tipo di acceleratore per l'istanza durante l'avvio. AWS trova la capacità Elastic Graphics disponibile e stabilisce una connessione di rete tra l'istanza e l'acceleratore Elastic Graphics.

> **Note**
>
> Le istanze bare metal non sono supportate.

Gli acceleratori Elastic Graphics sono disponibili nelle seguenti AWS regioni:`us-east-1`,`us-east-2`,,`us-west-2`,`ap-northeast-1`, `ap-southeast-1``ap-southeast-2`, `eu-central-1` e. `eu-west-1`

I tipi di istanza seguenti supportano gli acceleratori Grafica elastica:

- Uso generico: M3, M4, M5, M5d, M5dn, M5n, T2, T3

> **Note**
>
> Sono supportati solo i tipi di istanza `t2.medium`, `t3.medium` e versioni superiori.

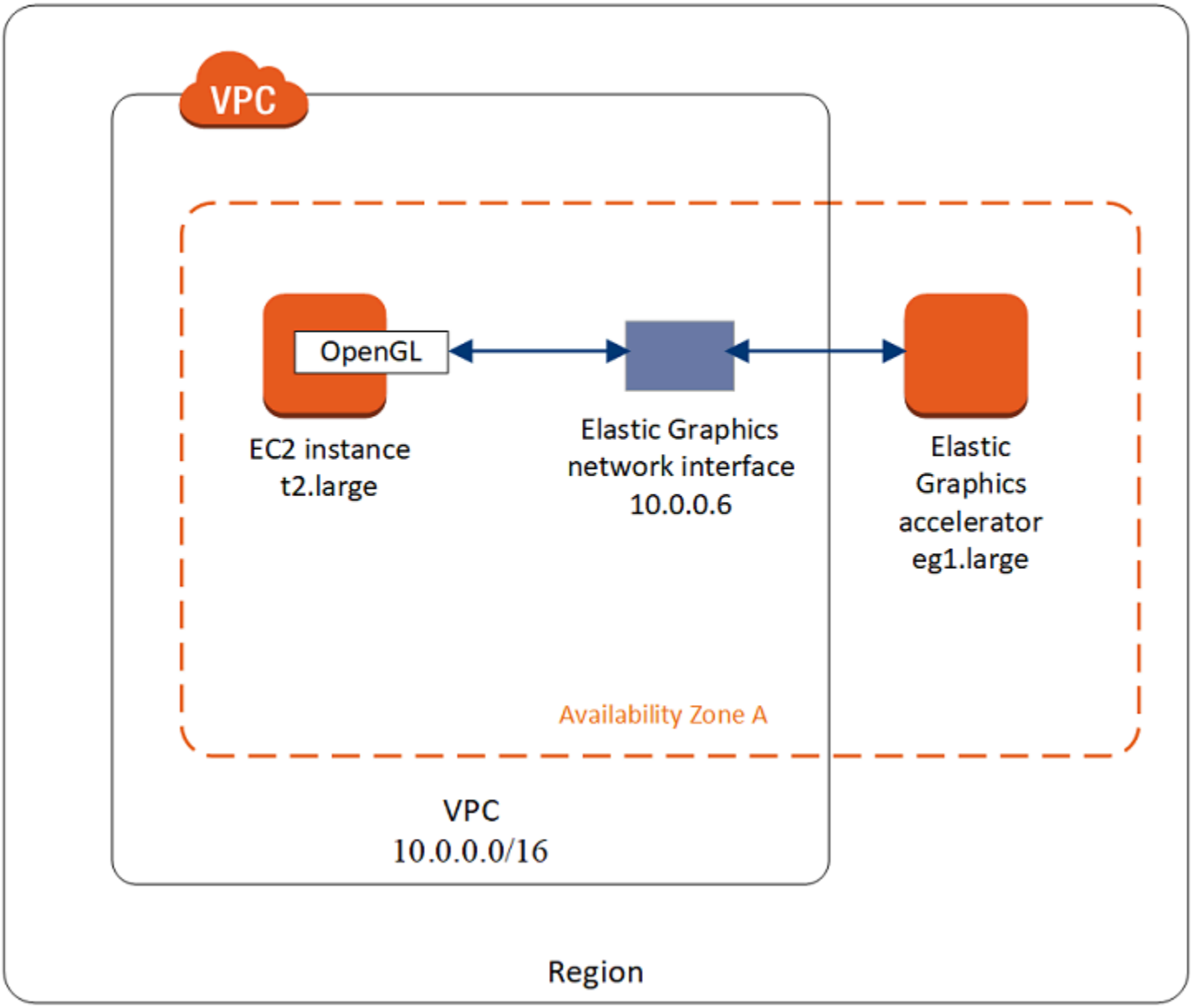
- Ottimizzate per il calcolo: C3, C4, C5, C5a, C5ad, C5d, C5n
- Ottimizzate per la memoria: R3, R4, R5, R5d, R5dn, R5n, X1, X1e, z1d
- Ottimizzate per l'archiviazione: D2, D3, D3en, H1, I3, I3en
- Calcolo accelerato: P2, P3, P3dn

Sono disponibili i seguenti acceleratori Grafica elastica: È possibile collegare qualsiasi acceleratore Grafica elastica a qualsiasi tipo di istanza supportato.

Acceleratore Grafica elastica	Memoria grafica (GB)
`eg1.medium`	1
`eg1.large`	2
`eg1.xlarge`	4
`eg1.2xlarge`	8

Un acceleratore Grafica elastica non fa parte dell'hardware dell'istanza. Invece, è collegato in rete attraverso un'interfaccia di rete, nota come interfaccia di rete Grafica elastica. Quando si avvia o si riavvia un'istanza con l'accelerazione grafica, l'interfaccia di rete Grafica elastica viene creata automaticamente nel proprio VPC.

L'interfaccia di rete Grafica elastica viene creata nella stessa sottorete e nello stesso VPC dell'istanza e tale sottorete le assegna un indirizzo IPv4 privato. L'acceleratore collegato all'istanza Amazon EC2 viene allocato da un pool di acceleratori elastici disponibili nella stessa zona di disponibilità dell'istanza.



Gli acceleratori Grafica elastica supportano gli standard API per OpenGL 4.3 API e versioni precedenti, che possono essere utilizzati per applicazioni batch o per l'accelerazione della grafica 3D. Una libreria OpenGL ottimizzata per Amazon sull'istanza rileva l'acceleratore collegato. Trasferisce le chiamate API OpenGL dall'istanza all'acceleratore, che a sua volta elabora le richieste e fornisce i risultati. Il traffico tra l'istanza e l'acceleratore utilizza la stessa larghezza di banda del traffico di rete dell'istanza, quindi consigliamo di avere a disposizione una larghezza di banda di rete adeguata. Per qualsiasi domanda sulla conformità e la versione di OpenGL, consulta il proprio fornitore di software.

Come impostazione predefinita, il gruppo di sicurezza predefinito del VPC è associato all'interfaccia di rete Grafica elastica. Il traffico di rete Grafica elastica utilizza il protocollo TCP e la porta 2007. Verificare che il gruppo di sicurezza per l'istanza lo consenta. Per ulteriori informazioni, consulta Configurazione dei gruppi di sicurezza.

Prezzi di Grafica elastica

Vieni addebitato per ogni secondo che un acceleratore Grafica elastica è collegato a un'istanza nello stato `running` quando l'acceleratore è nello stato `Ok`. Non verrà addebitato alcun costo per un acceleratore collegato a un'istanza nello stato `pending`, `stopping`, `stopped`, `shutting-down` o `terminated`. Inoltre, non verrà addebitato alcun costo se un acceleratore si trova nello stato `Unknown` o `Impaired`.

I prezzi degli acceleratori sono disponibili solo in base alle tariffe on demand. È possibile collegare un acceleratore a un'istanza riservata o un'istanza Spot, tuttavia si applica il prezzo on demand per l'acceleratore.

Per ulteriori informazioni, consulta Prezzi di Grafica elastica di Amazon.

Limitazioni di Grafica elastica

Prima di iniziare a utilizzare gli acceleratori Grafica elastica, è necessario conoscere le limitazioni seguenti:

- Puoi collegare gli acceleratori solo alle istanze di Windows con Microsoft Windows Server 2012 R2 o versioni successive. Le istanze Linux non sono attualmente supportate.
- Puoi collegare un acceleratore a un'istanza per volta.
- Puoi collegare un acceleratore solo durante l'avvio dell'istanza. Non è possibile collegare un acceleratore a un'istanza esistente.
- Non è possibile ibernare un'istanza con un acceleratore collegato.
- Non è possibile condividere un acceleratore tra istanze.
- Non è possibile distaccare un acceleratore da un'istanza o trasferirla a un'istanza diversa. Se un acceleratore non è più necessario, bisogna terminare l'istanza. Per modificare il tipo di acceleratore, crea un'AMI dall'istanza, termina l'istanza e avvia una nuova istanza con una specifica di acceleratore diversa.
- Le uniche versioni supportate sono OpenGL API 4.3 e le versioni precedenti. DirectX, CUDA e OpenCL non sono supportate.

- L'acceleratore Grafica elastica non è visibile o accessibile attraverso il gestore del dispositivo dell'istanza.
- Non è possibile prenotare o pianificare la capacità di un acceleratore.

Utilizzo di Grafica elastica

> **Important**
>
> Amazon Elastic Graphics ha raggiunto la fine del ciclo di vita l'8 gennaio 2024. Per carichi di lavoro che richiedono l'accelerazione grafica, ti consigliamo di utilizzare istanze Amazon EC2 G4ad, G4dn o G5.

È possibile avviare un'istanza e associarla a un acceleratore Grafica elastica durante il lancio. Devi quindi installare manualmente le librerie necessarie sull'istanza che attivano la comunicazione con l'acceleratore. Per le limitazioni, consulta Limitazioni di Grafica elastica.

Attività

- Configurazione dei gruppi di sicurezza
- Avvio di un'istanza con un acceleratore Grafica elastica
- Installazione del software necessario per Grafica elastica
- Verifica della funzionalità Grafica elastica nella propria istanza
- Visualizzazione delle informazioni su Grafica elastica
- Invia un feedback

Configurazione dei gruppi di sicurezza

Elastic Graphics richiede un gruppo di sicurezza autoreferenziale in cui sia consentito tutto il traffico in entrata e in uscita dal gruppo stesso. Il gruppo di sicurezza deve includere le regole in entrata e in uscita indicate di seguito.

In entrata

Type	Protocollo	Porta	Origine
Elastic Graphics	TCP	2007	L'ID del gruppo di sicurezza (ID della risorsa)

In uscita

Type	Protocollo	Intervallo porte	Destinazione
Elastic Graphics	TCP	2007	L'ID del gruppo di sicurezza (ID della risorsa)

Se utilizzi la console Amazon EC2 per avviare l'istanza con un acceleratore Elastic Graphics, puoi permettere alla procedura guidata dell'istanza di avvio di creare automaticamente le regole del gruppo di sicurezza necessarie oppure puoi selezionare una sicurezza creata in precedenza.

Se si avvia l'istanza utilizzando AWS CLI o un SDK, è necessario specificare un gruppo di sicurezza creato in precedenza.

Come creare un gruppo di sicurezza per Grafica elastica

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Security Groups (Gruppi di sicurezza) e quindi Create Security Group (Crea gruppo di sicurezza).
3. Nella finestra Create Security Group (Crea gruppo di sicurezza) effettuare le operazioni seguenti:
   a. In Nome gruppo di sicurezza, immettere un nome descrittivo per il gruppo di sicurezza, ad esempio `Elastic Graphics security group`.
   b. (Facoltativo) In Description (Descrizione), inserire una breve descrizione del gruppo di sicurezza.
   c. Per VPC, selezionare il VPC in cui utilizzare Elastic Graphics.
   d. Scegliere Create Security Group (Crea gruppo di sicurezza).
4. Nel riquadro di navigazione, scegliere Security Groups (Gruppi di sicurezza), selezionare il gruppo di sicurezza appena creato e nella scheda Dettagli copiare la scheda ID gruppo di sicurezza.

5. Nella scheda Inbound rules (Regole in entrata) scegliere Edit inbound rules (Modifica regole in entrata), quindi eseguire le seguenti operazioni:

   a. Scegli Aggiungi regola.

   b. Per Type (Tipo), selezionare Elastic Graphics (Grafica elastica).

   c. Per Source type (Tipo di origine), scegliere Custom (Personalizzato).

   d. Per Source (Origine), incollare l'ID del gruppo di sicurezza copiato in precedenza.

   e. Scegliere Salva regole.

6. Nella scheda Outbound rules (Regole in uscita) scegliere Edit outbound rules (Modifica regole in uscita), quindi eseguire le seguenti operazioni:

   a. Scegli Aggiungi regola.

   b. Per Type (Tipo), selezionare Elastic Graphics (Grafica elastica).

   c. Per Destination type (Tipo di destinazione), scegliere Custom (Personalizzato).

   d. Per Destination (Destinazione), incollare l'ID del gruppo di sicurezza copiato in precedenza.

   e. Scegliere Salva regole.

Per ulteriori informazioni, consulta Gruppi di sicurezza Amazon EC2 per le tue istanze EC2.

Avvio di un'istanza con un acceleratore Grafica elastica

È possibile associare un acceleratore Grafica elastica a un'istanza durante l'avvio. Se l'avvio non va a buon fine, il motivo può essere tra i seguenti:

- Capacità insufficiente dell'acceleratore Grafica elastica
- Superato il limite negli acceleratori Grafica elastica nella regione
- Non sono presenti abbastanza indirizzi IPv4 privati nel VPC per creare un'interfaccia di rete per l'acceleratore

Per ulteriori informazioni, consulta Limitazioni di Grafica elastica.

Come associare un acceleratore Grafica elastica durante il lancio dell'istanza (console)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di controllo, selezionare Launch Instance (Avvia istanza).

3. In Nome e tag, inserisci un valore per Nome. Facoltativamente, puoi scegliere Aggiungi tag aggiuntivi per aggiungere altri tag alle risorse associate all'istanza che stai avviando.
4. In Immagini dell'applicazione e del sistema operativo (Amazon Machine Image), seleziona un'AMI Windows.
5. In Instance type (Tipo di istanza), seleziona un tipo di istanza supportato. Per ulteriori informazioni, consulta Nozioni di base su Grafica elastica.
6. In Key pair (login) (Coppia di chiavi (login), per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o creane una nuova.
7. Accanto a Impostazioni di rete, scegli Modifica, quindi specifica le impostazioni di rete da utilizzare per l'istanza.

    a. Per Rete, seleziona un VPC per la tua istanza.

    b. Per Subnet, seleziona una sottorete in cui avviare l'istanza.

    c. Per Firewall (gruppi di sicurezza), puoi utilizzare il gruppo di sicurezza creato manualmente o lasciare che la console crei un gruppo di sicurezza con le regole in Configurazione dei gruppi di sicurezza entrata e in uscita richieste. Aggiungere ulteriori gruppi di sicurezza in base alle esigenze.
8. (Facoltativo) In Configura archiviazione, configura la dimensione del volume root e aggiungi altri volumi secondo necessità.
9. Espandi la sezione Dettagli avanzati.
10. In Dettagli avanzati, per Elastic GPU, seleziona un tipo di acceleratore Elastic Graphics.
11. Nel pannello Summary (Riepilogo), scegliere Launch instance (Avvia istanza).

Come associare un acceleratore di Elastic Graphics durante l'avvio dell'istanza (AWS CLI)

È possibile utilizzare il AWS CLI comando run-instances con il seguente parametro:

```
--elastic-gpu-specification Type=eg1.medium
```

Per il parametro `--security-group-ids`, devi includere un gruppo di sicurezza che ha le regole in entrata e in uscita necessarie. Per ulteriori informazioni, consulta Configurazione dei gruppi di sicurezza.

Per associare un acceleratore Elastic Graphics durante l'avvio dell'istanza (Tools for Windows) PowerShell

Utilizzate il PowerShell comando New-EC2InstanceTools for Windows.

Installazione del software necessario per Grafica elastica

Se hai avviato l'istanza utilizzando un'AMI AWS Windows corrente, il software richiesto viene installato automaticamente al primo avvio. Se hai avviato l'istanza utilizzando AMI Windows che non installano automaticamente il software necessario, devi installare il software necessario sull'istanza manualmente.

Come installare il software necessario per Grafica elastica (se necessario)

1. Collegarsi all'istanza.
2. Scaricare Programma di installazione di Elastic Graphics e aprirlo. Il gestore dell'installazione si connette all'endpoint di Grafica elastica e scarica l'ultima versione del software necessario.

   > **Note**
   >
   > Se il collegamento per il download non funziona, prova un browser diverso o copia l'indirizzo del collegamento e incollalo in una nuova scheda del browser.

3. Riavviare l'istanza da verificare.

Verifica della funzionalità Grafica elastica nella propria istanza

I pacchetti Grafica elastica nell'istanza includono strumenti che è possibile utilizzare per visualizzare lo stato dell'acceleratore e per verificare che i comandi OpenGL dalla istanza all'acceleratore siano funzionali.

Se l'istanza è stata avviata con un'AMI che non ha i pacchetti Grafica elastica preinstallati, è possibile scaricarli e installarli per conto proprio. Per ulteriori informazioni, consulta Installazione del software necessario per Grafica elastica.

Per la verifica della funzionalità di Grafica elastica dell'istanza è possibile utilizzare uno dei seguenti metodi.

> **Note**
>
> Se il monitor dello stato della grafica elastica o lo strumento da riga di comando restituisce un risultato imprevisto, consulta Risoluzione dei problemi relativi allo stato non integro.

Elastic Graphics status monitor

È possibile utilizzare lo strumento di monitoraggio di stato per visualizzare le informazioni riguardanti lo stato di un acceleratore Grafica elastica collegato. Come impostazione predefinita, tale strumento è disponibile nell'area di notifica della barra delle applicazioni nell'istanza di Windows e mostra lo stato dell'acceleratore della grafica. Di seguito sono riportati i valori possibili:

Integro

L'acceleratore Grafica elastica è attivo e integro.

Aggiornamento in corso

L'aggiornamento dello stato dell'acceleratore Grafica elastica è in corso. Potrebbero essere necessari alcuni minuti prima che lo stato venga visualizzato.

Fuori servizio

L'acceleratore Grafica elastica è fuori servizio. Per ottenere più informazioni sull'errore, seleziona Read More (Per saperne di più).

Elastic Graphics command line tool

Puoi utilizzare lo strumento a riga di comando di Grafica elastica, `egcli.exe`, per controllare lo stato dell'acceleratore. Se si verifica un problema con l'acceleratore, lo strumento restituisce un messaggio di errore.

Per avviare lo strumento, apri un prompt dei comandi dall'interno dell'istanza ed esegui il seguente comando:

```
C:\Program Files\Amazon\EC2ElasticGPUs\manager\egcli.exe
```

Lo strumento supporta anche i seguenti parametri:

`--json`, `-j`

Indica se visualizzare il messaggio JSON. I valori possibili sono `true` e `false`. Il valore di default è `true`.

`--imds`, `-i`

Indica se controllare la disponibilità dell'acceleratore nei metadati dell'istanza. I valori possibili sono `true` e `false`. Il valore di default è `true`.

Di seguito è riportato un output di esempio. Uno stato di OK indica che l'acceleratore è attivo e integro.

```
EG Infrastructure is available.
Instance ID egpu-f6d94dfa66df4883b284e96db7397ee6
Instance Type eg1.large
EG Version 1.0.0.885 (Manager) / 1.0.0.95 (OpenGL Library) / 1.0.0.69 (OpenGL
 Redirector)
EG Status: Healthy
JSON Message:
{
  "version": "2016-11-30",
  "status": "OK"
}
```

Di seguito sono riportati i valori possibili per `status`:

`OK`

L'acceleratore Grafica elastica è attivo e integro.

`UPDATING`

Il driver Grafica elastica: è in fase di aggiornamento.

`NEEDS_REBOOT`

Il driver Grafica elastica è stato aggiornato ed è necessario un riavvio dell'istanza Amazon EC2.

`LOADING_DRIVER`

Il driver Grafica elastica: è in fase di caricamento.

`CONNECTING_EGPU`

Il driver Grafica elastica sta verificando la connettività all'acceleratore Grafica elastica.

`ERROR_UPDATE_RETRY`

Si è verificato un errore durante l'aggiornamento del driver Grafica elastica, presto verrà eseguito un tentativo di aggiornamento.

`ERROR_UPDATE`

Si è verificato un errore irreversibile durante l'aggiornamento del driver Grafica elastica.

`ERROR_LOAD_DRIVER`

Si è verificato un errore durante il caricamento del driver Grafica elastica.

`ERROR_EGPU_CONNECTIVITY`

L'acceleratore Grafica elastica non è raggiungibile.

Visualizzazione delle informazioni su Grafica elastica

È possibile visualizzare le informazioni dell'acceleratore Grafica elastica collegato all'istanza.

Come visualizzare informazioni sull'acceleratore Grafica elastica (console)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Instances (Istanze) e selezionare l'istanza.
3. Nella scheda Details (Dettagli), trova Elastic Graphics ID. Selezionare l'ID per visualizzare le informazioni seguenti sull'acceleratore Grafica elastica:
   - Attachment State (Stato del collegamento)
   - Type
   - Health status (Stato di integrità)

Come visualizzare informazioni sull'acceleratore di Elastic Graphics (AWS CLI)

È possibile utilizzare il describe-elastic-gpus AWS CLI comando:

```
aws ec2 describe-elastic-gpus
```

È possibile utilizzare il describe-network-interfaces AWS CLI comando e filtrare in base all'ID del proprietario per visualizzare le informazioni sull'interfaccia di rete Elastic Graphics.

```
aws ec2 describe-network-interfaces --filters "Name=attachment.instance-owner-
id,Values=amazon-elasticgpus"
```

Per visualizzare informazioni su un acceleratore Elastic Graphics (Tools for Windows PowerShell)

Utilizza il seguente comando:

- Get-EC2ElasticGpu
- Get-EC2NetworkInterface

Come visualizzare le informazioni sull'acceleratore Grafica elastica tramite i metadati di istanza

1. Connettersi all'istanza Windows che sta utilizzando un acceleratore Grafica elastica.
2. Esegui una di queste operazioni:
   - Da PowerShell, utilizzare il seguente cmdlet:

     ```
     PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
     ```

   - Dal browser Web, incollare il seguente URL nel campo indirizzo:

     ```
     http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
     ```

Invia un feedback

È possibile inviare un feedback sulla propria esperienza con Elastic Graphics, in modo che il team possa apportare ulteriori miglioramenti.

Come inviare un feedback utilizzando il monitoraggio di stato di Grafica elastica

1. Nell'area di notifica della barra delle applicazioni nell'istanza Windows, aprire il monitoraggio di stato di Grafica elastica.
2. Nell'angolo in basso a sinistra, scegliere Feedback.
3. Immettere il feedback e scegliere Submit (Invia).

Manutenzione della grafica elastica

> **Important**
>
> Amazon Elastic Graphics ha raggiunto la fine del ciclo di vita l'8 gennaio 2024. Per carichi di lavoro che richiedono l'accelerazione grafica, ti consigliamo di utilizzare istanze Amazon EC2 G4ad, G4dn o G5.

AWS potrebbe determinare che un acceleratore Elastic Graphics è in uno stato non integro se:

- È necessario un aggiornamento della sicurezza o dell'infrastruttura
- È necessario un aggiornamento software
- Si è verificato un problema con l'host sottostante

Quando AWS determina che un acceleratore Elastic Graphics non è integro, pianifica il ritiro dell'acceleratore. AWS ti avvisa dell'imminente ritiro dell'acceleratore e ti fornisce le misure correttive da intraprendere.

Argomenti

In che modo riceverò l'avviso?

Quando AWS pianifica il ritiro di un acceleratore Elastic Graphics, invia un avviso di ritiro dell'acceleratore al cliente. AWS Health Dashboard AWS invia anche un'e-mail all'indirizzo e-mail associato al tuo account. AWS È lo stesso indirizzo e-mail che usi per accedere alla AWS Management Console.

> **Note**
>
> Se utilizzi un account e-mail che non controlli regolarmente, utilizza il AWS Health Dashboard per determinare se è previsto il ritiro di alcuni dei tuoi acceleratori Elastic Graphics. Puoi anche modificare le informazioni di contatto del tuo AWS account nella pagina Impostazioni account.

L'avviso di ritiro contiene le informazioni seguenti:

- ID dell'istanza a cui è collegato l'acceleratore
- Informazioni sul problema che interessa l'acceleratore
- Data di ritiro dell'acceleratore
- Misure correttive da intraprendere

che cosa si deve fare?

Quando si riceve una notifica relativa alla pianificazione del ritiro per l'acceleratore di grafica elastica, è necessario arrestare e riavviare l'istanza a cui è collegato l'acceleratore. In questo modo l'acceleratore unhealty (non integro) precedente verrà sostituito con uno nuovo, healthy (integro).

Si consiglia di chiudere le applicazioni di grafica in esecuzione sull'istanza prima di arrestare e riavviare l'istanza.

> **Important**
>
> Se non si arresta e si riavvia l'istanza prima della data di ritiro programmata, l'acceleratore associato all'istanza viene automaticamente arrestato, con conseguente interruzione del funzionamento delle applicazioni.
> È necessario arrestare e avviare l'istanza Il riavvio dell'istanza non sostituirà l'acceleratore non integro con uno integro.

Cosa accade quando un acceleratore raggiunge la data di ritiro?

Quando un acceleratore Elastic Graphics non funzionante raggiunge la data di ritiro prevista, lo interrompe AWS definitivamente. Per ricevere una sostituzione dell'acceleratore non integro, prima o dopo la data di ritiro, è necessario interrompere e avviare l'istanza a cui è collegato l'acceleratore.

Se non si arresta e si riavvia l'istanza prima della data di ritiro programmata, l'acceleratore associato all'istanza viene automaticamente arrestato, con conseguente interruzione del funzionamento delle applicazioni.

Usa le CloudWatch metriche per monitorare Elastic Graphics

> **Important**
>
> Amazon Elastic Graphics ha raggiunto la fine del ciclo di vita l'8 gennaio 2024. Per carichi di lavoro che richiedono l'accelerazione grafica, ti consigliamo di utilizzare istanze Amazon EC2 G4ad, G4dn o G5.

Puoi monitorare il tuo acceleratore Elastic Graphics utilizzando Amazon CloudWatch, che raccoglie metriche sulle prestazioni dell'acceleratore. Queste statistiche vengono registrate per un periodo di

due settimane, per permettere l'accesso a informazioni storiche e per offrire una prospettiva migliore sulle prestazioni del servizio.

Per impostazione predefinita, gli acceleratori Elastic Graphics inviano dati metrici in periodi di 5 minuti. CloudWatch

Per ulteriori informazioni su Amazon CloudWatch, consulta la Amazon CloudWatch User Guide.

Parametri di Grafica elastica

Lo spazio dei nomi `AWS/ElasticGPUs` include i parametri descritti di seguito per Grafica elastica.

Parametro	Descrizione
GPU ConnectivityCheckFailed	Segnala se la connettività all'acceleratore Grafica elastica è attiva o non è riuscita. Un valore pari a zero (0) indica che la connessione è attiva. Un valore pari a uno (1) indica un errore di connettività. Unità: numero
GPU HealthCheckFailed	Indica se l'acceleratore Grafica elastica ha superato un controllo dello stato nell'ultimo minuto. Un valore pari a zero (0) indica che il controllo dello stato è stato superato. Un valore pari a uno (1) indica che il controllo dello stato non è stato superato. Unità: numero
GPU MemoryUtilization	Memoria GPU utilizzata. Unità: MiB

Dimensioni di Grafica elastica

Puoi filtrate i dati dei parametri per gli acceleratori Grafica elastica utilizzando le seguenti dimensioni.

Dimensione	Descrizione
`EGPUId`	Filtra i dati in base all'acceleratore Grafica elastica.

Dimensione	Descrizione
`InstanceId`	Filtra i dati per l'istanza alla quale l'acceleratore Grafica elastica è collegato.

Visualizza le CloudWatch metriche per Elastic Graphics

I parametri sono raggruppati in primo luogo in base allo spazio dei nomi del servizio e in secondo luogo in base alle dimensioni supportate. Puoi utilizzare le procedure esposte di seguito per visualizzare i parametri per gli acceleratori Grafica elastica.

Per visualizzare le metriche di Elastic Graphics utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Se necessario, modificare la regione . Nella barra di navigazione, selezionare la regione nella quale si trova l'acceleratore Grafica elastica. Per ulteriori informazioni, consulta Regioni ed endpoint.
3. Nel riquadro di navigazione, seleziona Parametri.
4. Per All metrics (Tutti i parametri), selezionare Elastic Graphics, Elastic Graphics Metrics (Parametri Elastic Graphics).

Come visualizzare i parametri di Elastic Graphics (AWS CLI)

Utilizza il comando list-metrics seguente:

```
aws cloudwatch list-metrics --namespace "AWS/ElasticGPUs"
```

Crea CloudWatch allarmi per monitorare Elastic Graphics

Puoi creare un CloudWatch allarme che invia un messaggio Amazon SNS quando l'allarme cambia stato. Un allarme controlla un singolo parametro in un periodo di tempo specificato e invia una notifica a un argomento Amazon SNS in base al valore del parametro relativo a una determinata soglia in periodi di tempo specificati.

Ad esempio, è possibile creare un allarme che monitora l'integrità di un acceleratore Grafica elastica e invia una notifica quando l'acceleratore della grafica non passa un controllo dello stato per tre periodi consecutivi di 5 minuti.

Come creare un allarme per lo stato dell'acceleratore Grafica elastica

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Alarms (Allarmi), Create Alarm (Crea allarme).
3. Selezionare Select metric (Seleziona parametro), selezionare Elastic Graphics, Elastic Graphics Metrics (Parametri Elastic Graphics).
4. Seleziona la metrica GPU e scegli Seleziona HealthCheckFailed metrica.
5. Configurare l'allarme come segue:

   a. Per Alarm details (Dettagli allarme), digitare un nome e una descrizione per l'allarme. For Whenever (Ogni volta che), selezionare >= e tipo 1.

   b. Per Actions (Operazioni), seleziona un elenco di notifiche esistenti oppure selezionare New list (Nuovo elenco).

   c. Scegliere Create Alarm (Crea allarme).

Risoluzione dei problemi

> **Important**
>
> Amazon Elastic Graphics ha raggiunto la fine del ciclo di vita l'8 gennaio 2024. Per carichi di lavoro che richiedono l'accelerazione grafica, ti consigliamo di utilizzare istanze Amazon EC2 G4ad, G4dn o G5.

Di seguito sono riportati gli errori comuni e i passaggi per la risoluzione dei problemi.

Indice

- Perché si vedono più ENI?

Analisi dei problemi di prestazioni delle applicazioni

Grafica elastica utilizza la rete di istanze per inviare comandi OpenGL a una scheda grafica collegata in remoto. Inoltre, un desktop che esegue un'applicazione OpenGL con un acceleratore Grafica elastica è in genere accessibile utilizzando una tecnologia di accesso remoto. È importante distinguere tra un problema di prestazioni relativo al rendering di OpenGL e la tecnologia di accesso remoto del desktop.

Problemi di prestazioni relativi al rendering di OpenGL

Le prestazioni di rendering di OpenGL sono determinate dal numero di comandi e frame di OpenGL generati sull'istanza remota.

Le prestazioni di rendering possono variare a seconda dei fattori seguenti:

- Prestazioni acceleratore Grafica elastica
- Prestazioni di rete
- Prestazioni della CPU
- Modello di rendering, complessità dello scenario
- Comportamento dell'applicazione OpenGL

Un modo semplice di valutare le prestazioni è quello di visualizzare il numero di frame sottoposti a rendering sull'istanza remota. Gli acceleratori di Elastic Graphics visualizzano un massimo di 25 FPS sull'istanza remota per ottenere la migliore qualità percepita, riducendo al contempo l'utilizzo della rete.

Visualizzare il numero di frame prodotti

1. Aprire il file seguente in un editor di testo. Se il file non esiste, crearlo.

   ```
   C:\Program Files\Amazon\EC2ElasticGPUs\conf\eg.conf
   ```

2. Individuare la sezione `[Application]` o aggiungerla se non è presente e aggiungere il parametro di configurazione seguente:

   ```
   [Application]
   ```

```
show_fps=1
```

3. Riavviare l'applicazione e verificare nuovamente l'FPS

Se FPS raggiunge 15-25 FPS durante l'aggiornamento della scena di rendering, le prestazioni dell'acceleratore Grafica elastica sono al massimo. Qualsiasi altro problema di prestazione che si verifica probabilmente è legato all'accesso remoto al desktop dell'istanza. In tal caso, consulta la sezione Problemi di prestazioni dell'accesso remoto.

Se il numero di FPS è inferiore a 15, provare la procedura seguente:

- Migliora le prestazioni dell'acceleratore Grafica elastica selezionando un tipo di acceleratore della grafica più potente.
- Migliorare le prestazioni complessive della rete utilizzando i suggerimenti seguenti:
  - Controlla la quantità di larghezza di banda in entrata e in uscita da e verso l'endpoint dell'acceleratore Grafica elastica. L'endpoint dell'acceleratore Elastic Graphics può essere recuperato con il seguente comando: PowerShell

    ```
    PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/meta-data/elastic-gpus/
    associations/[ELASTICGPU_ID]).content
    ```

  - Il traffico di rete dall'istanza all'endpoint dell'acceleratore Grafica elastica si riferisce al volume di comandi che l'applicazione OpenGL sta producendo.
  - Il traffico di rete dall'endpoint dell'acceleratore Grafica elastica all'istanza si riferisce al numero di frame generati dall'acceleratore della grafica.
  - Se si nota che l'utilizzo della rete raggiunge la velocità effettiva di rete massima delle istanze, provare a utilizzare un'istanza con una velocità effettiva di rete superiore.
- Migliorare le prestazioni della CPU:
  - Le applicazioni possono necessitare di molte risorse della CPU oltre a quelle necessarie all'acceleratore Grafica elastica. Se Windows Task Manager riporta un uso elevato di risorse della CPU, provare a utilizzare un'istanza con una maggiore potenza della CPU.

Problemi di prestazioni relativi all'accesso remoto

Un'istanza con un acceleratore Grafica elastica collegato è accessibile utilizzando diverse tecnologie di accesso remoto. Le prestazioni e la qualità possono variare a seconda di:

- Tag dell'istanza nei metadati dell'istanza
- Prestazioni dell'istanza
- Prestazioni del client
- Latenza di rete e larghezza di banda tra il client e l'istanza

Tra le scelte possibili del protocollo di accesso remoto ci sono:

- Microsoft Remote Desktop Connection
- NICE DCV
- VNC

Per ulteriori informazioni sull'ottimizzazione, consulta il protocollo specifico.

Risoluzione dei problemi relativi allo stato non integro

Se l'acceleratore Grafica elastica non è in uno stato non integro, utilizza le seguenti procedure di risoluzione dei problemi per risolvere il problema.

Controllare la configurazione dell'istanza

Se lo strumento a riga di comando Elastic Graphics, `egcli.exe`, restituisce un output simile al seguente, assicurarsi che il gruppo di sicurezza è configurato correttamente e l'istanza sia stata avviata con Instance Metadata Service abilitato.

```
EG Version 1.0.7.4240 (Manager) / N/A (OpenGL Library) / N/A (OpenGL Redirector)
EG Status: Out Of Service
Something prevented the EG Infrastructure to work properly.
```

Arrestare e avviare l'istanza

Se l'acceleratore Grafica elastica è in uno stato non integro, l'opzione più semplice è quella di arrestare l'istanza e avviarla di nuovo. Per ulteriori informazioni, consulta Arresta e avvia manualmente le istanze.

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

Verificare i componenti installati

Aprire il Pannello di controllo di Windows e verificare che i seguenti componenti siano installati:

- Amazon Elastic Graphics Manager
- Amazon Elastic Graphics OpenGL Library
- Amazon EC2 Elastic GPUs OpenGL Redirector

Se manca una di queste voci, la devi installare manualmente. Per ulteriori informazioni, consulta Installazione del software necessario per Grafica elastica.

Controllo dei log Grafica elastica

Apri il Visualizzatore eventi di Windows, espandi la sezione Application and Services Logs (Log di applicazioni e servizi) e cercare errori nei log di eventi seguenti.

- EC2ElasticGPU
- EC2ElasticGPUs GUI

Perché si vedono più ENI?

Quando si chiama StartInstancesun'istanza EC2 con un acceleratore Elastic Graphics, viene creata una nuova Elastic Network Interface (ENI) sull'istanza per consentire l'invio dei comandi OpenGL alla scheda grafica collegata in remoto.

Se chiami più StartInstancesvolte in un breve periodo di tempo (pochi secondi o meno) sulla stessa istanza EC2, viene creata una nuova interfaccia di rete per ogni chiamata. Tuttavia:

- L'acceleratore Elastic Graphics utilizzerà un'unica interfaccia di rete.
- Le interfacce di rete aggiuntive non comportano costi aggiuntivi e verranno rilasciate automaticamente in 24 ore.

Installazione di WSL sulla tua istanza di Windows

Windows Subsystem per Linux (WSL) è disponibile come download gratuito da installare sull'istanza di Windows. Installando WSL, puoi eseguire strumenti nativi della riga di comando di Linux direttamente sull'istanza di Windows e utilizzare gli strumenti di Linux per lo scripting, accanto al tradizionale desktop di Windows. Puoi passare facilmente da Linux a Windows su una singola istanza di Windows, utile per esempio in un ambiente di sviluppo.

Per ulteriori informazioni su WSL, consulta la Documentazione di Windows Subsystem per Linux sul sito web Microsoft Build.

Limitazioni

- WSL è disponibile in due versioni: WSL 1 e WSL 2.
  - Per le istanze EC2 `.metal`, puoi installare WSL 1 o WSL 2.
  - Per le istanze EC2 virtualizzate, è necessario installare WSL 1.
- Per i sistemi operativi Windows Server, WSL può essere installato solo su istanze che eseguono quanto segue:
  - Windows Server 2019
  - Windows Server 2022

Installare WSL

Le seguenti istruzioni installano WSL su un'istanza EC2 che esegue Windows Server 2022. Per le istruzioni sull'installazione di WSL su un'istanza EC2 che esegue Windows Server 2019, consulta Install WSL on previous versions of Windows Server sul sito Web di Microsoft. Dopo aver seguito queste istruzioni, puoi utilizzare il passaggio 3 delle istruzioni seguenti per configurare WSL a utilizzare WSL 1.

Installa WSL 1

1. Per installare WSL, eseguire il seguente comando di installazione standard sull'istanza EC2, ma assicurarsi di abilitare WSL 1 includendo `--enable-wsl1`. Per impostazione predefinita, è installato WSL 2. Se l'istanza è stata avviata utilizzando un tipo di istanza virtualizzata, devi completare il passaggio 3 di questa procedura per impostare la versione su WSL 1.

   ```
   wsl --install --enable-wsl1 --no-launch
   ```

2. Riavviare l'istanza EC2.

```
shutdown -r -t 20
```

3. Per configurare WSL in modo che utilizzi WSL 1, eseguire il seguente comando sulla propria istanza. Per ulteriori informazioni sull'impostazione della versione WSL, vedere Passaggi per l'installazione manuale delle versioni precedenti di WSL nel sito web Microsoft Build.

```
wsl --set-default-version 1
```

4. Installa la distribuzione predefinita.

```
wsl --install
```

Installa WSL 2

- Per installare WSL, eseguire il seguente comando di installazione standard sull'istanza EC2. Per impostazione predefinita, è installato WSL 2. Se stai installando WSL su un'istanza `.metal`, questo è l'unico passaggio da eseguire.

```
wsl --install
```

Per ulteriori informazioni, consultaInstallare Linux su Windows con WSL sul sito web di Microsoft Build.

Aggiornamento di un'istanza Amazon EC2 Windows a una versione più recente di Windows Server

Esistono due metodi per aggiornare una versione precedente di Windows Server in esecuzione su un'istanza: aggiornamento sul posto e migrazione (denominata anche side-by-side aggiornamento). L'aggiornamento in loco aggiorna i file del sistema operativo senza modificare i file e le impostazioni personali. La migrazione implica l'acquisizione di impostazioni, configurazioni e dati che vengono trasferiti su un sistema operativo più recente su un'istanza Amazon EC2 aggiornata.

In genere Microsoft consiglia di effettuare la migrazione a una versione più recente di Windows Server invece dell'aggiornamento. La migrazione può comportare meno errori o problemi di aggiornamento, ma può impiegare più tempo rispetto a un aggiornamento in loco poiché occorre

effettuare il provisioning di una nuova istanza, pianificare e trasferire le applicazioni e modificare le impostazioni di configurazione sulla nuova istanza. L'aggiornamento in loco può essere più rapido, ma le incompatibilità del software possono causare degli errori.

Indice

Esegui un aggiornamento immediato sull'istanza di Windows

Prima di eseguire un aggiornamento in loco, devi stabilire quali driver di rete sono in esecuzione sull'istanza. I driver di rete PV ti consentono di accedere all'istanza tramite Desktop remoto. Le istanze utilizzano i driver AWS PV, Intel Network Adapter o Enhanced Networking. Per ulteriori informazioni, consulta Driver paravirtuali per le istanze Windows.

Prima di avviare un aggiornamento in loco

Completa le attività seguenti e annota i dettagli importanti riportati di seguito prima di avviare l'aggiornamento in loco.

- Leggi la documentazione Microsoft per informazioni sui requisiti di aggiornamento, i problemi noti e le limitazioni. Rivedi inoltre le istruzioni ufficiali di aggiornamento.
  - Opzioni di aggiornamento per Windows Server 2012
  - Opzioni di aggiornamento per Windows Server 2012 R2
  - Opzioni di aggiornamento e conversione per Windows Server 2016
  - Opzioni di aggiornamento e conversione per Windows Server 2019
  - Opzioni di aggiornamento e conversione per Windows Server 2022
  - Centro di aggiornamento a Windows Server
- Consigliamo di effettuare l'aggiornamento di un sistema operativo su istanze con almeno 2 vCPU e 4GB di RAM. Se necessario, è possibile modificare l'istanza in dimensioni più grandi dello stesso tipo (ad esempio da t2.small a t2.large), eseguire l'aggiornamento e ridimensionarla alle dimensioni originali. Se è necessario mantenere le dimensioni dell'istanza, è possibile monitorare il progresso

utilizzando l'acquisizione di screenshot della console. Per ulteriori informazioni, consulta Cambiare il tipo di istanza.

- Verifica che il volume root dell'istanza Windows disponga di sufficiente spazio libero sul disco. Il processo di Installazione di Windows potrebbe non inviare alcun avviso relativo allo spazio sul disco insufficiente. Per informazioni sulla quantità di spazio sul disco necessaria per aggiornare un sistema operativo specifico, consulta la documentazione Microsoft. Puoi espandere il volume se non è presente spazio sufficiente. Per ulteriori informazioni, consulta Amazon EBS Elastic Volumes nella Amazon EBS User Guide.
- Scegli il percorso di aggiornamento. È necessario aggiornare il sistema operativo alla stessa architettura. Ad esempio, devi aggiornare un sistema a 32-bit a un sistema a 32-bit. Windows Server 2008 R2 e versioni successive sono solo a 64 -bit.
- Disabilita i firewall e i software antivirus e anti-spyware. Questo tipo di software può entrare in conflitto con il processo di aggiornamento. Riabilita i firewall e i software antivirus e anti-spyware al termine dell'aggiornamento.
- Aggiornamenti agli ultimi driver, come descritto in Esegui la migrazione di un'istanza Windows a un tipo di istanza della generazione corrente
- Il servizio dell'helper di aggiornamento supporta soltanto le istanze che eseguono i driver Citrix PV. Se l'istanza esegue i driver Red Hat, è necessario innanzitutto aggiornare tali driver manualmente.

Aggiorna un'istanza sul posto con i driver AWS PV, Intel Network Adapter o Enhanced Networking

Completa la procedura seguente per aggiornare un'istanza Windows Server con i driver di rete AWS PV, i driver della scheda di rete Intel o di Reti avanzate.

Per effettuare un aggiornamento in loco

1. Crea un'AMI del sistema che intendi aggiornare per scopi di backup o di testing. È quindi possibile effettuare l'aggiornamento sulla copia per simulare un ambiente di test. Se l'aggiornamento viene completato, è possibile modificare il traffico su questa istanza con un breve intervallo di inattività. Se l'aggiornamento non riesce, è possibile tornare al backup. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.
2. Assicurati che l'istanza Windows Server utilizzi i driver di rete più recenti.
    a. Per aggiornare il driver AWS PV, consulta. Aggiornamento dei driver PV sulle istanze Windows

b. Per aggiornare il driver ENA, consultaInstalla il driver Elastic Network Adapter (ENA).

c. Per aggiornare i driver Intel, vedi Abilita reti avanzate con l'interfaccia Intel 82599 VF sulle tue istanze EC2

3. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
4. Nel riquadro di navigazione, seleziona Instances (Istanze). Individua l'istanza. Annota l'ID istanza e la zona di disponibilità dell'istanza. Queste informazioni saranno necessarie più avanti in questa procedura.
5. Se stai effettuando l'upgrade da Windows Server 2012 o 2012 R2 a Windows Server 2016, 2019 o 2022, completa la procedura seguente sull'istanza prima di continuare:

   a. Disinstalla il servizio EC2Config. Per ulteriori informazioni, consulta Arresto, riavvio, eliminazione o disinstallazione di EC2Config.

   b. Installare EC2Launch v1 o l'agente EC2Launch v2. Per ulteriori informazioni, consulta Configurazione dell'istanza Windows tramite EC2Launch e Configurare un'istanza Windows tramite EC2Launch v2.

   c. Installa l'agente AWS Systems Manager SSM. Per ulteriori informazioni, consulta Utilizzo dell'SSM Agent nella Guida per l'utente di AWS Systems Manager Systems Manager.
6. Crea un nuovo volume da uno snapshot dei supporti di installazione di Windows Server.

   a. Nel pannello di navigazione, in Elastic Block Store selezionare Snapshots (Snapshot).

   b. Nella barra del filtro, scegli Snapshot pubblici.

   c. Nella barra di ricerca, specifica i seguenti filtri:

      - Scegli Alias proprietario, quindi =, poi amazon.
      - Scegli Descrizione, quindi inizia a digitare **`Windows`**. Seleziona il filtro Windows corrispondente all'architettura del sistema e alla preferenza di lingua a cui stai effettuando l'aggiornamento. Ad esempio, scegli Supporto di installazione Windows 2019 in lingua inglese per effettuare l'aggiornamento a Windows Server 2019.

   d. Seleziona la casella di controllo accanto allo snapshot che corrisponde all'architettura di sistema e alla preferenza di lingua a cui stai eseguendo l'aggiornamento, quindi scegli Azioni, Crea volume da snapshot.

   e. Nella pagina Crea volume, scegli la zona di disponibilità corrispondente all'istanza Windows e seleziona Crea volume.
7. Nel banner Volume creato con successo vol-***`1234567890example`*** nella parte superiore della pagina, scegli l'ID del volume appena creato.

8. Scegliere Actions (Operazioni), Attach Volume (Collega volume).
9. Nella pagina Allega volume, per Istanza ad esempio, seleziona l'ID dell'istanza della tua istanza di Windows, quindi scegli Allega volume.
10. Rendi il nuovo volume disponibile per l'uso seguendo la procedura descritta in Make an Amazon EBS volume disponibile per l'uso.

> **Important**
>
> Non inizializzare il disco perché in questo modo si eliminano i dati esistenti.

11. In Windows PowerShell, passa alla nuova unità di volume. Avviare l'aggiornamento per aprire il volume del supporto dell'installazione collegato all'istanza.

    a. Se si sta effettuando l'aggiornamento a Windows Server 2016 o a versioni più recenti, eseguire quanto riportato di seguito:

    ```
    .\setup.exe /auto upgrade /dynamicupdate disable
    ```

    > **Note**
    >
    > L'esecuzione di setup.exe con l'opzione `/dynamicupdate` impostata su disabilitata impedisce a Windows di installare gli aggiornamenti durante il processo di upgrade di Windows Server, poiché l'installazione degli aggiornamenti durante l'upgrade può causare errori. È possibile installare gli aggiornamenti con Windows Update al termine dell'upgrade.

    Se stai effettuando l'aggiornamento a una versione precedente di Windows Server, esegui quanto riportato di seguito:

    ```
    Sources\setup.exe
    ```

    b. In Select the operating system you want to install (Seleziona il sistema operativo da installare), seleziona lo SKU di installazione completo dell'istanza Windows Server e scegliere Next (Successivo).

    c. In Which type of installation do you want? (Seleziona il tipo di installazione desiderato), scegli Upgrade (Aggiornamento).

d. Completa la procedura guidata.

L'installazione di Windows Server copia ed elabora i file. Dopo alcuni istanti, la sessione di Desktop remoto viene chiusa. Il tempo impiegato per l'aggiornamento dipende dal numero di applicazioni e ruoli del server in esecuzione sull'istanza Windows Server. Il processo di aggiornamento può impiegare da 40 minuti a diverse ore. Durante il processo di aggiornamento, l'istanza non supera il controllo dello stato 1 su 2. Al termine dell'aggiornamento, entrambi i controlli dello stato vengono superati. Puoi controllare il registro di sistema per l'output della console o utilizzare i CloudWatch parametri di Amazon per l'attività del disco e della CPU per determinare se l'aggiornamento sta procedendo.

> **Note**
>
> In caso di aggiornamento a Windows Server 2019, al termine dell'operazione, se lo si desidera, è possibile modificare manualmente lo sfondo del desktop per rimuovere il nome del sistema operativo precedente.

Se l'istanza non ha superato entrambi i controlli dello stato dopo diverse ore, consulta Risolvi i problemi relativi a un aggiornamento su un'istanza di Windows.

Attività post-aggiornamento

1. Accedere all'istanza per avviare un aggiornamento di .NET Framework e riavviare il sistema quando richiesto.
2. Se non l'hai già fatto in un passaggio precedente, installa l'agente EC2Launch v1 o EC2Launch v2. Per ulteriori informazioni, consulta Configurazione dell'istanza Windows tramite EC2Launch e Configurare un'istanza Windows tramite EC2Launch v2.
3. Se hai eseguito l'aggiornamento a Windows Server 2012 R2, ti consigliamo di aggiornare i driver PV ai AWS driver PV. Se hai effettuato l'aggiornamento a un'istanza basata su Nitro, ti consigliamo di installare o aggiornare i driver NVME ed ENA. Per ulteriori informazioni, consulta Windows Server 2012 R2, Installa o aggiorna i driver NVMe utilizzando AWS PowerShell o Abilitazione delle reti avanzate su Windows.
4. Riabilitare i firewall e i software antivirus e anti-spyware.

Esegui un aggiornamento automatico sull'istanza di Windows

È possibile eseguire un aggiornamento automatico delle istanze di Windows e SQL Server AWS con i runbook di AWS Systems Manager automazione.

Indice

Servizi correlati

Nel processo di aggiornamento automatico vengono utilizzati i seguenti AWS servizi:

- AWS Systems Manager. AWS Systems Manager è un'interfaccia potente e unificata per la gestione centralizzata delle AWS risorse. Per ulteriori informazioni, consulta la Guida per l'utente AWS Systems Manager.
- AWS Systems Manager Agent (SSM Agent) è un software Amazon che può essere installato e configurato su un'istanza Amazon EC2, un server locale o una macchina virtuale (VM). SSM Agent consente a Systems Manager di aggiornare, gestire e configurare tali risorse. L'agente elabora le richieste dal servizio Systems Manager nel cloud AWS , quindi le esegue come specificato nella richiesta. Per ulteriori informazioni, consulta Utilizzo dell'SSM Agent nella Guida per l'utente di AWS Systems Manager Systems Manager.
- AWS Systems Manager Runbook SSM. Un runbook SSM definisce le operazioni eseguite da Systems Manager sulle istanze gestite. I runbook SSM utilizzano JavaScript Object Notation (JSON) o YAML e includono passaggi e parametri specificati dall'utente. Questo argomento prevede l'uso di due documenti SSM Systems Manager per l'automazione. Per ulteriori informazioni, consulta la Documentazione di riferimento del runbook di automazione di AWS Systems Manager nella Guida per l'utente di AWS Systems Manager .

Opzioni di esecuzione

Una volta selezionato Automation (Automazione) nella console di Systems Manager, selezionare Execute (Esegui). Dopo aver selezionato un documento di automazione, viene richiesto di scegliere un'opzione di esecuzione per l'automazione. Seleziona una delle opzioni seguenti. Nelle fasi per i

percorsi forniti più avanti in questo argomento viene utilizzata l'opzione Simple execution (Esecuzione semplice).

Esecuzione semplice

Scegli questa opzione per aggiornare una singola istanza senza però esaminare ogni fase dell'automazione per verificare i risultati. Questa opzione è spiegata nei dettagli nelle fasi di aggiornamento descritte di seguito.

Rate control (Controllo velocità)

Scegli questa opzione per applicare l'aggiornamento a più di una istanza. Puoi definire le impostazioni seguenti.

- Parameter

  Questa impostazione, configurata anche nelle impostazioni per Multi-Account and Region, definisce come si dirama l'automazione.
- Targets

  Seleziona la destinazione in cui applicare l'automazione. Questa impostazione è configurata anche nelle impostazioni per Multi-Account and Region.
- Parameter Values

  Utilizza i valori definiti nei parametri del documento di automazione.
- Resource Group

  In AWS, una risorsa è un'entità con cui puoi lavorare. Gli esempi includono istanze Amazon EC2, AWS CloudFormation stack o bucket Amazon S3. Se lavori con più risorse, potrebbe essere utile gestirle in gruppo anziché passare da un AWS servizio all'altro per ogni attività. In alcuni casi potresti voler gestire grandi quantità di risorse correlate, ad esempio delle istanze EC2 che formano un livello applicativo. In questo caso è probabile che sia necessario eseguire contemporaneamente azioni in blocco su queste risorse.
- Tag

  I tag consentono di classificare AWS le risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Questa categorizzazione è utile quando disponi di numerose risorse dello stesso tipo. Puoi così identificare velocemente una risorsa specifica in base ai tag a questa assegnati.
- Rate control

Questa impostazione è configurata anche nelle impostazioni per Multi-Account and Region. Quando imposti i parametri di controllo della velocità, definisci in che misura applicare l'automazione al tuo parco istanze, come conteggio delle destinazioni o come percentuale del parco istanze.

Multi-Account and Region

Oltre ai parametri specificati in Rate Control e utilizzate anche nelle impostazioni per Multi-Account and Region, sono presenti altre due impostazioni:

- Accounts and organizational units (OUs)

  Specifica più account su cui eseguire l'automazione.
- Regioni AWS

  Specificane più punti Regioni AWS in cui desideri eseguire l'automazione.

Esecuzione manuale

Simile a Simple execution (Esecuzione semplice), questa opzione consente di entrare in ciascuna fase dell'automazione per verificare i risultati.

Aggiornamento di Windows Server

Il runbook di `AWSEC2-CloneInstanceAndUpgradeWindows` crea un'Amazon Machine Image (AMI) da un'istanza Windows Server nel proprio account e aggiorna l'AMI a una versione supportata di propria scelta. Si tratta di una procedura in più fasi il cui completamento può richiedere fino a due ore.

Nella procedura di aggiornamento automatizzata sono incluse due AMI:

- Istanza attualmente in esecuzione. La prima AMI è l'istanza attualmente in esecuzione, che non è aggiornata. Questa AMI viene utilizzata per avviare un'altra istanza per eseguire l'aggiornamento locale. Una volta completato il processo, l'AMI viene eliminata dall'account, a meno che tu non richieda specificatamente di mantenere l'istanza originale. È un'impostazione gestita dal parametro `KeepPreUpgradeImageBackUp` (il cui valore predefinito è `false`, ovvero di default l'AMI viene rimossa).
- AMI aggiornata. Questa AMI è il risultato della procedura di automazione.

Il risultato finale è un'unica AMI, che è l'istanza aggiornata dell'AMI.

Una volta completato l'aggiornamento, è possibile testare la funzionalità dell'applicazione lanciando la nuova AMI nel Amazon VPC in uso. Al termine del test e prima di eseguire un altro aggiornamento, pianifica il tempo di inattività dell'applicazione prima di passare in modo definitivo all'istanza aggiornata.

Prerequisiti

Per automatizzare l'aggiornamento di Windows Server con il documento di AWS Systems Manager automazione, è necessario eseguire le seguenti attività:

- Crea un ruolo IAM con le policy IAM specificate per consentire ad Systems Manager di eseguire le attività di automazione sulle istanze Amazon EC2 e verificare che siano soddisfatti i prerequisiti per utilizzare Systems Manager. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'AWS Identity and Access Management utente.
- Seleziona l'opzione per la modalità di esecuzione dell'automazione. Le opzioni di esecuzione sono Simple execution (Esecuzione semplice), Rate control (Controllo velocità), Multi-account and Region (Più account e regioni) e Manual execution (Esecuzione manuale). Per ulteriori informazioni su queste opzioni, consulta Opzioni di esecuzione.
- Verificare che SSM Agent sia installato nell'istanza. Per ulteriori informazioni, consultare Installazione e configurazione del SSM Agent sulle istanze Amazon EC2 per Windows Server.
- È necessario installare Windows PowerShell 3.0 o versione successiva sull'istanza.
- Per le istanze che vengono aggiunte a un dominio Microsoft Active Directory, si consiglia di specificare un `SubnetId` che non dispone di connettività ai controller di dominio per evitare conflitti di nomi host.
- La sottorete dell'istanza deve disporre di connettività in uscita a Internet, che consente l'accesso Servizi AWS ad Amazon S3 e l'accesso al download di patch da Microsoft. Questo requisito è soddisfatto se la sottorete è una sottorete pubblica e l'istanza ha un indirizzo IP pubblico o se la sottorete è una sottorete privata con un percorso che invia il traffico Internet a un dispositivo NAT pubblico.
- Questa automazione funziona con istanze in esecuzione su Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 e Windows Server 2019
- Verificare che l'istanza disponga di 20 GB di spazio sul disco di avvio.
- Se l'istanza non utilizza una licenza Windows fornita da AWS, specifica un ID snapshot di Amazon EBS che includa i supporti di installazione di Windows Server 2012 R2. Per farlo:

1. Verificare che l'istanza Amazon EC2 esegua Windows Server 2012 o versioni successive.
2. Creare un volume Amazon EBS da 6 GB nella stessa zona di disponibilità in cui l'istanza è in esecuzione. Collegare il volume all'istanza. Montare il volume, ad esempio come unità D.
3. Fare clic con il pulsante destro del mouse sull'oggetto ISO e montarlo su un'istanza, ad esempio, sull'unità E.
4. Copiare il contenuto dell'oggetto ISO dall'unità E:\ all'unità D:\
5. Creare uno snapshot Amazon EBS del volume da 6 GB creato nella precedente fase 2.

Limitazioni dell'aggiornamento per Windows Server

Questa automazione non supporta l'aggiornamento di controller di dominio Windows, cluster o sistemi operativi per desktop Windows. Questa automazione, inoltre, non supporta le istanze Amazon EC2 per Windows Server con i seguenti ruoli installati:

- Remote Desktop Session Host (RDSH)
- Remote Desktop Connection Broker (RDCB)
- Remote Desktop Virtualization Host (RDVH)
- Remote Desktop Web Access (RDWA)

Procedura per eseguire un aggiornamento automatico di Windows Server

Segui questi passaggi per aggiornare l'istanza di Windows Server utilizzando il runbook di automazione a AWSEC2. CloneInstanceAndUpgradeWindows

1. Aprire Systems Manager dalla Console di gestione AWS .
2. Nel riquadro di navigazione a sinistra, in Change Management (Gestione delle modifiche), scegliere Automation (Automazione).
3. Selezionare Execute automation (Esegui automazione).
4. Cercare il documento di automazione denominato `AWSEC2-CloneInstanceAndUpgradeWindows`.
5. Quando compare il nome del documento, selezionarlo. Una volta selezionato, vengono visualizzati i dettagli del documento.
6. Scegliere Execute automation (Esegui automazione) per inserire i parametri per questo documento. Lasciare selezionato Simple execution (Esecuzione semplice) in alto nella pagina.
7. Immettere i parametri richiesti in base alle indicazioni seguenti.

- `InstanceID`

  Tipo: stringa

  (Obbligatorio) L'istanza che esegue Windows Server 2008 R2, 2012 R2, 2016 o 2019 con l'agente SSM installato.

- `InstanceProfile`.

  Tipo: stringa

  (Obbligatorio) Il profilo dell'istanza IAM. Questo è il ruolo IAM utilizzato per eseguire l'automazione di Systems Manager sull'istanza Amazon EC2 e AWS sulle AMI. Per ulteriori informazioni, consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager .

- `TargetWindowsVersion`

  Tipo: stringa

  (Obbligatorio) Selezionare la versione di Windows di destinazione.

- `SubnetId`

  Tipo: stringa

  (Obbligatorio) La sottorete per la procedura di aggiornamento, in cui risiede l'istanza EC2. Verifica che la sottorete disponga di connettività in uscita ai AWS servizi, incluso Amazon S3, e anche a Microsoft (per scaricare le patch).

- `KeepPreUpgradedBackUp`

  Tipo: stringa

  (Facoltativo) Se questo parametro è impostato su `true`, l'automazione mantiene l'immagine creata dall'istanza. L'impostazione predefinita è `false`.

- `RebootInstanceBeforeTakingImage`

  Tipo: stringa

  (Facoltativo) L'impostazione predefinita è `false` (nessun riavvio). Se questo parametro è impostato su `true`, Systems Manager riavvia l'istanza prima di creare un'AMI per l'aggiornamento.

8. Dopo avere immesso i parametri, selezionare Execute (Esegui). Una volta avviata l'automazione, è possibile monitorare l'avanzamento dell'esecuzione.
9. Terminata l'automazione, sarà visualizzato l'ID dell'AMI. È possibile avviare l'AMI per verificare l'aggiornamento del sistema operativo Windows.

> **Note**
>
> L'automazione non deve necessariamente eseguire tutte le fasi. Le fasi dipendono dal comportamento dell'automazione e dell'istanza. Systems Manager potrebbe ignorare alcuni passaggi non richiesti.
> Inoltre, alcune fasi potrebbero scadere. Systems Manager tenta di aggiornare e installare tutte le patch più recenti. A volte, tuttavia, si verificano timeout in funzione di un'impostazione di timeout definibile per una determinata fase. In questi casi, il servizio di automazione di Systems Manager continua con la fase successiva per garantire che il sistema operativo interno venga aggiornato alla versione Windows Server di destinazione.

10. Una volta completata l'automazione, è possibile avviare un'istanza Amazon EC2 tramite l'ID dell'AMI per verificare l'aggiornamento. Per ulteriori informazioni su come creare un'istanza Amazon EC2 da un' AWS AMI, vedi Come posso lanciare un'istanza EC2 da un'AMI personalizzata?

Aggiornamento di SQL Server

Lo script `AWSEC2-CloneInstanceAndUpgradeSQLServer` crea un'AMI da un'istanza Amazon EC2 con SQL Server in esecuzione nell'account, quindi aggiorna l'AMI a una versione più recente di SQL Server. Si tratta di una procedura in più fasi il cui completamento può richiedere fino a due ore.

In questo flusso di lavoro, l'automazione crea un'AMI dall'istanza e quindi avvia la nuova AMI creata nella sottorete specificata. L'automazione esegue quindi un aggiornamento locale di SQL Server. Una volta completato l'aggiornamento, l'automazione crea una nuova AMI prima di terminare l'istanza aggiornata.

Nella procedura di aggiornamento automatizzata sono incluse due AMI:

- Istanza attualmente in esecuzione. La prima AMI è l'istanza attualmente in esecuzione, che non è aggiornata. Questa AMI viene utilizzata per avviare un'altra istanza per eseguire l'aggiornamento locale. Una volta completato il processo, l'AMI viene eliminata dall'account, a meno che tu non

richieda specificatamente di mantenere l'istanza originale. È un'impostazione gestita dal parametro `KeepPreUpgradeImageBackUp` (il cui valore predefinito è `false`, ovvero di default l'AMI viene rimossa).

- AMI aggiornata. Questa AMI è il risultato della procedura di automazione.

Il risultato finale è un'unica AMI, che è l'istanza aggiornata dell'AMI.

Una volta completato l'aggiornamento, è possibile testare la funzionalità dell'applicazione lanciando la nuova AMI nel Amazon VPC in uso. Al termine del test e prima di eseguire un altro aggiornamento, pianifica il tempo di inattività dell'applicazione prima di passare in modo definitivo all'istanza aggiornata.

Prerequisiti

Per automatizzare l'aggiornamento di SQL Server con il documento di AWS Systems Manager automazione, devi eseguire le seguenti attività:

- Crea un ruolo IAM con le policy IAM specificate per consentire ad Systems Manager di eseguire le attività di automazione sulle istanze Amazon EC2 e verificare che siano soddisfatti i prerequisiti per utilizzare Systems Manager. Per ulteriori informazioni, consulta la pagina relativa alla creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di AWS Identity and Access Management .
- Seleziona l'opzione per la modalità di esecuzione dell'automazione. Le opzioni di esecuzione sono Simple execution (Esecuzione semplice), Rate control (Controllo velocità), Multi-account and Region (Più account e regioni) e Manual execution (Esecuzione manuale). Per ulteriori informazioni su queste opzioni, consulta Opzioni di esecuzione.
- L'istanza Amazon EC2 deve utilizzare una versione uguale o successiva a di Windows Server 2008 R2 e SQL Server 2008 (o versione successiva).
- Verificare che SSM Agent sia installato nell'istanza. Per ulteriori informazioni, consulta Installazione e configurazione di SSM Agent sulle istanze Amazon EC2 per Windows Server.
- Verificare che l'istanza disponga di sufficiente spazio libero sul disco:
  - Se si esegue l'aggiornamento da Windows Server 2008 R2 a 2012 R2, oppure da Windows Server 2012 R2 a un sistema operativo successivo, verificare di disporre di 20 GB di spazio libero sul disco di avvio dell'istanza.
  - Se si esegue l'aggiornamento da Windows Server 2008 R2 a 2016 o successivo, verificare che l'istanza disponga di 40 GB di spazio libero sul disco di avvio dell'istanza.

- Per istanze che utilizzano una versione Bring-Your-Own-License (uso di licenze proprie) di SQL Server, si applicano i seguenti prerequisiti aggiuntivi:
  - Specificare un ID snapshot Amazon EBS contenente il supporto di installazione di SQL Server. Per farlo:
    1. Verificare che l'istanza Amazon EC2 esegua Windows Server 2008 R2 o versioni successive.
    2. Creare un volume Amazon EBS da 6 GB nella stessa zona di disponibilità in cui l'istanza è in esecuzione. Collegare il volume all'istanza. Montare il volume, ad esempio come unità D.
    3. Fare clic con il pulsante destro del mouse sull'oggetto ISO e montarlo su un'istanza, ad esempio, sull'unità E.
    4. Copiare il contenuto dell'oggetto ISO dall'unità E:\ all'unità D:\
    5. Creare uno snapshot Amazon EBS del volume da 6 GB creato nella fase 2.

Limitazioni dell'aggiornamento automatico per SQL Server

Le seguenti limitazioni si applicano quando si utilizza il runbook AWSECCloneInstanceAndUpgrade2-SQLServer per eseguire un aggiornamento automatico:

- L'aggiornamento può essere eseguito solo su un'istanza SQL Server che usa l'autenticazione di Windows.
- Verificare che sulle istanze non siano presenti aggiornamenti delle patch di sicurezza in sospeso. Aprire Control Panel (Pannello di controllo), quindi scegliere Check for updates (Verifica disponibilità aggiornamenti).
- Le distribuzioni di SQL Server in modalità HA (High Availability, disponibilità elevata) e mirroring non sono supportate.

Procedura per eseguire un aggiornamento automatico di SQL Server

Segui questi passaggi per aggiornare SQL Server utilizzando il runbook di automazione AWSECCloneInstanceAndUpgrade2-SQLServer.

1. Se non è già stato fatto, scaricare il file .iso di SQL Server 2016 e montarlo sul server di origine.
2. Una volta completato questo passaggio, copiare tutti i file dei componenti e posizionarli in un volume a scelta.

3. Eseguire uno snapshot Amazon EBS del volume e copiare l'ID snapshot negli appunti per usarlo in un secondo momento. Per ulteriori informazioni, consulta Create snapshot Amazon EBS nella Amazon EBS User Guide.
4. Collegare il profilo dell'istanza all'istanza Amazon EC2 di origine. Ciò consente a Systems Manager di comunicare con l'istanza EC2 ed eseguire comandi su di essa dopo che è stata aggiunta al AWS Systems Manager servizio. Per questo esempio, il ruolo è stato denominato `SSM-EC2-Profile-Role` con la policy `AmazonSSMManagedInstanceCore` collegata al ruolo stesso. Consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager .
5. Nella AWS Systems Manager console, nel riquadro di navigazione a sinistra, scegli Managed Instances. Verificare che l'istanza EC2 sia presente nell'elenco delle istanze gestite. Se l'istanza non viene visualizzata dopo qualche secondo, consulta Dove sono le mie istanze? nella Guida per l'utente di AWS Systems Manager .
6. Nel riquadro di navigazione a sinistra, sottoGestione delle modifichescegliereAutomazione.
7. Selezionare Execute automation (Esegui automazione).
8. Cercare il documento di automazione denominato `AWSEC2-CloneInstanceAndUpgradeSQLServer`.
9. Scegliere il documento SSM `AWSEC2-CloneInstanceAndUpgradeSQLServer`, quindi scegliere Next (Successivo).
10. Assicurarsi che sia selezionata l'opzione Simple execution (Esecuzione semplice).
11. Immettere i parametri richiesti in base alle indicazioni seguenti.

    - `InstanceId`

      Tipo: stringa

      (Obbligatorio) L'istanza su cui è in esecuzione SQL Server 2008 R2 (o versioni successive).
    - `IamInstanceProfile`

      Tipo: stringa

      (Obbligatorio) Il profilo dell'istanza IAM.
    - `SQLServerSnapshotId`

      Tipo: stringa

(Obbligatorio) L'ID snapshot del supporto di installazione di SQL Server. Questo parametro non è richiesto per le istanze di SQL Server. incluse in licenza

- `SubnetId`

  Tipo: stringa

  (Obbligatorio) La sottorete per la procedura di aggiornamento, in cui risiede l'istanza EC2. Verifica che la sottorete disponga di connettività in uscita ai AWS servizi, incluso Amazon S3, e anche a Microsoft (per scaricare le patch).

- `KeepPreUpgradedBackUp`

  Tipo: stringa

  (Facoltativo) Se questo parametro è impostato su `true`, l'automazione mantiene l'immagine creata dall'istanza. L'impostazione predefinita è `false`.

- `RebootInstanceBeforeTakingImage`

  Tipo: stringa

  (Facoltativo) L'impostazione predefinita è `false` (nessun riavvio). Se questo parametro è impostato su `true`, Systems Manager riavvia l'istanza prima di creare un'AMI per l'aggiornamento.

- `TargetSQLVersion`

  ▬Tipo: stringa

  (Facoltativo) La versione di SQL Server di destinazione. Il valore predefinito è `2016`.

12. Dopo avere immesso i parametri, selezionare Execute (Esegui). Una volta avviata l'automazione, è possibile monitorare l'avanzamento dell'esecuzione.
13. Quando Execution status (Stato esecuzione) indica Riuscito, espandere Outputs (Output) per visualizzare le informazioni sull'AMI. È possibile utilizzare l'ID AMI per avviare l'istanza SQL Server nel VPC preferito.
14. Aprire la console Amazon EC2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI). Verrà visualizzata la nuova AMI.
15. Per verificare la corretta installazione di SQL Server, scegliere la nuova AMI, quindi Launch (Avvia).

16. Scegliere il tipo di istanza desiderata per l'AMI, il VPC e la sottorete in cui distribuirla e l'archiviazione da utilizzare. Poiché l'avvio della nuova istanza avviene da un'AMI, i volumi sono presentati come un'opzione da includere nell'istanza EC2 da avviare. È possibile rimuovere tali volumi o aggiungerne altri.
17. Aggiungere un tag per facilitare l'identificazione dell'istanza.
18. Aggiungere all'istanza il gruppo o i gruppi di sicurezza.
19. Scegliere Launch Instance (Avvia istanza).
20. Scegliere il nome del tag per l'istanza e selezionare Connect (Connetti) nel menu a discesa Actions (Operazioni).
21. Verificare che la versione di SQL Server sia il nuovo motore di database sulla nuova istanza.

Esegui la migrazione di un'istanza Windows a un tipo di istanza della generazione corrente

Le AMI AWS Windows sono configurate con le impostazioni predefinite utilizzate dai supporti di installazione Microsoft, con alcune personalizzazioni. Le personalizzazioni includono driver e configurazioni che supportano i tipi di istanze di ultima generazione, che sono istanze basate sul sistema AWS Nitro, come M5 o C5.

Tuttavia, quando si esegue la migrazione alle istanze supportate da Nitro, incluse le istanze bare metal, si consiglia di seguire le fasi descritte in questo argomento nei seguenti casi:

- Se si stanno avviando istanze dalle AMI di Windows personalizzate
- Se si stanno avviando istanze dalle AMI di Windows fornite da Amazon create prima di agosto 2018

Per ulteriori informazioni, consulta Aggiornamento di Amazon EC2: altri tipi di istanza, sistema Nitro e opzioni CPU.

> **Note**
>
> Le procedure di migrazione seguenti possono essere eseguite in Windows Server 2008 R2 e versioni successive. Per migrare le istanze Linux ai tipi di istanze di ultima generazione, consulta. the section called “Cambiare il tipo di istanza”

Indice

> **Note**
>
> In alternativa, puoi utilizzare il documento di automazione `AWSSupport-UpgradeWindowsAWSDrivers` per automatizzare le procedure descritte nelle parti 1, 2 e 3. Se scegli di utilizzare la procedura automatizzata, vedi (Alternativa) Aggiornate i AWS driver PV, ENA e NVMe utilizzando AWS Systems Manager, quindi continua con le parti 4 e 5.

Prima di iniziare

Questa procedura presuppone che tu stia attualmente utilizzando un tipo di istanza basata su Xen di generazione precedente, come M4 o C4, e che tu stia migrando a un'istanza basata sul sistema Nitro. AWS

È necessario utilizzare la PowerShell versione 3.0 o successiva per eseguire correttamente l'aggiornamento.

> **Note**
>
> Durante la migrazione a istanze di ultima generazione, le configurazioni di rete DNS personalizzate o l'IP statico sull'ENI esistente potrebbero andare perse, poiché l'istanza passerà in modo predefinito a un nuovo dispositivo Enhanced Networking Adapter.

Prima di seguire la procedura della guida, si consiglia di creare un backup dell'istanza. Dalla console EC2 scegli l'istanza che deve effettuare la migrazione, apri il menu contestuale (pulsante destro del mouse) e seleziona Instance State (Stato istanza), quindi Stop (Arresta).

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per conservare i dati nei volumi di archivio istanza, eseguire il backup di tutti i dati dei volumi in un'archiviazione persistente.

Apri il menu contestuale (pulsante destro del mouse) dell'istanza nella console EC2, scegli Image (Immagine), quindi Create Image (Crea immagine).

> **Note**
>
> Le parti 4 e 5 di queste istruzioni possono essere completate dopo aver migrato o modificato il tipo di istanza all'ultima generazione. Tuttavia, ti consigliamo di completarle prima della migrazione se stai migrando specificamente verso un tipo di istanza bare metal.

Parte 1: installazione e aggiornamento dei driver PV AWS

Sebbene i driver AWS PV non siano utilizzati nel sistema Nitro, è comunque necessario aggiornarli se si utilizzano versioni precedenti di Citrix PV o PV. AWS Gli ultimi driver AWS PV risolvono i bug delle precedenti versioni, che possono comparire quando operi in un sistema NItro o se ti occorre tornare a un'istanza basato su Xen. Come procedura ottimale, consigliamo di eseguire sempre l'aggiornamento ai driver più recenti per le istanze Windows attive. AWS

Utilizzate la seguente procedura per eseguire un aggiornamento sul posto dei driver AWS PV o per eseguire l'aggiornamento dai driver Citrix PV ai driver AWS PV su Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019. Per ulteriori informazioni, consulta Aggiornamento dei driver PV sulle istanze Windows.

Per aggiornare un controller di dominio, consulta Aggiornare un controller di dominio (aggiornamento PV)AWS

Per eseguire un aggiornamento o ai driver PV AWS

1. Connettiti all'istanza utilizzando Desktop remoto e prepara l'istanza per l'aggiornamento. Disconnetti tutti i dischi non del sistema prima di eseguire l'aggiornamento. Se si esegue un aggiornamento diretto dei driver AWS PV, questo passaggio non è necessario. Imposta i servizi non essenziali sull'avvio Manual (Manuale) nella console Servizi.
2. Scarica il pacchetto di driver più recente per l'istanza.
3. Estrai i contenuti della cartella ed esegui `AWSPVDriverSetup.msi`.

Dopo avere eseguito l'MSI, l'istanza si riavvia automaticamente e aggiorna il driver. L'istanza potrebbe non essere disponibile per un massimo di 15 minuti.

Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli dello stato nella console Amazon EC2, connettiti all'istanza utilizzando Desktop remoto e verifica che il nuovo driver sia installato. In Gestione dispositivi, in Controller di storage, individua AWS Scheda host storage PV. Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS cronologia dei pacchetti di driver PV.

Parte 2: installare e aggiornare ENA

Effettua l'aggiornamento al driver Elastic Network Adapter più recente per garantire che siano supportate tutte le funzionalità di rete. Se è stata avviata l'istanza ma la funzionalità di reti avanzate non è già abilitata, è necessario scaricare e installare il driver per la scheda di rete richiesto sull'istanza. Quindi imposta l'attributo di istanza enaSupport per attivare le reti avanzate. Puoi abilitare questo attributo solo sui tipi di istanza supportati e solo se il driver ENA è installato. Per ulteriori informazioni, consulta Abilita una rete avanzata con l'Elastic Network Adapter (ENA) sulle tue istanze EC2.

1. Scarica il driver più recente per l'istanza. Se è necessaria una versione precedente del driver, consulta. the section called “Driver ENA per Windows”
2. Estrai l'archivio .zip.
3. Installa il driver eseguendo lo `install.ps1` PowerShell script dalla cartella estratta.

> **Note**
>
> Per evitare errori di installazione, esegui lo script `install.ps1` come amministratore.

4. Verifica che enaSupport sia attivato per l'AMI. In caso contrario, prosegui seguendo la documentazione in Abilita una rete avanzata con l'Elastic Network Adapter (ENA) sulle tue istanze EC2.

Parte 3: aggiornamento dei driver AWS NVMe

AWS I driver NVMe vengono utilizzati per interagire con i volumi di archiviazione delle istanze Amazon EBS e SSD esposti come dispositivi a blocchi NVMe nel sistema Nitro per prestazioni migliori.

> **Important**
>
> Le seguenti istruzioni vengono modificate specificamente per quando si installa o si aggiorna AWS NVMe su un'istanza di generazione precedente con l'intenzione di migrare l'istanza al tipo di istanza di ultima generazione.

1. Scarica il pacchetto di driver più recente per l'istanza.
2. Estrai l'archivio .zip.
3. Installa il driver eseguendo `dpinst.exe`.
4. Apri una PowerShellsessione ed esegui il comando seguente:

```
PS C:\> start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

> **Note**
>
> Per applicare il comando, è necessario eseguire la PowerShell sessione come amministratore. PowerShell Le versioni (x86) genereranno un errore.
> Questo comando esegue sysprep solo sui driver dei dispositivi. Non esegue la preparazione completa di sysprep.

5. Per Windows Server 2008 R2 e Windows Server 2012, arrestare l'istanza, modificare il tipo di istanza in un tipo di ultima generazione e avviarla, quindi continuare con la Parte 4. Se avvii nuovamente l'istanza in un tipo di una generazione precedente prima di eseguire la migrazione verso un tipo di istanza di ultima generazione, l'istanza non verrà avviata. Per le altre AMI Windows supportate, è possibile modificare il tipo di istanza in qualsiasi momento dopo il sysprep del dispositivo.

Parte 4: aggiornare EC2Config ed EC2Launch

Per le istanze Windows, le ultime utilità EC2Config ed EC2Launch forniscono funzionalità e informazioni aggiuntive, se eseguite sul sistema Nitro, incluso Bare Metal EC2. Per impostazione predefinita, il servizio EC2Config è incluso nelle AMI da prima di Windows Server 2016. EC2Launch sostituisce il servizio EC2Config sulle AMI di Windows Server 2016 o versione successiva.

Quando i servizi EC2Config ed EC2Launch vengono aggiornati, le nuove AMI di Windows da AWS includono la versione più recente del servizio. Tuttavia, è necessario aggiornare le AMI di Windows e le istanze con la versione più recente di EC2Config e di EC2Launch.

Per installare o aggiornare EC2Config

1. Scarica e decomprimi il programma di installazione di EC2Config.
2. Esegui `EC2Install.exe`. Per un elenco completo delle opzioni, esegui `EC2Install` con l'opzione `/?`. Per impostazione predefinita, la configurazione mostra i prompt. Per eseguire il comando senza alcun prompt, utilizza l'opzione `/quiet`.

Per ulteriori informazioni, consulta Installazione della versione più recente di EC2Config.

Per installare o aggiornare EC2Launch

1. Se EC2Launch è già stato installato e configurato su un'istanza, eseguire un backup del file di configurazione di EC2Launch. Il processo di installazione non conserva le modifiche apportate a questo file. Per impostazione predefinita, il file si trova nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Scaricare EC2-Windows-Launch.zip in una directory dell'istanza.
3. Scaricare install.ps1 nella stessa directory in cui è stato scaricato `EC2-Windows-Launch.zip`.
4. Esegui `install.ps1`.

> **Note**
>
> Per evitare errori di installazione, esegui lo script `install.ps1` come amministratore.

5. Se è stato eseguito il backup del file di configurazione di EC2Launch, copiarlo nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Per ulteriori informazioni, consulta Configurazione dell'istanza Windows tramite EC2Launch.

Parte 5: installare il driver di porta seriale per le istanze bare metal

Il tipo di istanza `i3.metal` utilizza un dispositivo seriale basato su PCI anziché su porte I/O. Le ultime AMI Windows utilizzano automaticamente il dispositivo seriale basato su PCI e hanno il driver di porta seriale installato. Se non utilizzi un'istanza avviata da un'AMI Windows fornita da Amazon datata 11/04/2018 o in data successiva, devi installare il driver di porta seriale per attivare funzioni EC2 nel dispositivo seriale, come la generazione di password e l'output della console. Le ultime utilità EC2Config ed EC2Launch supportano anche i3.metal e forniscono funzionalità aggiuntive, pertanto segui i passaggi della parte 4, se non l'hai ancora fatto.

Per installare il driver di porta seriale

1. Scarica il pacchetto di driver seriale per l'istanza.
2. Estrai il contenuto della cartella, apri il menu contestuale (pulsante destro del mouse) per `aws_ser.INF` e seleziona Install (Installa).
3. Seleziona Okay.

Parte 6: aggiornare le impostazioni di risparmio energia

Il seguente aggiornamento alle impostazioni di Power Management imposta lo spegnimento del display su mai, per consentire arresti regolari del sistema operativo sul sistema Nitro. Tutte le AMI Windows fornite da Amazon al 28.11. 2018 hanno già questa configurazione predefinita.

1. Aprire un prompt dei comandi o PowerShell una sessione.
2. Esegui i comandi seguenti:

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Parte 7: aggiornare i driver Intel Chipset per nuovi tipi di istanza

I tipi di istanza `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` utilizzano l'hardware che richiede i driver chipset precedentemente installati sulle AMI di Windows. Se non utilizzi un'istanza avviata da un'AMI Windows fornita da Amazon datata 19/11/2018 o in data successiva, devi installare i driver utilizzando l'utilità INF Intel Chipset.

Per installare i driver chipset

1. Scarica l'utilità del chipset nell'istanza.
2. Estrai i file.
3. Esegui `SetupChipset.exe`.
4. Accetta l'accordo di licenza del software Intel e installa i driver chipset.
5. Riavviare l'istanza.

(Alternativa) Aggiornate i AWS driver PV, ENA e NVMe utilizzando AWS Systems Manager

Il documento di automazione `AWSSupport-UpgradeWindowsAWSDrivers` automatizza le fasi descritte in Parte 1, Parte 2 e Parte 3. Questo metodo può anche riparare un'istanza in cui non è stato possibile eseguire gli aggiornamenti dei driver.

Il documento di `AWSSupport-UpgradeWindowsAWSDrivers` automazione aggiorna o ripara i AWS driver di storage e di rete sull'istanza EC2 specificata. Il documento tenta di installare le versioni più recenti dei AWS driver online chiamando l' AWS Systems Manager agente (agente SSM). Se l'agente SSM non è contattabile, il documento può eseguire un'installazione offline dei AWS driver se richiesto esplicitamente.

> **Note**
>
> Questa procedura non andrà a buon fine su un controller di dominio. Per aggiornare i driver su un controller di dominio, consulta Aggiornare un controller di dominio (aggiornamento PV)AWS.

Per aggiornare automaticamente i driver AWS PV, ENA e NVMe utilizzando AWS Systems Manager

1. Apri la console Systems Manager all'indirizzo https://console.aws.amazon.com/systems-manager.
2. Seleziona Automation (Automazione), Execute Automation (Esecuzione automazione).
3. Cerca e seleziona il documento AWSSupport- UpgradeWindows AWSDrivers automazione, quindi scegli Esegui automazione.
4. Nella sezione Parametri di input, configura le seguenti opzioni:

   ID istanza

   Immetti l'ID univoco dell'istanza da aggiornare.

   AllowOffline

   (Facoltativo) Seleziona una delle seguenti tre opzioni:

   - `True` — Scegli questa opzione per eseguire l'installazione offline. Durante il processo di aggiornamento, l'istanza viene arrestata e riavviata.

     > **Warning**
     >
     > Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per conservare i dati nei volumi di instance store, esegui il backup di tutti i dati dei volumi in uno storage persistente.

   - `False` — (Predefinito) Lascia questa opzione selezionata per eseguire l'installazione online. Durante il processo di aggiornamento, l'istanza viene riavviata.

     > **Important**
     >
     > Gli aggiornamenti online e offline creano un'AMI prima di provare le operazioni di aggiornamento. L'AMI persiste dopo il completamento dell'automazione. Proteggi l'accesso all'AMI o eliminarla, se non è più necessaria.

   SubnetId

   (Facoltativo) Immetti uno dei seguenti valori:

- `SelectedInstanceSubnet` — (Predefinito) Il processo di aggiornamento avvia l'istanza helper nella stessa sottorete dell'istanza da aggiornare. La sottorete deve consentire la comunicazione verso gli endpoint Systems Manager (`ssm.*`).
- `CreateNewVPC` — Il processo di aggiornamento avvia l'istanza helper in un nuovo VPC. Utilizza questa opzione se non sei sicuro che la sottorete dell'istanza di destinazione consenta la comunicazione verso gli endpoint `ssm.*`. L'utente deve disporre delle autorizzazioni per creare un VPC.
- ID di una sottorete specifica — Specificare l'ID di una sottorete specifica in cui avviare l'istanza helper. La sottorete deve trovarsi nella stessa zona di disponibilità dell'istanza da aggiornare e deve consentire la comunicazione con gli endpoint `ssm.*`.

5. Scegliere Execute (Esegui).
6. Consenti il completamento dell'aggiornamento. Per completare un aggiornamento online possono essere necessari fino a 10 minuti, mentre per quello offline fino a 25 minuti.

Esegui la migrazione di un'istanza Windows dai tipi di istanza Nitro ai tipi di istanza Xen

La procedura seguente presuppone che si stia attualmente utilizzando un tipo di istanza basato su Nitro e che si stia migrando verso un'istanza basata sul sistema Xen, come M4 o C4. Per le specifiche del tipo di istanza, consulta la Amazon EC2 Instance Types Guide. Esegui la procedura seguente prima della migrazione per evitare errori durante il processo di avvio.

Per migrare da Nitro a Xen

1. Eseguire il backup dei dati.
2. Verifica che la policy SAN di Windows consenta la connessione online di volumi di storage non root.
3. AWS I driver PV devono essere installati e aggiornati su un'istanza Nitro prima di migrare a un'istanza Xen. Per la procedura di installazione e aggiornamento AWS dei driver PV, consulta. Parte 1: installazione e aggiornamento dei driver PV AWS
4. Esegui l'aggiornamento alla versione EC2Launch v2 più recente. Per le fasi, consulta Migrazione a EC2Launch v2.
5. Apri una PowerShell sessione ed esegui il seguente comando come amministratore per sysprep i driver del dispositivo. L'esecuzione di sysprep garantisce che i driver di archiviazione di avvio anticipato necessari per l'avvio su istanze Xen siano correttamente registrati con Windows.

> **Note**
>
> L'esecuzione del comando utilizzando le versioni PowerShell (x86) genererà un errore. Questo comando aggiunge solo i driver di periferica critici per l'avvio al database delle periferiche critiche. Non esegue la preparazione completa di sysprep.

```
Start-Process rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

6. Esegui la migrazione a un tipo di istanza Xen al termine del processo sysprep.

Assistente di ripiattaforma da Windows a Linux per database Microsoft SQL Server

Per informazioni sulla ripiattaforma dei database di Microsoft SQL Server da Windows a Linux, consulta l'assistente di ripiattaforma da Windows a Linux per i database di Microsoft SQL Server nella Guida per l'utente di Microsoft SQL Server on Amazon EC2.

Risolvi i problemi relativi a un aggiornamento su un'istanza di Windows

AWS fornisce supporto per l'aggiornamento in caso di problemi o problemi con l'Upgrade Helper Service, un' AWS utilità che consente di eseguire aggiornamenti sul posto utilizzando i driver Citrix PV.

In seguito all'aggiornamento, durante l'ottimizzazione di .NET Framework da parte del servizio di ottimizzazione di runtime .NET, sull'istanza potrebbe verificarsi un utilizzo della CPU temporaneamente superiore alla media. Questo è il comportamento previsto.

Se l'istanza non ha superato entrambi i controlli dello stato dopo diverse ore, consulta quanto segue.

- Se hai effettuato l'aggiornamento a Windows Server 2008 ed entrambi i controlli dello stato non riescono dopo diverse ore, l'aggiornamento potrebbe non essere riuscito con la visualizzazione dell'istruzione Click OK (Fare clic su OK) per confermare il rollback. Dal momento che la console non è accessibile in questa fase, non è possibile fare clic sul pulsante in alcun modo. Per risolvere questo problema, riavvia tramite l'API o la console Amazon EC2. Per l'inizializzazione del riavvio sono necessari almeno dieci minuti. L'istanza potrebbe diventare disponibile dopo 25 minuti.
- Rimuovi le applicazioni o i ruoli del server dal server e riprova.

Se l'istanza non supera entrambi i controlli dello stato dopo la rimozione delle applicazioni o dei ruoli del server dal server, procedi come segue.

- Arresta l'istanza e collega il volume root a un'altra istanza. Per ulteriori informazioni, consulta la descrizione di come arrestare e collegare il volume root a un'altra istanza in "In attesa del servizio di metadati".
- Analizza i file e di log e i log degli eventi di Installazione Windows per verificare la presenza di errori.

Per altri problemi relativi alla migrazione o all'aggiornamento di un sistema operativo, ti consigliamo di consultare gli articoli in Prima di avviare un aggiornamento in loco.

EC2 Fleet EC2 e serie di istanze spot

EC2 Fleet e Serie di istanze spot sono progettati per essere strumenti utili per avviare un parco istanze o un gruppo di istanze con AWS. Ogni istanza di un parco istanze si basa su un modello di lancio o su un set di parametri di lancio configurati manualmente al momento del lancio.

I parchi istanze offrono le seguenti funzionalità e vantaggi. Questi vantaggi consentono di massimizzare il risparmio sui costi e ottimizzare la disponibilità e le prestazioni durante l'esecuzione di applicazioni su più istanze EC2.

Più tipi di istanza e opzioni di acquisto

In una singola chiamata API, un parco istanze può avviare più tipi di istanza e opzioni di acquisto (istanze on demand e spot), consentendo di ottimizzare i costi tramite l'uso di istanze spot. È anche possibile usufruire di sconti sulle istanze riservate e sui Savings Plans utilizzandoli in combinazione con le istanze on demand del parco istanze.

Distribuzione di istanze tra le zone di disponibilità

Un parco istanze tenta automaticamente di distribuire le istanze in modo uniforme tra più zone di disponibilità per garantire una disponibilità elevata. In questo modo viene garantita la resilienza nel caso in cui una zona di disponibilità non sia più disponibile.

Sostituzione automatica delle istanze spot

Se il parco istanze include istanze spot, può richiedere automaticamente la sostituzione della capacità spot se le istanze spot vengono interrotte o compromesse per via di un cambiamento dell'integrità dell'istanza. Grazie al ribilanciamento della capacità, un parco istanze può anche monitorare e sostituire proattivamente le istanze spot sono a un elevato rischio di interruzione.

EC2 Fleet è una buona opzione se hai bisogno di flessibilità per la gestione degli aspetti del ciclo di vita delle istanze o dei meccanismi di scalabilità. È anche possibile utilizzare Serie di istanze spot, ma non consigliamo di farlo poiché è un'API legacy senza investimenti pianificati. Tuttavia, se Serie di istanze spot è già in uso, è possibile continuare a utilizzarlo. Serie di istanze spot ed EC2 Fleet offrono le stesse funzionalità di base.

> **Tip**
>
> Come best practice generale, consigliamo piuttosto di lanciare flotte di istanze Spot e On-Demand con Amazon EC2 Auto Scaling perché fornisce funzionalità aggiuntive che puoi

utilizzare per gestire la tua flotta. La lista di funzionalità aggiuntive include sostituzioni dei controlli dell'integrità sia per le istanze spot che per le istanze on demand, controlli dell'integrità basato sulle applicazioni e un'integrazione con Elastic Load Balancing per garantire una distribuzione uniforme del traffico delle applicazioni nelle istanze integre. Puoi utilizzare i gruppi Auto Scaling anche quando utilizzi AWS servizi come Amazon ECS, Amazon EKS (gruppi di nodi autogestiti) e Amazon VPC Lattice. Per ulteriori informazioni, consulta Guida per l'utente di Dimensionamento automatico Amazon EC2.

Argomenti

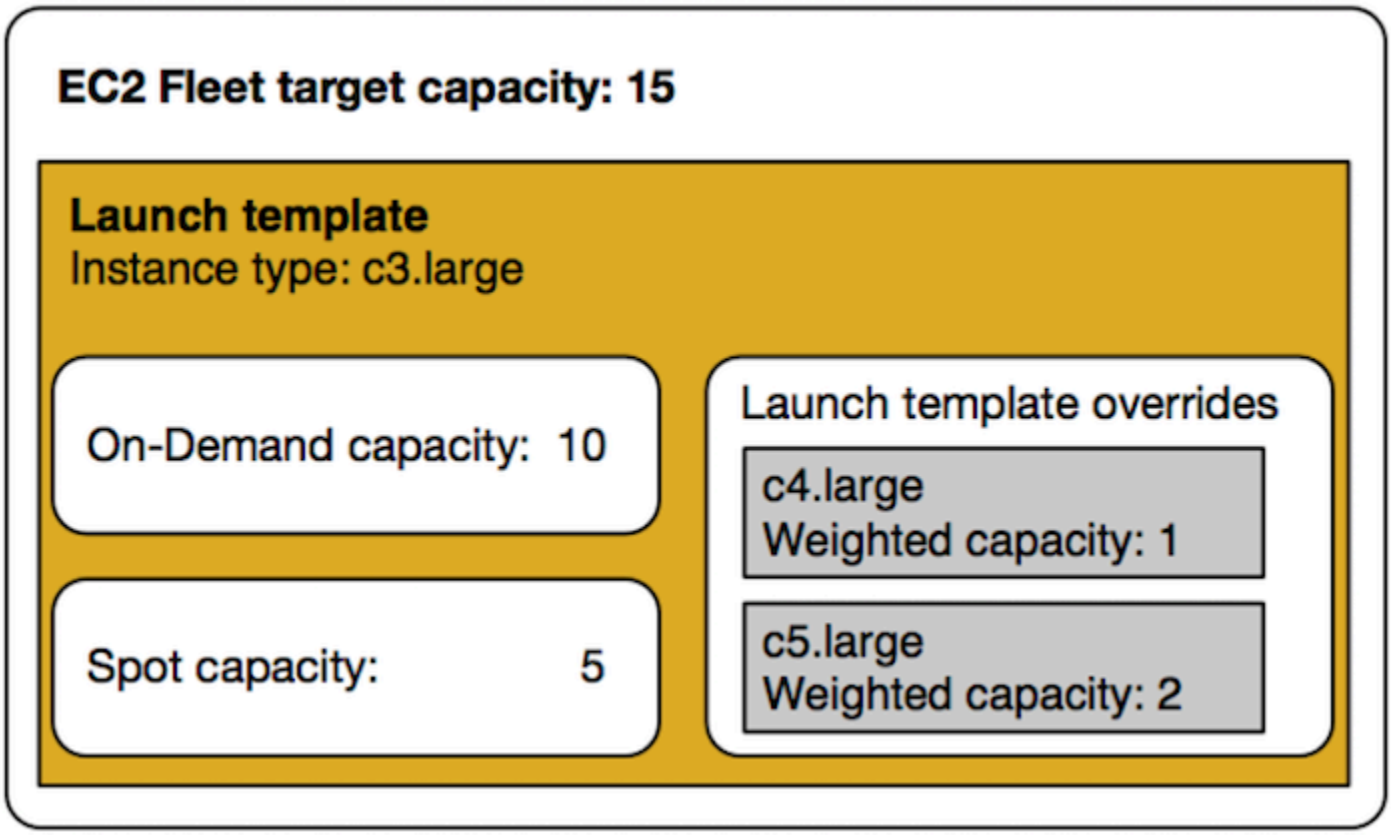
EC2 Fleet

Un parco istanze EC2 contiene le informazioni di configurazione per avviare un parco istanze. In una singola chiamata API, un parco istanze può avviare più tipi di istanze in più zone di disponibilità utilizzando insieme le opzioni di acquisto di istanza spot, istanza on demand, istanza riservata e Savings Plans. Con EC2 Fleet puoi:

- Definire target di capacità spot e on-demand diversi e l'importo massimo che sei disposto a pagare all'ora
- Specificare i tipi di istanza più adatti per le tue applicazioni
- Specificare in che modo Amazon EC2 deve distribuire la capacità del parco istanze all'interno di ogni opzione di acquisto

Puoi inoltre impostare un importo massimo all'ora che sei disposto a pagare per il parco istanze: EC2 Fleet avvierà le istanze finché non raggiunge tale importo. A questo punto, il parco istanze interrompe l'avvio delle istanze, anche se non è stata raggiunta la capacità target.

EC2 Fleet EC2 prova ad avviare il numero di istanze necessarie per soddisfare la capacità di destinazione specificata nella richiesta. Se hai specificato un prezzo totale massimo all'ora, soddisfa la capacità finché non raggiunge l'importo massimo che sei disposto a pagare. Il parco istanze può anche tentare di mantenere la propria capacità spot target se le Istanze spot vengono interrotte. Per ulteriori informazioni, consulta Come funzionano Istanze spot.



È possibile indicare un numero illimitato di tipi di istanza per parco istanze EC2. È possibile effettuare il provisioning di tali tipi di istanze utilizzando le opzioni di acquisto spot e on demand. Puoi anche specificare più zone di disponibilità, specificare prezzi Spot massimi diversi per ogni istanza e scegliere opzioni Spot aggiuntive per ogni parco istanze. Amazon EC2 utilizza le opzioni specificate per effettuare il provisioning della capacità all'avvio del parco istanze.

Mentre il parco istanze è in esecuzione, se Amazon EC2 recupera un'istanza spot a causa di un aumento del prezzo o del fallimento di un'istanza, il parco istanze EC2 può provare a sostituire le istanze con uno qualsiasi dei tipi di istanze specificati. In questo modo è più semplice riguadagnare la capacità durante un picco dei prezzi Spot. È possibile sviluppare una strategia delle risorse elastica e flessibile per ogni parco istanze. Per esempio, all'interno di parchi istanze specifici, è possibile integrare la propria capacità primaria on demand con una capacità spot meno costosa, se disponibile.

Se disponi di istanze riservate e specifichi istanze on demand nel tuo parco istanze, EC2 Fleet utilizzerà le istanze riservate. Ad esempio, se il proprio parco istanze indica una Istanza on demand come `c4.large` e si dispone di Istanze riservate per `c4.large`, si ricevono i prezzi della Istanza riservata. Lo stesso vale se si utilizza un Savings Plan.

L'utilizzo di EC2 Fleet non comporta costi supplementari. Si pagano solo le istanze EC2 che il parco istanze avvia al posto dell'utente.

Indice

Limitazioni di EC2 Fleet

Le limitazioni seguenti riguardano EC2 Fleet:

- EC2 Fleet è disponibile solo tramite l'API Amazon EC2, la AWS CLI, gli SDK AWS e AWS CloudFormation.
- Una richiesta EC2 Fleet non può AWS estendersi su più regioni. È necessario creare un EC2 Fleet separato per ciascuna regione.
- Una richiesta di EC2 Fleet non può comprendere sottoreti diverse della stessa zona di disponibilità.

Istanze a prestazioni espandibili

Se avvii le tue istanze spot utilizzando un tipo di istanza a prestazioni espandibili, e prevedi di utilizzare immediatamente le istanze spot a prestazioni espandibili per un breve periodo, senza alcun tempo di inattività per accumulare crediti CPU, suggeriamo di avviarla in Modalità Standard in modo da evitare costi più elevati. Se avvii le istanze spot a prestazioni espandibili in Modalità Illimitata ed espandi la capacità di CPU immediatamente, l'espansione implicherà il dispendio dei crediti in più. Se l'istanza viene utilizzata per un periodo di tempo limitato, non riesce ad accumulare crediti CPU per ripagare i crediti extra, che i vengono quindi addebitati al termine dell'istanza.

La modalità illimitata è adatta per la Istanze spot con prestazioni burstable solo se l'istanza viene eseguita per un periodo di tempo sufficiente ad accumulare i crediti CPU per l'espansione. In caso contrario, il pagamento di crediti in eccedenza rende le prestazioni Istanze spot espandibili più costose rispetto all'utilizzo di altre istanze. Per ulteriori informazioni, consulta Quando utilizzare la modalità illimitata rispetto alla CPU fissa.

I crediti di avvio hanno lo scopo di fornire un'esperienza di avvio iniziale produttiva per le istanze T2, fornendo risorse di calcolo sufficienti per configurare l'istanza. Non sono consentiti avvii ripetuti di istanze T2 per accedere a nuovi crediti di avvio. Se occorre una CPU duratura, è possibile guadagnare crediti (rimanendo inattivi per un certo periodo) utilizzando la Unlimited mode (Modalità Illimitata) per istanze spot T2 o un tipo di istanza con una CPU dedicata.

Tipi di richiesta di EC2 Fleet

Esistono tre tipi di richieste di EC2 Fleet:

`instant`

Se configuri il tipo di richiesta come `instant`, EC2 Fleet inserisce una richiesta una tantum sincrona per la capacità desiderata. Nella risposta API, restituisce le istanze avviate, assieme agli errori per le istanze che non è stato possibile avviare. Per ulteriori informazioni, consulta Utilizzo di un EC2 Fleet di tipo "istantaneo".

`request`

Se configuri il tipo di richiesta come `request`, EC2 Fleet inserisce una richiesta asincrona una tantum per la capacità desiderata. Successivamente, se la capacità è diminuita a causa delle interruzioni di Spot, il parco istanze non tenta di rifornire Istanze spot e non invia nemmeno richieste in pool di capacità spot alternativi se la capacità non è disponibile.

`maintain`

(Predefinito) Se configuri il tipo di richiesta come `maintain`, EC2 Fleet effettua una richiesta asincrona per la capacità desiderata e mantiene la capacità rifornendo automaticamente le Istanze spot interrotte.

Tutti e tre i tipi di richiesta traggono vantaggio da una strategia di allocazione. Per ulteriori informazioni, consulta Strategie di allocazione per istanze spot.

Utilizzo di un EC2 Fleet di tipo "istantaneo"

L'EC2 Fleet di tipo istantaneo è una richiesta una tantum sincrona che effettua un solo tentativo di avviare la capacità desiderata. La risposta dell'API restituisce le istanze avviate, insieme agli errori per quelle istanze che non è stato possibile avviare. L'utilizzo di un EC2 Fleet di tipo istantaneo comporta diversi vantaggi, descritti in questo articolo. Le configurazioni di esempio sono fornite alla fine dell'articolo.

Per i carichi di lavoro che richiedono un'API di solo avvio per avviare le istanze EC2, puoi utilizzare l'API. RunInstances Tuttavia, con RunInstances, puoi avviare solo istanze On-Demand o Istanze Spot, ma non entrambe nella stessa richiesta. Inoltre, quando si utilizzano istanze Spot RunInstances per avviare istanze Spot, la richiesta di istanza Spot è limitata a un tipo di istanza e a una zona di disponibilità. L'istanza ha come obiettivo un pool di capacità spot (un insieme di istanze inutilizzate con lo stesso tipo di istanza e zona di disponibilità). Se il pool di capacità Spot non dispone di una capacità di istanze Spot sufficiente per la richiesta, la RunInstances chiamata ha esito negativo.

Invece di RunInstances utilizzarla per avviare le istanze Spot, ti consigliamo di utilizzare l' CreateFleet API con il `type` parametro impostato su `instant` per ottenere i seguenti vantaggi:

- Avvia le istanze on demand e le istanze spot in una richiesta. Un EC2 Fleet può avviare istanze on demand, istanze spot o entrambe. La richiesta di Istanze spot viene soddisfatta se c'è capacità disponibile e il prezzo massimo all'ora specificato nella richiesta supera il prezzo Spot.
- Aumenta la disponibilità di istanze spot. Utilizzando un EC2 Fleet di tipo `instant`, puoi avviare istanze spot seguendo Best practice di istanze spot con i seguenti vantaggi:
  - Best practice di istanze spot: essere flessibili riguardo tipi di istanza e zone di disponibilità.

    Vantaggio: specificando diversi tipi di istanza e zone di disponibilità, aumenti il numero di pool di capacità spot. Ciò offre al servizio Spot maggiori possibilità di trovare e allocare la capacità di calcolo Spot desiderata. Una buona regola è quella di essere flessibili su almeno 10 tipi di istanza per ogni carico di lavoro e assicurarsi che tutte le zone di disponibilità siano configurate per l'utilizzo nel VPC.
  - Best practice di Spot: utilizza la strategia di price-capacity-optimized allocazione.

    Vantaggio: la strategia di `price-capacity-optimized` allocazione identifica le istanze dai pool di capacità Spot più disponibili e quindi effettua automaticamente il provisioning delle istanze dai prezzi più bassi di questi pool. Poiché la capacità dell'istanza spot viene restituita da pool con capacità ottimale, ciò riduce la possibilità che le istanze spot vengano interrotte quando Amazon EC2 recupera la capacità.

- Accedi a un set più ampio di funzionalità. Per i carichi di lavoro che richiedono un'API solo per il lancio e in cui preferisci gestire il ciclo di vita dell'istanza piuttosto che lasciare che EC2 Fleet lo gestisca per te, utilizza il tipo EC2 Fleet anziché l'API. `instant` RunInstances EC2 Fleet offre un set di funzionalità più ampio rispetto RunInstances a, come dimostrato negli esempi seguenti. Per tutti gli altri carichi di lavoro, è consigliabile utilizzare Dimensionamento automatico Amazon EC2 perché fornisce un set di funzionalità più completo per un'ampia gamma di carichi di lavoro, ad esempio applicazioni supportate da ELB, carichi di lavoro containerizzati e processi di elaborazione delle code.

È possibile utilizzare EC2 Fleet di tipo instantaneo per avviare istanze in Blocchi di capacità. Per ulteriori informazioni, consulta Tutorial: avvio delle istanze in Blocchi di capacità.

AWS servizi come Amazon EC2 Auto Scaling e Amazon EMR utilizzano EC2 Fleet of type Instant per avviare istanze EC2.

Prerequisiti per un EC2 Fleet di tipo istantaneo

Per i prerequisiti per la creazione di un EC2 Fleet, consulta Prerequisiti di parco istanze EC2.

Come funziona un EC2 Fleet istantaneo

Quando si utilizza un EC2 Fleet di tipo `instant`, la sequenza degli eventi è la seguente:

1. Configura il tipo di richiesta come. CreateFleet`instant` Per ulteriori informazioni, consulta Creazione di un parco istanze EC2. Dopo aver effettuato la chiamata API, non puoi più modificarla.
2. Quando effettui la chiamata API, il parco istanze EC2 inserisce una richiesta una tantum sincrona per la capacità desiderata.
3. La risposta dell'API restituisce le istanze avviate, insieme agli errori per quelle istanze che non è stato possibile avviare.
4. Puoi descrivere il tuo parco istanze EC2, elencare le istanze associate al tuo parco istanze EC2 e visualizzare la cronologia del tuo parco istanze EC2.
5. Dopo il lancio delle istanze, puoi eliminare la richiesta del parco istanze. Quando elimini la richiesta del parco istanze, puoi scegliere di terminare le istanze associate o di lasciarle in esecuzione.
6. È possibile terminare le istanze in qualsiasi momento.

Esempi

Gli esempi seguenti mostrano come utilizzare EC2 Fleet di tipo `instant` per diversi casi d'uso. Per ulteriori informazioni sull'utilizzo dei parametri dell' CreateFleet API EC2, consulta CreateFleetAmazon EC2 API Reference.

Esempi

Esempio 1: Avvio di istanze spot con la strategia di allocazione ottimizzata per la capacità

L'esempio seguente indica i parametri necessari in un parco istanze EC2 di tipo `instant`: un modello di avvio, una capacità target, un'opzione di acquisto predefinita e sostituzioni del modello di avvio.

- Il modello di avvio viene identificato dal nome e dal numero di versione.
- Le 12 sostituzioni del modello di avvio specificano 4 tipi di istanza e 3 sottoreti differenti, ognuna in una zona di disponibilità separata. Ogni combinazione di tipo di istanza e sottorete definisce un pool di capacità spot, restituendo 12 pool di capacità spot.
- La capacità obiettivo per il parco istanze è 20 istanze.

- L'opzione di acquisto predefinita è `spot`; con questa opzione, il parco istanze tenta di avviare 20 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 2: Avvio di una singola istanza spot con la strategia di allocazione ottimizzata per la capacità

Puoi avviare in modo ottimale un'istanza Spot alla volta effettuando più chiamate di tipo EC2 Fleet API`instant`, impostando il valore su 1. TotalTargetCapacity

L'esempio seguente indica i parametri necessari in un parco istanze EC2 di tipo istantaneo: un modello di avvio, una capacità target, un'opzione di acquisto predefinita e sostituzioni del modello di avvio. Il modello di avvio viene identificato dal nome e dal numero di versione. Le 12 sostituzioni del modello di avvio hanno 4 tipi di istanza e 3 sottoreti differenti, ognuna in una zona di disponibilità separata. La capacità obiettivo per il parco istanze è 1 istanza e l'opzione di acquisto predefinita è Spot, il che comporta il tentativo di avviare un'istanza spot da uno dei 12 pool di capacità spot

basati sulla strategia di allocazione ottimizzata per la capacità, per avviare un'istanza spot dal pool di capacità più disponibile.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
```

```
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 3: Avvio di istanze spot utilizzando la ponderazione di istanza

Gli esempi seguenti utilizzano la ponderazione d'istanza; questo significa che il prezzo è calcolato a ora per unità anziché a ora per istanza. Ogni configurazione di avvio presenta un tipo di istanza diverso e un peso diverso in base al numero di unità del carico di lavoro che può essere eseguito sull'istanza, supponendo che un'unità del carico di lavoro richieda 15 GB di memoria e 4 vCPU. Ad esempio, m5.xlarge (4 vCPU e 16 GB di memoria) può eseguire una sola unità e il suo peso è 1, m5.2xlarge (8 vCPU e 32 GB di memoria) può eseguire 2 unità e il suo peso è 2 e così via. La capacità obiettivo totale è impostata su 40 unità. L'opzione di acquisto predefinita è spot e la strategia di allocazione è ottimizzata per la capacità, il che si traduce in 40 m5.xlarge (40 diviso per 1), 20 m5.2xlarge (40 diviso per 2), 10 m5.4xlarge (40 diviso per 4), 5 m5.8xlarge (40 diviso per 8) o un mix dei tipi di istanza con pesi che si sommano alla capacità desiderata sulla base della strategia di allocazione ottimizzata per la capacità.

Per ulteriori informazioni, consulta Ponderazione istanza parco istanze EC2.

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":2
            },
            {
```

```
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":8
            }
         ]
      }
   ],
   "TargetCapacitySpecification":{
      "TotalTargetCapacity":40,
      "DefaultTargetCapacityType":"spot"
   },
   "Type":"instant"
}
```

Esempio 4: Avvio di istanze spot in una singola zona di disponibilità

Puoi configurare un parco istanze per avviare tutte le istanze in un'unica zona di disponibilità impostando le opzioni SingleAvailabilityZone Spot su true.

Le 12 sostituzioni del modello di avvio hanno tipi di istanza e sottoreti differenti, ognuna in una zona di disponibilità separata ma con la stessa capacità ponderata. La capacità obiettivo totale è di 20 istanze, l'opzione d'acquisto predefinita è spot e la strategia di allocazione spot è ottimizzata per la capacità. Il parco istanze EC2 avvia 20 istanze spot, tutte in una singola zona di disponibilità, dai pool di capacità spot con capacità ottimale, utilizzando le specifiche di avvio.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
```

```
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-49e41922"
            }
        ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 5: Avvio di istanze spot di un singolo tipo in una singola zona di disponibilità

Puoi configurare un parco istanze per avviare tutte le istanze dello stesso tipo e in un'unica zona di disponibilità impostando SpotOptions SingleInstanceType true e SingleAvailabilityZone true.

Le 12 sostituzioni del modello di avvio hanno tipi di istanza e sottoreti differenti, ognuna in una zona di disponibilità separata ma con la stessa capacità ponderata. La capacità obiettivo totale è di 20 istanze, l'opzione d'acquisto predefinita è spot, la strategia di allocazione spot è ottimizzata per la capacità. Il parco istanze EC2 avvia 20 istanze spot dello stesso tipo, tutte in una singola zona di disponibilità, dal pool di istanze spot con capacità ottimale, utilizzando le specifiche di avvio.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
```

```
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 6: Avvio di istanze spot solo se è possibile avviare una capacità target minima

Puoi configurare un parco istanze per avviare le istanze solo se è possibile avviare la capacità target minima impostando le opzioni Spot sulla MinTargetCapacity capacità target minima che desideri avviare insieme.

Le 12 sostituzioni del modello di avvio hanno tipi di istanza e sottoreti differenti, ognuna in una zona di disponibilità separata ma con la stessa capacità ponderata. La capacità obiettivo totale e la capacità obiettivo minima sono entrambe impostate su 20 istanze, l'opzione di acquisto predefinita è spot e la strategia di allocazione spot è ottimizzata per la capacità. Il parco istanze EC2 avvia 20 istanze spot dal pool di capacità spot con capacità ottimale utilizzando le sostituzioni del modello di avvio, solo se è in grado di avviare tutte e 20 le istanze contemporaneamente.

```
{
```

```
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
```

```
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 7: Avvio di istanze spot solo se è possibile avviare una capacità target minima dello stesso tipo di istanza in una singola zona di disponibilità

Puoi configurare un parco istanze per lanciare istanze solo se la capacità target minima può essere avviata con un singolo tipo di istanza in un'unica zona di disponibilità impostando le opzioni MinTargetCapacity Spot sulla capacità target minima che desideri avviare insieme alle opzioni SingleInstanceType e e SingleAvailabilityZone alle opzioni.

Le 12 specifiche di avvio che sostituiscono il modello di avvio hanno tipi di istanza e subnet differenti, ognuna in una zona di disponibilità separata ma con la stessa capacità ponderata. La capacità target totale e la capacità target minima sono entrambe impostate su 20 istanze, l'opzione di acquisto predefinita è spot, la strategia di allocazione Spot è ottimizzata in termini di capacità, questo è vero ed è vero. SingleInstanceType SingleAvailabilityZone Il parco istanze EC2 avvia 20 istanze spot dello stesso tipo, tutte in una singola zona di disponibilità, dal pool di istanze spot con capacità ottimale, utilizzando le specifiche di avvio, solo se è possibile avviare tutte e 20 le istanze contemporaneamente.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
```

```
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 8: Avvio di istanze con più modelli di avvio

Puoi configurare un parco istanze per avviare istanze con specifiche di avvio diverse per tipi di istanza o gruppi di tipi di istanza diversi, specificando più modelli di avvio. In questo esempio vogliamo avere dimensioni del volume EBS diverse per diversi tipi di istanza e abbiamo ciò che è configurato nei modelli di avvio ec2-fleet-lt-4xl, ec2-fleet-lt-9xl e ec2-fleet-lt-18xl.

In questo esempio, stiamo utilizzando 3 diversi modelli di avvio per i 3 tipi di istanza, in base alle loro dimensioni. Le sostituzioni delle specifiche di avvio su tutti i modelli di avvio utilizzano i pesi delle istanze in base alle vCPU del tipo di istanza. La capacità obiettivo totale è di 144 unità, l'opzione d'acquisto predefinita è spot e la strategia di allocazione spot è ottimizzata per la capacità. Il parco istanze EC2 può avviare 9 c5n.4xlarge (144 diviso per 16) utilizzando il modello di avvio ec2-fleet-4xl o 4 c5n.9xlarge (144 diviso per 36) utilizzando il modello di avvio ec2-fleet-9xl o 2 c5n.18xlarge (144

diviso per 72) utilizzando il modello di avvio ec2-fleet-18xl o un mix dei tipi di istanza con pesi si sommano alla capacità desiderata, in base alla strategia di allocazione ottimizzata per la capacità.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":72
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-9xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":36
            },
            {
```

```
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":36
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-4xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":16
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 144,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 9: Avvio di istanze spot con una base di istanze on demand

L'esempio seguente specifica la capacità target totale di 20 istanze per il parco istanze e una capacità target di 5 istanze on demand. L'opzione di acquisto predefinita è spot. Il parco istanze avvia 5 istanze on demand come indicato, ma deve avviare altre 15 istanze per soddisfare la capacità target totale. L'opzione di acquisto per la differenza è calcolata come TotalTargetCapacity — OnDemandTargetCapacity = DefaultTargetCapacityType, il che fa sì che la flotta lanci 15 istanze Spot costituiscano uno dei 12 pool di capacità Spot in base alla strategia di allocazione ottimizzata per la capacità.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
```

```
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 10: Avvio di istanze spot utilizzando una strategia di allocazione ottimizzata per la capacità con una base di istanze on demand che utilizza prenotazioni di capacità e la strategia di allocazione con priorità

È possibile configurare una flotta in modo che utilizzi innanzitutto le prenotazioni di capacità on demand al momento del lancio di una base di istanze on demand con il tipo di capacità target

predefinito come spot impostando la strategia di utilizzo per Capacity Reservations su. use-capacity-reservations-first E se più pool di istanze presentano prenotazioni di capacità inutilizzate, viene applicata la strategia di allocazione on demand scelta. In questo esempio, la strategia di allocazione on demand ha la priorità.

In questo esempio, ci sono 6 prenotazioni della capacità disponibili non utilizzate. Questa capacità è inferiore alla capacità target on demand del parco istanze di 10 istanze on demand.

L'account presenta le seguenti 6 prenotazioni della capacità inutilizzate in 2 pool. Il numero di prenotazioni di capacità in ogni pool è indicato da. AvailableInstanceCount

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

La seguente configurazione del parco istanze mostra solo le configurazioni pertinenti per questo esempio. La strategia di allocazione On-Demand ha la priorità, mentre la strategia di utilizzo per Capacity Reservations è. use-capacity-reservations-first La strategia di allocazione spot è ottimizzata per la capacità. La capacità obiettivo totale è 20, la capacità obiettivo on demand è 10 e il tipo di capacità obiettivo predefinito è spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
```

```
        "CapacityReservationOptions": {
          "UsageStrategy": "use-capacity-reservations-first"
        },
        "AllocationStrategy":"prioritized"
    },
    "LaunchTemplateConfigs": [
      {
        "LaunchTemplateSpecification":{
           "LaunchTemplateName":"ec2-fleet-lt1",
           "Version":"$Latest"
        },
        "Overrides":[
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-fae8c380",
              "Priority": 1.0
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-e7188bab",
              "Priority": 2.0
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-49e41922",
              "Priority": 3.0
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-fae8c380",
              "Priority": 4.0
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-e7188bab",
              "Priority": 5.0
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-49e41922",
              "Priority": 6.0
           },
           {
              "InstanceType":"m5.large",
```

```
               "SubnetId":"subnet-fae8c380",
               "Priority": 7.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 8.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 9.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 10.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 11.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 12.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 10,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Dopo aver creato il parco istanze istantaneo utilizzando la configurazione precedente, le seguenti 20 istanze vengono avviate per soddisfare la capacità target:

- 7 istanze on demand c5.large in us-east-1a: le istanze c5.large in us-east-1a hanno la massima priorità e sono disponibili 3 prenotazioni della capacità c5.large inutilizzate. Le prenotazioni della capacità vengono utilizzate innanzitutto per avviare 3 istanze on demand più 4 ulteriori istanza on demand che vengono avviate secondo la strategia di allocazione on demand, che in questo esempio ha la priorità.
- 3 istanze on demand m5.large in us-east-1a: m5.large in us-east-1a ha la seconda priorità e ci sono 3 prenotazioni di capacità c3.large inutilizzate disponibili.
- 10 istanze spot da uno dei 12 pool di capacità spot con capacità ottimale in base alla strategia di allocazione ottimizzata per la capacità.

Dopo il lancio della flotta, puoi correre describe-capacity-reservationsper vedere quante prenotazioni di capacità non utilizzate sono rimaste. In questo esempio, dovresti vedere la seguente risposta, che mostra che sono state utilizzate tutte le prenotazioni della capacità c5.large e m5.large.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
}
```

Esempio 11: avvia le istanze Spot utilizzando capacity-optimized-prioritized la strategia di allocazione

L'esempio seguente indica i parametri necessari in un parco istanze EC2 di tipo istantaneo: un modello di avvio, una capacità target, un'opzione di acquisto predefinita e sostituzioni del modello di avvio. Il modello di avvio viene identificato dal nome e dal numero di versione. Le 12 specifiche di avvio che sostituiscono il modello di avvio hanno 4 tipi di istanza diversi con una priorità assegnata e 3 sottoreti diverse, ognuna in una zona di disponibilità separata. La capacità target per il parco istanze è di 20 istanze e l'opzione di acquisto predefinita è spot, in base alla quale il parco istanze tenta di lanciare 20 istanze Spot da uno dei 12 pool di capacità Spot in base alla strategia di capacity-optimized-prioritized allocazione, che implementa le priorità con il massimo impegno, ma ottimizza innanzitutto la capacità.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 2.0
            },
            {
               "InstanceType":"m5.large",
```

```
                "SubnetId":"subnet-fae8c380",
                "Priority": 3.0
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab",
                "Priority": 3.0
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 3.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380",
                "Priority": 4.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab",
                "Priority": 4.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 4.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Strategie di configurazione di EC2 Fleet

Un parco istanze EC2 è un gruppo di istanze on demand e di istanze spot. Il parco istanze EC2 può anche essere un gruppo di istanze di Blocchi di capacità.

Istanze on demand e istanze spot

EC2 Fleet tenta di avviare il numero di istanze necessarie per soddisfare la capacità di destinazione specificata nella richiesta. Il parco istanze può comprendere solo Istanze on demand, solo Istanze spot oppure una combinazione di Istanze on demand e Istanze spot. La richiesta di Istanze spot viene soddisfatta se c'è capacità disponibile e il prezzo massimo all'ora specificato nella richiesta supera il prezzo Spot. Il parco istanze tenta inoltre di mantenere la propria capacità target se le Istanze spot vengono interrotte.

Puoi inoltre impostare un importo massimo all'ora che sei disposto a pagare per il parco istanze: Parco istanze EC2 avvierà le istanze finché non raggiunge tale importo. A questo punto, il parco istanze interrompe l'avvio delle istanze, anche se non è stata raggiunta la capacità target.

Un pool di capacità spot è un insieme di istanze EC2 inutilizzate con lo stesso tipo di istanza e zona di disponibilità. Quando si crea un EC2 Fleet, è possibile includere più specifiche di avvio, che variano a seconda del tipo di istanza, della zona di disponibilità, della sottorete e del prezzo massimo. Il parco istanze seleziona i pool di capacità spot che vengono utilizzati per soddisfare la richiesta, sulla base delle specifiche di avvio incluse nella richiesta, e la configurazione della richiesta. Le Istanze spot provengono dai pool selezionati.

Un EC2 Fleet consente di assegnare grandi quantità di capacità EC2 che sono utili per l'applicazione in base al numero di core o istanze o alla quantità di memoria. Ad esempio, è possibile indicare a un parco istanze EC2 di avviare una capacità obiettivo di 200 istanze, delle quali 130 sono istanze on demand e il resto sono istanze spot.

Istanze di Blocchi di capacità

I blocchi di capacità per ML ti consentono di prenotare istanze GPU in date future per supportare carichi di lavoro di machine learning (ML) di breve durata. Le istanze eseguite in un Capacity Block vengono automaticamente collocate vicine all'interno di Amazon UltraClusters EC2. Per ulteriori informazioni sui blocchi di capacità, consulta la pagina Blocchi di capacità per ML.

Utilizzare le strategie di configurazione adeguate per creare un parco istanze EC2 che soddisfi le proprie esigenze.

Indice

- Configurazione di EC2 Fleet per il backup on demand
- Ribilanciamento della capacità
- Sostituzioni prezzo massimo
- Controllo delle spese
- Ponderazione istanza parco istanze EC2

Pianificazione di un parco istanze EC2

Nella pianificazione del proprio EC2 Fleet, consigliamo di procedere come segue:

- Stabilisci se creare un EC2 Fleet che invii una richiesta una tantum sincrona o asincrona per la capacità di destinazione desiderata o uno che mantenga una capacità di destinazione nel tempo. Per ulteriori informazioni, consulta Tipi di richiesta di EC2 Fleet.
- Indicare il tipo di istanza che soddisfa i propri requisiti in termini di applicazioni.
- Se si intende includere le istanze spot nel proprio parco istanze EC2, prima di creare il parco istanze consulta Best practice Spot. Quando si programma il proprio parco istanze, utilizzare queste best practice in modo da allestire le istanze al prezzo più basso possibile.
- Stabilire la capacità di destinazione per EC2 Fleet. È possibile impostare una capacità di destinazione in istanze o in unità personalizzate. Per ulteriori informazioni, consulta Ponderazione istanza parco istanze EC2.
- Stabilire quale porzione della capacità di destinazione di EC2 Fleet deve essere capacità on-demand e capacità spot. È possibile indicare 0 come capacità on demand o capacità spot o entrambe.
- Se si utilizza la ponderazione d'istanza, stabilire il prezzo per unità. Per calcolare il prezzo per unità, dividere il prezzo all'ora per istanza per il numero di unità (o peso) che tale istanza rappresenta. Se non si utilizza la ponderazione d'istanza, il prezzo predefinito per unità è il prezzo all'ora per istanza.
- Imposta l'importo massimo all'ora che sei disposto a pagare per il parco istanze. Per ulteriori informazioni, consulta Controllo delle spese.
- Rivedere le possibili opzioni per il proprio EC2 Fleet. Per informazioni sui parametri del parco istanze, consulta create-fleet nella Guida di riferimento ai comandi AWS CLI . Per gli esempi di configurazione di un EC2 Fleet, consulta Configurazioni parco istanze EC2 di esempio.

Strategie di allocazione per istanze spot

La configurazione di avvio determina tutti i possibili pool di capacità spot (tipi di istanze e zone di disponibilità) da cui EC2 Fleet può avviare istanze spot. Tuttavia, al momento del lancio delle istanze, EC2 Fleet utilizza la strategia di allocazione specificata per scegliere i pool specifici da tutti i pool possibili.

> **Note**
>
> (Solo istanze Linux) Se configuri l'istanza Spot per l'avvio con AMD SEV-SNP attivato, ti verrà addebitata una tariffa di utilizzo oraria aggiuntiva equivalente al 10% della tariffa oraria on demand per il tipo di istanza selezionato. Se la strategia di allocazione utilizza il prezzo come input, il parco istanze EC2 non include questa tariffa aggiuntiva; viene utilizzato solo il prezzo spot.

Strategie di allocazione

Puoi specificare una delle seguenti strategie di allocazione per le istanze spot:

`price-capacity-optimized`(consigliato)

Il parco istanze EC2 identifica i pool con la massima capacità disponibile per il numero di istanze che si stanno avviando. Ciò implica che richiederemo istanze spot dai pool che riteniamo avere le minori possibilità di interruzione nel breve termine. Dopodiché, il parco istanze EC2 richiede istanze spot dal pool con il prezzo più basso tra questi pool.

La strategia di allocazione `price-capacity-optimized` è la scelta migliore per la maggior parte dei carichi di lavoro spot, come applicazioni containerizzate stateless, microservizi, applicazioni Web, processi di dati e analisi ed elaborazione in batch.

`capacity-optimized`

Il parco istanze EC2 identifica i pool con la massima capacità disponibile per il numero di istanze che si stanno avviando. Ciò implica che richiederemo istanze spot dai pool che riteniamo avere le minori possibilità di interruzione nel breve termine. Facoltativamente, puoi impostare una priorità per ogni tipo di istanza del parco istanze utilizzando `capacity-optimized-prioritized`. EC2 Fleet ottimizzerà innanzitutto la capacità, ma rispetterà le priorità del tipo di istanza sulla base del miglior tentativo.

Con Istanze spot, i prezzi cambiano lentamente nel tempo in base ai trend a lungo termine dell'offerta e della domanda, ma la capacità fluttua in tempo reale. La strategia `capacity-optimized` avvia automaticamente Istanze spot nei pool più disponibili esaminando i dati di capacità in tempo reale e prevedendo quali sono le più disponibili. Questa strategia è ideale per carichi di lavoro che possono avere un costo più elevato di interruzione associato al riavvio del lavoro, ad esempio carichi di lavoro di integrazione continua (CI), rendering di immagini e media, deep learning e calcolo ad alte prestazioni (HPC), che possono avere un costo più elevato di interruzione associato al riavvio del lavoro. Offrendo la possibilità di ridurre il numero di interruzioni, la strategia `capacity-optimized` può ridurre il costo complessivo del carico di lavoro.

In alternativa, puoi utilizzare la strategia di allocazione di `capacity-optimized-prioritized` con un parametro di priorità e quindi impostare l'ordine dei tipi di istanza dalla priorità più alta alla più bassa. Puoi impostare la stessa priorità per diversi tipi di istanza. EC2 Fleet ottimizzerà innanzitutto la capacità, ma rispetterà le priorità del tipo di istanza sulla base del miglior tentativo (ad esempio, se il rispetto delle priorità non influirà in modo significativo sulla capacità di EC2 Fleet di fornire capacità ottimale). Questa è una buona opzione per i carichi di lavoro in cui è necessario ridurre al minimo la possibilità di interruzioni e la preferenza per determinati tipi di istanza è importante. Tieni presente che quando imposti la priorità per `capacity-optimized-prioritized`, la stessa priorità viene applicata anche alle istanze on demand se la `AllocationStrategy` on demand è impostata su `prioritized`.

`diversified`

I Istanze spot sono distribuiti in tutti i pool di capacità spot.

`lowest-price`(non consigliato)

> **Warning**
>
> Non consigliamo la strategia di `lowest-price` allocazione perché presenta il rischio di interruzione più elevato per le istanze Spot.

Le istanze spot provengono dal pool con il prezzo più basso che ha capacità disponibile. Questa è la strategia predefinita. Tuttavia, consigliamo di sostituire il valore predefinito specificando la strategia di allocazione `price-capacity-optimized`.

Se il pool con il prezzo più basso non ha capacità disponibile, le istanze spot provengono dal successivo pool con il prezzo più basso che ha capacità disponibile.

Se un pool esaurisce la capacità prima di soddisfare la capacità desiderata, il parco istanze EC2 continuerà a soddisfare la richiesta attingendo dal successivo pool con il prezzo più basso. Per accertarti che la capacità desiderata sia soddisfatta, potresti ricevere istanze spot da vari pool.

Poiché questa strategia considera solo il prezzo dell'istanza e non la capacità disponibile, potrebbe comportare tassi di interruzione elevati.

`InstancePoolsToUseCount`

Il numero di pool Spot in cui allocare la capacità Spot di destinazione. Valido solo quando la strategia di allocazione è impostata su `lowest-price`. Il parco istanze EC2 seleziona i pool spot con il prezzo più basso e alloca in modo uniforme la capacità spot obiettivo tra i pool spot specificati.

Tieni presente che EC2 Fleet prova a prelevare istanze spot dal numero di pool specificati sulla base del massimo sforzo. Se un pool esaurisce la capacità spot prima di soddisfare la capacità obiettivo, il parco istanze EC2 continuerà a soddisfare la tua richiesta attingendo al pool con il prezzo più basso successivo. Per garantire che la capacità di destinazione sia soddisfatta, è possibile ricevere istanze spot da un numero di pool maggiore di quello specificato. Analogamente, se la maggior parte dei pool non dispone di capacità spot, è possibile ricevere la capacità di destinazione completa da un numero di pool inferiore a quello specificato.

Scelta della strategia di allocazione adeguata

Puoi ottimizzare il tuo parco istanze in base al tuo caso d'uso scegliendo la strategia di allocazione spot appropriata. Per la capacità obiettivo di istanza on demand, il parco istanze EC2 seleziona sempre il tipo di istanza più economico in base al prezzo pubblico on demand, continuando comunque a seguire la strategia di allocazione (`price-capacity-optimized`, `capacity-optimized`, `diversified` o `lowest-price`) per le istanze spot.

Equilibrio tra prezzo più basso e capacità disponibile

Per bilanciare i compromessi tra i pool di capacità spot con il prezzo più basso e i pool di capacità spot con la massima capacità disponibile, ti consigliamo di utilizzare la strategia di allocazione `price-capacity-optimized`. Questa strategia decide a quali pool richiedere le istanze spot tenendo conto sia del prezzo dei pool sia della capacità di istanze spot disponibile in tali pool. Ciò implica che richiederemo istanze spot dai pool che riteniamo avere le minori possibilità di interruzione nel breve termine, tenendo comunque conto del prezzo.

Se il tuo parco istanze esegue carichi di lavoro resilienti e stateless, tra cui applicazioni containerizzate, microservizi, applicazioni Web, processi di dati e analisi ed elaborazione in batch, utilizza la strategia di allocazione `price-capacity-optimized` per risparmiare sui costi e disporre di una capacità ottimale.

Se il parco istanze esegue carichi di lavoro che possono avere un costo più elevato di interruzione associato al riavvio del lavoro, ti consigliamo implementare i checkpoint affinché le applicazioni possano riavviarsi da quel punto in caso di interruzione. Utilizzando i checkpoint, la strategia di allocazione `price-capacity-optimized` è una buona scelta per questi carichi di lavoro perché alloca la capacità dai pool con il prezzo più basso che offrono anche una bassa frequenza di interruzione delle istanze spot.

Per una configurazione di esempio che utilizza la strategia di allocazione `price-capacity-optimized`, consulta la pagina Esempio 10: avvio di istanze Spot in un parco istanze price-capacity-optimized .

Quando i carichi di lavoro hanno un costo di interruzione elevato

Facoltativamente, è possibile utilizzare la strategia `capacity-optimized` se si eseguono carichi di lavoro che utilizzano tipi di istanze con prezzi simili o in cui il costo dell'interruzione è così significativo che qualsiasi risparmio sui costi è inadeguato rispetto a un aumento marginale delle interruzioni. Questa strategia alloca la capacità dai pool di capacità spot con maggiore disponibilità che offrono una possibilità minore di interruzioni, il che può ridurre il costo complessivo del carico di lavoro. Per una configurazione di esempio che utilizza la strategia di allocazione `capacity-optimized`, consulta la pagina Esempio 8: avvio di istanze Spot in un parco istanze ottimizzato in termini di capacità.

Quando è necessario ridurre al minimo la possibilità di interruzione ma la preferenza per determinati tipi di istanza è importante, puoi esprimere le priorità dei pool utilizzando la strategia di allocazione `capacity-optimized-prioritized` e quindi impostare l'ordine dei tipi di istanza da utilizzare dalla priorità più alta alla più bassa. Per un esempio di configurazione, consulta Esempio 9: avvia le istanze Spot in un parco istanze con priorità ottimizzate in termini di capacità.

Tieni presente che quando imposti le priorità per `capacity-optimized-prioritized`, le stesse priorità vengono applicate anche alle istanze on demand se la `AllocationStrategy` on demand è impostata su `prioritized`.

Quando il carico di lavoro è flessibile in termini di tempo e la capacità disponibile non è un fattore rilevante

Se il parco istanze è piccolo o viene eseguito per un breve periodo di tempo, puoi utilizzare `price-capacity-optimized` per massimizzare i risparmi sui costi pur tenendo conto della capacità disponibile.

Quando il parco istanze è grande o viene eseguito per un lungo periodo di tempo

Se il parco istanze è grande o funziona per un lungo periodo di tempo, puoi aumentare la disponibilità del parco istanze distribuendo la Istanze spot tra più pool utilizzando la strategia `diversified`. Ad esempio, se EC2 Fleet specifica 10 pool e una capacità target pari a 100 istanze, il parco istanze avvia 10 istanze spot in ogni pool. Se il prezzo Spot per un pool supera il prezzo massimo per tale pool, solo il 10% del parco istanze ne è interessato. L'utilizzo di questa strategia rende inoltre il parco istanze meno sensibile agli aumenti del prezzo Spot in ogni pool unico nel tempo. Con la strategia `diversified`, EC2 Fleet non avvia le Istanze spot nei pool con un prezzo Spot uguale o maggiore del prezzo on demand.

Mantenere la capacità target

Dopo che le istanze spot sono terminate a causa di una modifica del prezzo di Spot o della capacità disponibile di un pool di capacità spot, un EC2 Fleet di tipo `maintain` avvia il istanze spot di sostituzione. La strategia di allocazione determina i pool da cui vengono avviate le istanze sostitutive, come segue:

- Se la strategia di allocazione è `price-capacity-optimized`, il parco istanze avvia le istanze sostitutive nei pool che hanno la massima capacità disponibile di istanze spot tenendo in considerazione e identificando anche i pool con il prezzo più basso con una capacità disponibile elevata.
- Se la strategia di allocazione è `capacity-optimized`, il parco istanze avvia le istanze sostitutive nei pool che hanno la massima capacità disponibile di istanze spot.
- Se la strategia di allocazione è `diversified`, il parco istanze distribuisce le Istanze spot sostitutive nei pool rimanenti.

Selezione del tipo di istanza basata su attributi per il parco istanze EC2

Quando si crea un parco istanze EC2, è necessario specificare uno o più tipi di istanza per la configurazione delle istanze on-demand e delle istanze spot nel parco istanze. In alternativa alla

specifica manuale dei tipi di istanza, è possibile specificare gli attributi che un'istanza deve avere e Amazon EC2 identificherà tutti i tipi di istanza con tali attributi. Questo è noto come selezione del tipo di istanza basata su attributi. Ad esempio, è possibile specificare il numero minimo e massimo di vCPU richieste per le istanze e il parco istanze EC2 avvierà le istanze utilizzando qualsiasi tipo di istanza disponibile che soddisfi i requisiti di tali vCPU.

La selezione del tipo di istanza basata su attributi è ideale per carichi di lavoro e framework che possono essere flessibili sui tipi di istanza utilizzati, ad esempio quando si eseguono container o parchi istanze Web, elaborazione di Big Data e implementazione di strumenti CI/CD (Continuous Integration and Deployment).

Vantaggi

La selezione del tipo di istanza basata su attributi comporta i seguenti vantaggi:

- Usa facilmente i tipi di istanza giusti: con così tanti tipi di istanze disponibili, trovare i tipi di istanza giusti per il tuo carico di lavoro può richiedere molto tempo. Quando si specificano gli attributi dell'istanza, i tipi di istanza avranno automaticamente gli attributi richiesti per il carico di lavoro.
- Configurazione semplificata: per specificare manualmente più tipi di istanze per una flotta EC2, è necessario creare un override del modello di lancio separato per ogni tipo di istanza. Tuttavia, con la selezione del tipo di istanza basata su attributi, per fornire più tipi di istanza è necessario specificare solo gli attributi dell'istanza nel modello di avvio o in una sostituzione di un modello di avvio.
- Uso automatico di nuovi tipi di istanze: quando si specificano gli attributi delle istanze anziché i tipi di istanze, il parco istanze può utilizzare tipi di istanze di nuova generazione non appena vengono rilasciati, «a prova di futuro» della configurazione del parco istanze.
- Flessibilità del tipo di istanza: quando si specificano gli attributi dell'istanza anziché i tipi di istanza, EC2 Fleet può scegliere tra un'ampia gamma di tipi di istanze per il lancio delle istanze Spot, in linea con le migliori pratiche Spot in materia di flessibilità dei tipi di istanze.

Argomenti

- Anteprima di tipi di istanza con attributi specificati

Come funziona la selezione del tipo di istanza basata su attributi

Per utilizzare la selezione del tipo di istanza basata su attributi nella configurazione del parco istanze, è necessario sostituire l'elenco dei tipi di istanza con un elenco di attributi di istanza richiesti dalle istanze. Il parco istanze EC2 avvierà le istanze su qualsiasi tipo di istanza disponibile con gli attributi di istanza specificati.

Argomenti

- Tipi di attributi di istanza
- Dove configurare la selezione del tipo di istanza basata su attributi
- Come il parco istanze EC2 utilizza la selezione del tipo di istanza basata su attributi durante il provisioning di un parco istanze

Tipi di attributi di istanza

Esistono diversi attributi di istanza che puoi specificare per esprimere i tuoi requisiti di calcolo, come:

- Numero di vCPU: il numero minimo e massimo di vCPU per istanza.
- Memoria: il numero minimo e massimo GiBs di memoria per istanza.
- Archiviazione locale: se utilizzare EBS o i volumi di Instance Store per l'archiviazione locale.
- Prestazioni affidabili: se utilizzare la famiglia di istanze T, inclusi i tipi T4g, T3a, T3 e T2.

Per una descrizione di ogni attributo e dei valori predefiniti, InstanceRequirementsconsulta Amazon EC2 API Reference.

Dove configurare la selezione del tipo di istanza basata su attributi

A seconda che utilizzi la console o la AWS CLI, puoi specificare gli attributi dell'istanza per la selezione del tipo di istanza basata sugli attributi come segue:

Nella console è possibile specificare gli attributi di istanza nel seguente componente di configurazione del parco istanze:

- In un modello di avvio, facendo successivamente riferimento al modello di avvio nella richiesta del parco istanze

In AWS CLI, è possibile specificare gli attributi dell'istanza in uno o tutti i seguenti componenti di configurazione della flotta:

- In un modello di avvio, facendo successivamente riferimento al modello di avvio nella richiesta del parco istanze
- In una sostituzione del modello di avvio

  Se si desidera un mix di istanze che utilizzano AMI diverse, è possibile specificare gli attributi di istanza in più sostituzioni di modelli di avvio. Ad esempio, diversi tipi di istanza possono utilizzare processori x86 e ARM.

Come il parco istanze EC2 utilizza la selezione del tipo di istanza basata su attributi durante il provisioning di un parco istanze

Il parco istanze EC2 fornisce un parco istanze nel seguente modo:

- Il parco istanze EC2 identifica i tipi di istanza che hanno gli attributi specificati.
- Il parco istanze EC2 utilizza la protezione dei prezzi per determinare quali tipi di istanza escludere.
- EC2 Fleet determina i pool di capacità da cui prenderà in considerazione l'avvio delle istanze in base alle AWS regioni o alle zone di disponibilità con tipi di istanze corrispondenti.
- Il parco istanze EC2 applica la strategia di allocazione specificata per determinare da quali pool di capacità avviare le istanze.

  Notare che la selezione del tipo di istanza basata su attributi non sceglie i pool di capacità da cui effettuare il provisioning del parco istanze; questo è il compito delle strategie di allocazione.

  Se si specifica una strategia di allocazione, EC2 Fleet avvierà le istanze in base alla strategia di allocazione specificata.

  - Per le istanze spot, la selezione del tipo di istanza basata su attributi supporta le strategie di allocazione `price-capacity-optimized`, `capacity-optimized` e `lowest-price`. Tieni presente che non consigliamo la strategia di allocazione `lowest-price` Spot perché presenta il rischio di interruzione più elevato per le tue istanze Spot.
  - Per le istanze on demand, la selezione del tipo di istanza basata su attributi supporta la strategia di allocazione `lowest-price`.
- Se non è presente alcuna capacità per i tipi di istanza con gli attributi di istanza specificati, non è possibile avviare le istanze e il parco istanze restituisce un errore.

Protezione del prezzo

La protezione dei prezzi è una funzione che impedisce al proprio EC2 Fleet di utilizzare tipi di istanza troppo costosi anche se si adattano agli attributi specificati. Per utilizzare la protezione del prezzo, devi impostare una soglia di prezzo. Quindi, quando Amazon EC2 seleziona i tipi di istanza con i tuoi attributi, esclude i tipi di istanza con un prezzo superiore alla soglia.

Il modo in cui Amazon EC2 calcola la soglia di prezzo è il seguente:

- Amazon EC2 identifica innanzitutto il tipo di istanza con il prezzo più basso tra quelle che corrispondono ai tuoi attributi.
- Amazon EC2 prende quindi il valore (espresso in percentuale) specificato per il parametro di protezione del prezzo e lo moltiplica per il prezzo del tipo di istanza identificato. Il risultato è il prezzo utilizzato come soglia di prezzo.

Esistono soglie di prezzo separate per le istanze on demand e le istanze Spot.

Quando crei un parco istanze con selezione del tipo di istanza basata sugli attributi, la protezione del prezzo è abilitata per impostazione predefinita. Puoi mantenere i valori predefiniti oppure puoi specificarne uno personalizzato.

Puoi anche disattivare la protezione del prezzo. Per indicare l'assenza di una soglia di protezione del prezzo, specifica un valore percentuale elevato, ad esempio`999999`.

Argomenti

Come viene identificato il tipo di istanza con il prezzo più basso

Amazon EC2 determina il prezzo su cui basare la soglia di prezzo identificando il tipo di istanza con il prezzo più basso tra quelle che corrispondono agli attributi specificati. Lo fa nel modo seguente:

- Innanzitutto esamina i tipi di istanza C, M o R dell'attuale generazione che corrispondono ai tuoi attributi. Se trova delle corrispondenze, identifica il tipo di istanza con il prezzo più basso.

- Se non c'è alcuna corrispondenza, esamina tutti i tipi di istanza della generazione corrente che corrispondono ai tuoi attributi. Se trova delle corrispondenze, identifica il tipo di istanza con il prezzo più basso.
- Se non c'è alcuna corrispondenza, esamina tutti i tipi di istanza della generazione precedente che corrispondono ai tuoi attributi e identifica il tipo di istanza con il prezzo più basso.

Protezione del prezzo delle istanze On-Demand

La soglia di protezione del prezzo per i tipi di istanze On-Demand viene calcolata come percentuale superiore al tipo di istanza On-Demand identificato con il prezzo più basso (). `OnDemandMaxPricePercentageOverLowestPrice` Specifichi la percentuale più alta che sei disposto a pagare. Se non specifichi questo parametro, `20` viene utilizzato un valore predefinito di per calcolare una soglia di protezione del prezzo del 20% superiore al prezzo identificato.

Ad esempio, se il prezzo dell'istanza On-Demand identificata è`0.4271`, e lo si specifica`25`, la soglia di prezzo è superiore del 25% rispetto a`0.4271`. Viene calcolato come segue:`0.4271 * 1.25 = 0.533875`. Il prezzo calcolato è il massimo che sei disposto a pagare per le istanze On-Demand e, in questo esempio, Amazon EC2 escluderà qualsiasi tipo di istanza On-Demand che costa più di. `0.533875`

Protezione del prezzo delle istanze Spot

Per impostazione predefinita, Amazon EC2 applicherà automaticamente una protezione ottimale del prezzo delle istanze Spot per scegliere in modo coerente tra un'ampia gamma di tipi di istanze. Puoi anche impostare manualmente la protezione del prezzo. Tuttavia, lasciare che Amazon EC2 lo faccia per te può aumentare la probabilità che la tua capacità Spot venga soddisfatta.

Puoi specificare manualmente la protezione del prezzo utilizzando una delle seguenti opzioni. Se imposti manualmente la protezione del prezzo, ti consigliamo di utilizzare la prima opzione.

- Una percentuale del tipo di istanza On-Demand identificato con il prezzo più basso [] `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`

  Ad esempio, se il prezzo del tipo di istanza On-Demand identificato è`0.4271`, e lo si specifica`60`, la soglia di prezzo è pari al 60% di. `0.4271` Viene calcolato come segue:`0.4271 * 0.60 = 0.25626`. Il prezzo calcolato è il massimo che sei disposto a pagare per le istanze Spot e, in questo esempio, Amazon EC2 escluderà qualsiasi tipo di istanza Spot che costa più di. `0.25626`
- Una percentuale superiore al tipo di istanza Spot identificato con il prezzo più basso [] `SpotMaxPricePercentageOverLowestPrice`

Ad esempio, se il prezzo del tipo di istanza Spot identificato è`0.1808`, e lo si specifica`25`, la soglia di prezzo è superiore del 25% rispetto a`0.1808`. Viene calcolato come segue:`0.1808 * 1.25 = 0.226`. Il prezzo calcolato è il massimo che sei disposto a pagare per le istanze Spot e, in questo esempio, Amazon EC2 escluderà qualsiasi tipo di istanza Spot che costa più di. `0.266` Non consigliamo di utilizzare questo parametro perché i prezzi Spot possono variare e pertanto anche la soglia di protezione del prezzo potrebbe variare.

Specificate la soglia di protezione del prezzo

Per specificare la soglia di protezione del prezzo

Durante la creazione del parco istanze EC2, configura il parco istanze per la selezione del tipo di istanza basata su attributi ed esegui le seguenti operazioni:

- Per specificare la soglia di protezione del prezzo dell'istanza on demand, nel file di configurazione JSON, nella struttura `InstanceRequirements`, per `OnDemandMaxPricePercentageOverLowestPrice`, inserisci la soglia di protezione del prezzo in percentuale.
- Per specificare la soglia di protezione del prezzo dell'istanza Spot, nel file di configurazione JSON, nella `InstanceRequirements` struttura, specifica uno dei seguenti parametri:
  - Per`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, inserisci la soglia di protezione del prezzo come percentuale.
  - Per`SpotMaxPricePercentageOverLowestPrice`, inserite la soglia di protezione del prezzo in percentuale.

Per ulteriori informazioni sulla creazione del parco istanze, consulta Creazione di un EC2 Fleet con la selezione del tipo di istanza basata su attributi.

> **Note**
>
> Durante la creazione del parco istance EC2, se imposti `TargetCapacityUnitType` su `vcpu` o `memory-mib`, la soglia di protezione del prezzo viene applicata in base al prezzo per vCPU o per memoria, anziché al prezzo per istanza.

Considerazioni

- È possibile specificare i tipi di istanza o gli attributi di istanza in un parco istanze EC2, ma non entrambi nello stesso momento.

  Quando si utilizza la CLI, le sostituzioni del modello di avvio sovrascriveranno il modello di avvio. Ad esempio, se il modello di avvio contiene un tipo di istanza e la sostituzione del modello di avvio contiene attributi di istanza, le istanze identificate dagli attributi di istanza sostituiranno il tipo di istanza nel modello di avvio.
- Quando si utilizza la CLI e si specificano gli attributi di istanza come sostituzioni, non è possibile specificare pesi o priorità.
- In una configurazione di richiesta è possibile specificare un massimo di quattro strutture `InstanceRequirements`.

Creazione di un EC2 Fleet con la selezione del tipo di istanza basata su attributi

È possibile configurare un parco istanze in modo da utilizzare la selezione del tipo di istanza basata su attributi tramite la AWS CLI.

Creazione di un parco istanze EC2 con la selezione del tipo di istanza basata su attributi (AWS CLI)

Utilizza il comando create-fleet (AWS CLI) per creare un EC2 Fleet. Specificare la configurazione del parco istanze in un file JSON.

```
aws ec2 create-fleet \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Esempio di file *file_name*`.json`

L'esempio seguente contiene i parametri che configurano un parco istanze EC2 in modo da utilizzare la selezione del tipo di istanza basata su attributi ed è seguito da una spiegazione.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
```

```
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

I parametri per la selezione del tipo di istanza basata su attributi sono specificati nella struttura `InstanceRequirements`. In questo esempio, vengono specificati due attributi:

- `VCpuCount`: viene specificato un minimo di 2 vCPU. Poiché non è specificato alcun massimo, non esiste un limite massimo.
- `MemoryMiB`: viene specificato un minimo di 4 MiB di memoria. Poiché non è specificato alcun massimo, non esiste un limite massimo.

Verranno identificati tutti i tipi di istanza con 2 o più vCPU e 4 MiB o più di memoria. Tuttavia, la protezione dei prezzi e la strategia di allocazione potrebbero escludere alcuni tipi di istanze quando il parco istanze EC2 alloca le istanze.

Per un elenco e le descrizioni di tutti i possibili attributi che puoi specificare, consulta InstanceRequirementsAmazon EC2 API Reference.

> **Note**
>
> Quando `InstanceRequirements` è incluso nella configurazione del parco istanze, `InstanceType` e `WeightedCapacity` devono essere esclusi; non possono determinare la configurazione del parco istanze contemporaneamente agli attributi di istanza.

Il JSON contiene anche la seguente configurazione del parco istanze:

- `"AllocationStrategy": "price-capacity-optimized"`: la strategia di allocazione per le istanze spot nel parco istanze.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"`: il modello di avvio contiene alcune informazioni sulla configurazione delle istanze; tuttavia, se vengono specificati dei tipi di istanza, questi verranno sostituiti dagli attributi specificati in `InstanceRequirements`.
- `"TotalTargetCapacity": 20`: la capacità obiettivo è di 20 istanze.
- `"DefaultTargetCapacityType": "spot"`: la capacità predefinita è istanze spot.
- `"Type": "instant"`: il tipo di richiesta per il parco istanze è `instant`.

Esempi di configurazioni valide e non valide

Se utilizzi il AWS CLI per creare una flotta EC2, devi assicurarti che la configurazione del tuo parco veicoli sia valida. I seguenti esempi mostrano configurazioni valide e non valide.

Le configurazioni sono considerate non valide quando contengono quanto segue:

- Una singola struttura `Overrides` con `InstanceRequirements` e `InstanceType`
- Due strutture `Overrides`, una con `InstanceRequirements` e l'altra con `InstanceType`
- Due strutture `InstanceRequirements` con valori di attributo sovrapposti all'interno dello stesso `LaunchTemplateSpecification`

Configurazioni di esempio

- Configurazione valida: modello di avvio singolo con sostituzioni
- Configurazione valida: modello di lancio singolo con più modelli InstanceRequirements
- Configurazione valida: due modelli di avvio, ognuno con sostituzioni
- Configurazione valida: specificati solo InstanceRequirements, nessun valore di attributo sovrapposto
- Configurazione non valida: Overrides contiene InstanceRequirements e InstanceType
- Configurazione non valida: due Overrides contengono InstanceRequirements e InstanceType
- Configurazione non valida: valori di attributo sovrapposti

Configurazione valida: modello di avvio singolo con sostituzioni

La configurazione seguente è valida. Contiene un modello di avvio e una struttura `Overrides` contenente una struttura `InstanceRequirements`. Di seguito è riportata una spiegazione della configurazione di esempio.

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
        "DefaultTargetCapacityType": "spot",
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

Per utilizzare la selezione dell'istanza basata su attributi, è necessario includere la struttura `InstanceRequirements` nella configurazione del parco istanze e specificare gli attributi desiderati per le istanze nel parco istanze.

Nell'esempio precedente, vengono specificati i seguenti attributi di istanza:

- `VCpuCount`: i tipi di istanza devono avere un minimo di 2 e un massimo di 8 vCPU.
- `MemoryMiB`: i tipi di istanza devono avere un massimo di 10240 MiB di memoria. Un minimo di 0 indica nessun limite minimo.
- `MemoryGiBPerVCpu`: i tipi di istanza devono avere un massimo di 10.000 MiB di memoria per vCPU. Il parametro `Min` è facoltativo. Omettendolo, non si indica alcun limite minimo.

`TargetCapacityUnitType`

Il parametro `TargetCapacityUnitType` specifica l'unità per la capacità di destinazione. Nell'esempio, la capacità di destinazione è `5000` e il tipo di unità della capacità di destinazione è `vcpu`, che insieme specificano una capacità di destinazione desiderata di 5.000 vCPU. Il parco istanze EC2 avvierà una quantità sufficiente di istanze in modo che il numero totale di vCPU nel parco istanze sia 5.000.

Configurazione valida: modello di lancio singolo con più modelli InstanceRequirements

La configurazione seguente è valida. Contiene un modello di avvio e una struttura `Overrides` contenente due strutture `InstanceRequirements`. Gli attributi specificati in `InstanceRequirements` sono validi perché i valori non si sovrappongono; la prima struttura `InstanceRequirements` specifica un `VCpuCount` di 0-2 vCPU, mentre la seconda struttura `InstanceRequirements` specifica 4-8 vCPU.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
```

```
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configurazione valida: due modelli di avvio, ognuno con sostituzioni

La configurazione seguente è valida. Contiene due modelli di avvio, ognuno con una struttura `Overrides` contenente una struttura `InstanceRequirements`. Questa configurazione è utile per il supporto delle architetture `arm` e `x86` nello stesso parco istanze.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
```

```
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configurazione valida: specificati solo **`InstanceRequirements`**, nessun valore di attributo sovrapposto

La configurazione seguente è valida. Contiene due strutture `LaunchTemplateSpecification`, ognuna con un modello di avvio e una struttura `Overrides` contenente una struttura `InstanceRequirements`. Gli attributi specificati in `InstanceRequirements` sono validi perché i

valori non si sovrappongono; la prima struttura `InstanceRequirements` specifica un `VCpuCount` di 0-2 vCPU, mentre la seconda struttura `InstanceRequirements` specifica 4-8 vCPU.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
```

```
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configurazione non valida: **`Overrides`** contiene **`InstanceRequirements`** e **`InstanceType`**

La configurazione seguente non è valida. La struttura `Overrides` include sia `InstanceRequirements` che `InstanceType`. Per le `Overrides`, è possibile specificare `InstanceRequirements` o `InstanceType`, ma non entrambi.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
```

```
    }
}
```

Configurazione non valida: due **`Overrides`** contengono **`InstanceRequirements`** e **`InstanceType`**

La configurazione seguente non è valida. Le strutture `Overrides` contengono sia `InstanceRequirements` che `InstanceType`. È possibile specificare `InstanceRequirements` o `InstanceType` ma non entrambi, anche se si trovano in strutture `Overrides` differenti.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
```

```
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configurazione non valida: valori di attributo sovrapposti

La configurazione seguente non è valida. Le due strutture `InstanceRequirements`, ognuna contenente `"VCpuCount": {"Min": 0, "Max": 2}`. I valori di questi attributi si sovrappongono, il che restituirà pool di capacità duplicati.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
```

```
                ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Anteprima di tipi di istanza con attributi specificati

È possibile utilizzare il AWS CLI comando get-instance-types-from-instance-requirements per visualizzare in anteprima i tipi di istanza che corrispondono agli attributi specificati. Ciò è particolarmente utile per capire quali attributi specificare nella configurazione della richiesta senza avviare alcuna istanza. Si noti che il comando non considera la capacità disponibile.

Per visualizzare in anteprima un elenco di tipi di istanze specificando gli attributi utilizzando il AWS CLI

1. (Facoltativo) Per generare tutti i possibili attributi che possono essere specificati, utilizzate il comando get-instance-types-from-instance-requirements e il parametro. `--generate-cli-skeleton` Facoltativamente, è possibile indirizzare l'output a un file per salvarlo tramite `input > attributes.json`.

   ```
   aws ec2 get-instance-types-from-instance-requirements \
       --region us-east-1 \
       --generate-cli-skeleton input > attributes.json
   ```

   Output previsto

   ```
   {
       "DryRun": true,
       "ArchitectureTypes": [
           "i386"
       ],
       "VirtualizationTypes": [
           "hvm"
       ],
       "InstanceRequirements": {
           "VCpuCount": {
   ```

```
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
```

```
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Creare un file di configurazione JSON utilizzando l'output del passaggio precedente e configurarlo come segue:

> **Note**
>
> È necessario fornire valori per `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. È possibile omettere gli altri attributi, nel qual caso saranno utilizzati i valori di default.
> Per una descrizione di ogni attributo e dei relativi valori predefiniti, consulta get-instance-types-from-instance-requirements in Amazon EC2 Command Line Reference.

   a. Per `ArchitectureTypes`, specificare uno o più tipi di architettura del processore.

   b. Per `VirtualizationTypes`, specificare uno o più tipi di virtualizzazione.

c. Per `VCpuCount`, specificare il numero minimo e massimo di vCPU. Per non specificare un limite minimo, per `Min`, specificare `0`. Per non specificare alcun limite massimo, omettere il parametro `Max`.

d. Per `MemoryMiB`, specificare la quantità minima e massima di memoria in MiB. Per non specificare un limite minimo, per `Min`, specificare `0`. Per non specificare alcun limite massimo, omettere il parametro `Max`.

e. Facoltativamente, è possibile specificare uno o più altri attributi per limitare ulteriormente l'elenco di tipi di istanza restituiti.

3. Per visualizzare in anteprima i tipi di istanza con gli attributi specificati nel file JSON, usa il comando get-instance-types-from-instance-requirements e specifica il nome e il percorso del file JSON utilizzando il parametro. `--cli-input-json` Facoltativamente, è possibile formattare l'output in modo che venga visualizzato in un formato tabella.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Esempio di file *attributes.json*

In questo esempio gli attributi richiesti sono inclusi nel file JSON. Tali attributi sono `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. Inoltre, è incluso anche l'attributo facoltativo `InstanceGenerations`. Tenere presente che per `MemoryMiB`, il valore `Max` può essere omesso per indicare che non c'è alcun limite.

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
```

```
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

Output di esempio

```
----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+--------------------------------------+
||             InstanceTypes            ||
|+------------------------------------+|
||             InstanceType             ||
|+------------------------------------+|
||  c4.xlarge                         ||
||  c5.xlarge                         ||
||  c5a.xlarge                        ||
||  c5ad.xlarge                       ||
||  c5d.xlarge                        ||
||  c5n.xlarge                        ||
||  d2.xlarge                         ||
...
```

4. Dopo aver identificato i tipi di istanza che soddisfano le proprie esigenze, prendere nota degli attributi di istanza utilizzati in modo da poterli utilizzare durante la configurazione della richiesta del parco istanze.

Configurazione di EC2 Fleet per il backup on demand

Se si hanno esigenze di dimensionamento urgenti e imprevedibili, come per esempio un sito web di notizie che deve essere ridimensionato in caso di una notizia importante o un lancio di un gioco, si consiglia di specificare tipi di istanza alternativi per le Istanze on demand, nel caso in cui l'opzione preferita non abbia sufficiente capacità disponibile. Ad esempio, si potrebbero preferire Istanze on demand `c5.2xlarge`, ma se non c'è abbastanza capacità disponibile, si potrebbe essere disposti a utilizzare alcune istanze `c4.2xlarge` durante i carichi di picco. In tal caso, il parco istanze EC2 tenta di soddisfare tutta la capacità target tramite le istanze `c5.2xlarge`, ma se la capacità è insufficiente, avvia automaticamente le istanze `c4.2xlarge` per soddisfare la capacità target.

Argomenti

Dare priorità ai tipi di istanze per la capacità on demand

Quando il parco istanze EC2 cerca di soddisfare la capacità on demand, per impostazione predefinita avvia come primo tipo di istanza quello con il prezzo più basso. Se `AllocationStrategy` è impostata su `prioritized`, il parco istanze EC2 utilizza la priorità per stabilire quale tipo di istanza utilizzare per primo per la capacità on demand. La priorità è assegnata alla sostituzione del modello di avvio e la priorità più alta viene lanciata per prima.

Esempio: assegnare priorità ai tipi di istanza

Ad esempio, hai configurato tre sostituzioni dei modelli di avvio, ognuna con un tipo di istanza diversa.

Il prezzo on demand per i tipi di istanze varia nel prezzo. Di seguito sono riportati i tipi di istanza utilizzati in questo esempio, elencati in ordine di prezzo, a partire dal tipo di istanza più economico:

- `m4.large`: meno costosa
- `m5.large`
- `m5a.large`

Se non usi la priorità per stabilire l'ordine, il parco istanze utilizza la capacità on demand partendo dal tipo di istanza con il prezzo più basso.

Tuttavia, poniamo che tu non abbia utilizzato le istanze riservate `m5.large` che vuoi utilizzare per prime. È possibile impostare la priorità di sostituzione del modello di avvio in modo che i tipi di istanze vengano utilizzati nell'ordine di priorità, come segue:

- `m5.large`: priorità 1
- `m4.large`: priorità 2
- `m5a.large`: priorità 3

Utilizzo di Prenotazioni di capacità per Istanze on demand

Le prenotazioni della capacità on demand ti permettono di prenotare la capacità di calcolo per le istanze on demand in una zona di disponibilità specifica per qualsiasi durata. È possibile configurare un parco istanze EC2 per utilizzare prima le prenotazioni della capacità all'avvio delle istanze on demand.

Le prenotazioni delle capacità sono configurate come `open` o `targeted`. Il parco istanze EC2 può avviare istanze on demand nelle prenotazioni della capacità `open` o `targeted` nel modo seguente:

- Se la prenotazione della capacità è `open`, le istanze on demand che hanno attributi corrispondenti vengono eseguite automaticamente nella capacità riservata.
- Se la prenotazione della capacità è `targeted`, le istanze on demand devono specificamente puntarla per l'esecuzione nella capacità riservata. Ciò è utile per utilizzare una specifica prenotazione della capacità o per controllare quando utilizzare specifiche prenotazioni della capacità.

Se si utilizzano le prenotazioni della capacità `targeted` nel parco istanze EC2, devono esservi sufficienti prenotazioni della capacità per soddisfare la capacità on demand obiettivo, altrimenti l'avvio non riesce. Per evitare un errore di avvio, aggiungere invece le prenotazioni della capacità `targeted` a un gruppo di risorse e quindi prendere come obiettivo il gruppo di risorse. Non è necessario che il gruppo di risorse disponga di prenotazioni della capacità sufficienti; se esaurisce le prenotazioni della capacità prima che venga soddisfatta la capacità on demand obiettivo, il parco istanze può avviare la capacità obiettivo rimanente nella normale capacità on demand.

Per utilizzare le prenotazioni della capacità con il parco istanze EC2

1. Configurare il parco istanze come tipo `instant`. Non è possibile utilizzare le prenotazioni della capacità per parchi istanze di altri tipi.
2. Configurare la strategia di utilizzo per le prenotazioni della capacità come `use-capacity-reservations-first`.
3. Nel modello di avvio, per Capacity reservation (Prenotazione della capacità) scegliere Open (Aperta) o Target by group (Obiettivo per gruppo). Se si sceglie Target by group (Definisci obiettivo in base al gruppo), specificare l'ID gruppo di risorsa della prenotazione della capacità.

Quando il parco istanze tenta di soddisfare la capacità on demand, se rileva che più pool di istanze hanno prenotazioni della capacità corrispondenti inutilizzate, determina i pool in cui avviare le istanze on demand in base alla strategia di allocazione on demand (`lowest-price` o `prioritized`).

Per esempi su come configurare un parco istanze affinché utilizzi le prenotazioni della capacità per gestire la capacità on demand, consulta Configurazioni parco istanze EC2 di esempio, in particolare gli esempi dal 5 al 7.

Per informazioni sulla configurazione delle prenotazioni della capacità, consulta Prenotazione della capacità on demand e le Domande frequenti sulla prenotazione della capacità on demand.

Ribilanciamento della capacità

È possibile configurare EC2 Fleet per l'avvio di un'istanza spot sostitutiva quando Amazon EC2 emette un suggerimento di ribilanciamento per notificare che un'istanza spot è a rischio elevato di interruzione. Il ribilanciamento della capacità consente di mantenere la disponibilità del carico di lavoro aumentando proattivamente il parco istanze con una nuova istanza spot prima che un'istanza in esecuzione venga interrotta da Amazon EC2. Per ulteriori informazioni, consulta Raccomandazioni per il ribilanciamento delle istanze EC2.

Per configurare un parco istanze EC2 in modo che avvii un'istanza spot sostitutiva, utilizza il comando create-fleet (AWS CLI) e i relativi parametri nella struttura di `MaintenanceStrategies`. Per ulteriori informazioni, vedere l' esempio di configurazione di avvio.

Limitazioni

- Il ribilanciamento della capacità è disponibile solo per i parchi istanza di tipo `maintain`.
- Quando il parco istanze è in esecuzione, non è possibile modificare l'impostazione di ribilanciamento della capacità. Per modificare l'impostazione di ribilanciamento capacità, è necessario eliminare il parco istanze e crearne uno nuovo.

Opzioni di configurazione

`ReplacementStrategy` per EC2 Fleet supporta i seguenti due valori:

`launch-before-terminate`

Amazon EC2 termina le istanze spot che ricevono una notifica di ribilanciamento dopo avere avviato le nuove istanze spot sostitutive. Se si specifica `launch-before-terminate`, occorre specificare un valore anche per `termination-delay`. Dopo l'avvio delle nuove istanze

sostitutive, Amazon EC2 attende la durata di `termination-delay`, quindi termina le vecchie istanze. Per `termination-delay`, il minimo è 120 secondi (2 minuti) e il massimo è di 7200 secondi (2 ore).

Consigliamo di utilizzare `launch-before-terminate` solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza. Ciò garantirà che le vecchie istanze vengano terminate solo dopo il completamento delle procedure di arresto. Tenere presente che Amazon EC2 può interrompere le vecchie istanze con un avviso di due minuti prima di `termination-delay`.

Consigliamo vivamente di non utilizzare la strategia di allocazione `lowest-price` insieme a `launch-before-terminate` per evitare di avere istanze spot sostitutive che presentano anche un rischio elevato di interruzione.

`launch`

Amazon EC2 avvia le istanze spot sostitutive quando viene emessa una notifica di ribilanciamento per le istanze spot esistenti. Amazon EC2 non termina le istanze che ricevono una notifica di ribilanciamento. È possibile terminare le vecchie istanze o lasciarle in esecuzione. Saranno addebitati i costi per entrambe le istanze durante la loro esecuzione.

Considerazioni

Se si configura un parco istanze EC2 per il ribilanciamento della capacità, è necessario considerare quanto segue:

Fornisci il maggior numero possibile di pool di capacità spot nella richiesta

Configura EC2 Fleet affinché utilizzi diversi tipi di istanza e zone di disponibilità. Ciò fornisce la flessibilità necessaria per avviare Istanze spot in vari pool di capacità spot. Per ulteriori informazioni, consulta Essere flessibili riguardo tipi di istanza e zone di disponibilità.

Evitare un rischio elevato di interruzione delle istanze spot sostitutive

Le Spot Instances (Istanze spot) sostitutive possono comportare un elevato rischio di interruzione se si utilizza la strategia di allocazione `lowest-price`. Questo perché Amazon EC2 avvierà sempre le istanze nel pool con capacità disponibile al prezzo più basso in quel momento, anche se è probabile che le istanze spot sostitutive vengano interrotte subito dopo l'avvio. Per evitare un rischio elevato di interruzione, raccomandiamo vivamente di non utilizzare la strategia di allocazione `lowest-price` ma utilizzare invece la strategia `capacity-optimized` o

`capacity-optimized-prioritized`. Queste strategie garantiscono che le Spot Instances (Istanze spot) sostitutive vengano avviate nei pool di capacità spot ottimali per cui è meno probabile che vengano interrotte nel prossimo futuro. Per ulteriori informazioni, consulta Utilizzo della strategia di allocazione ottimizzata per prezzo e capacità.

Amazon EC2 avvierà una nuova istanza solo se la disponibilità è uguale o migliore

Uno degli obiettivi del ribilanciamento della capacità è migliorare la disponibilità di un'istanza spot. Se un'istanza spot esistente riceve una raccomandazione di ribilanciamento, Amazon EC2 avvierà una nuova istanza solo se la nuova istanza fornisce una disponibilità uguale o migliore rispetto all'istanza esistente. Se il rischio di interruzione di una nuova istanza è peggiore di quello dell'istanza esistente, Amazon EC2 non avvierà una nuova istanza. Tuttavia, Amazon EC2 continuerà a valutare i pool di capacità spot e avvierà una nuova istanza se la disponibilità migliorerà.

È possibile che l'istanza esistente venga interrotta senza che Amazon EC2 avvii in modo proattivo una nuova istanza. In questo caso, Amazon EC2 tenterà di avviare una nuova istanza indipendentemente dal fatto che la nuova istanza presenti un rischio elevato di interruzione.

Il ribilanciamento della capacità non aumenta il tasso di interruzione dell'istanza Spot

Quando si abilita il ribilanciamento della capacità, non aumenta il tasso di interruzione dell'istanza spot (il numero di istanze Spot che vengono recuperate quando Amazon EC2 ha bisogno di capacità). Tuttavia, se il ribilanciamento della capacità rileva che un'istanza è a rischio di interruzione, Amazon EC2 tenterà immediatamente di avviare una nuova istanza. Il risultato è che potrebbero essere sostituite più istanze di quelle che sarebbero state sostituite se avessi aspettato che Amazon EC2 avviasse una nuova istanza dopo l'interruzione di quella a rischio.

Sebbene sia possibile sostituire più istanze mediante l'abilitazione del ribilanciamento delle capacità, è meglio prendersi più tempo per agire prima che le istanze vengano interrotte. Con un Avviso di interruzione dell'istanza Spot, in genere hai solo fino a due minuti per interrompere l'istanza. Con il ribilanciamento della capacità che avvia una nuova istanza in anticipo, offri ai processi esistenti maggiori possibilità di completamento sull'istanza a rischio, puoi avviare le procedure di chiusura dell'istanza e impedire la pianificazione di nuovi lavori sull'istanza a rischio. Puoi anche iniziare a preparare l'istanza appena avviata per assumere il controllo dell'applicazione. Con la sostituzione proattiva offerta dal ribilanciamento della capacità, puoi beneficiare di una continuità regolare.

Come esempio teorico per dimostrare i rischi e i benefici dell'utilizzo del ribilanciamento della capacità, osserviamo il seguente scenario:

- 14:00: viene ricevuto un suggerimento di ribilanciamento per l'istanza A e Amazon EC2 inizia immediatamente a tentare di avviare un'istanza sostitutiva B, dandoti il tempo di iniziare le procedure di arresto.*
- 14:30: viene ricevuto un suggerimento di ribilanciamento per l'istanza B, sostituita dall'istanza C dandoti il tempo di iniziare le procedure di arresto.*
- 14:32: se il ribilanciamento della capacità non fosse abilitato e se un avviso di interruzione dell'istanza Spot fosse stato ricevuto alle 14:32 per l'istanza A, avresti avuto solo fino a due minuti per agire, ma l'istanza A sarebbe stata in esecuzione fino a questo momento.

* Se `launch-before-terminate` è specificato, Amazon EC2 terminerà l'istanza a rischio dopo che l'istanza sostitutiva sarà online.

Amazon EC2 può avviare nuove Istanze spot sostitutive fino a quando la capacità soddisfatta non è il doppio della capacità obiettivo

Quando un parco istanze EC2 è configurato per il ribilanciamento della capacità, il parco istanze tenta di avviare una nuova istanza spot sostitutiva per ogni istanza spot che riceve un suggerimento di ribilanciamento. Dopo che un'istanza spot riceve un suggerimento di ribilanciamento, non viene più conteggiata come parte della capacità evasa. A seconda della strategia di sostituzione, Amazon EC2 termina l'istanza dopo un ritardo di terminazione preconfigurato o la lascia in esecuzione. In questo modo è possibile eseguire operazioni di ribilanciamento sull'istanza.

Se il parco istanze raggiunge il doppio della capacità target, smette di lanciare nuove istanze sostitutive anche se le istanze sostitutive stesse ricevono una raccomandazione di ribilanciamento.

Ad esempio, si crea un parco istanze EC2 con una capacità target di 100 istanze spot. Tutte le istanze spot ricevono un suggerimento di ribilanciamento, cosicché Amazon EC2 avvia 100 istanze spot sostitutive. In questo modo il numero di istanze spot evase sale a 200, che è il doppio della capacità target. Alcune istanze sostitutive ricevono una raccomandazione di ribilanciamento, ma non vengono più avviate istanze sostitutive perché il parco istanze non può superare il doppio della capacità target.

Tenere presente che tutte le istanze vengono addebitate mentre sono in esecuzione.

Si consiglia di configurare EC2 Fleet in modo che termini le istanze spot che ricevono un suggerimento di ribilanciamento

Se si configura il parco istanze EC2 per il ribilanciamento della capacità, consigliamo di scegliere `launch-before-terminate` con un ritardo di terminazione appropriato solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza. Ciò garantirà che le vecchie istanze vengano terminate solo dopo il completamento delle procedure di arresto.

Se si decide di terminare autonomamente le istanze suggerite per il ribilanciamento, si consiglia di monitorare il segnale di suggerimento del ribilanciamento ricevuto dalle istanze spot nel parco istanze. Monitorando il segnale, puoi eseguire rapidamente le operazioni di ribilanciamento sulle istanze interessate prima che Amazon EC2 le interrompa; poi potrai terminarle manualmente. Se non si terminano le istanze, verranno addebitati i relativi costi fintantoché sono in esecuzione. Amazon EC2 non termina automaticamente le istanze che ricevono un suggerimento di ribilanciamento.

Puoi configurare le notifiche utilizzando Amazon EventBridge o i metadati delle istanze. Per ulteriori informazioni, consulta Monitorare i segnali di raccomandazione di ribilanciamento.

parco istanze EC2 non conteggia le istanze che ricevono una raccomandazione di ribilanciamento quando calcola la capacità evasa durante il dimensionamento orizzontale o verticale

Se EC2 Fleet è configurato per il ribilanciamento della capacità e si modifica la capacità di destinazione per l'aumento o la diminuzione, il parco istanze non conteggia le istanze contrassegnate per il ribilanciamento come parte della capacità evasa, come indicato di seguito:

- Riduzione orizzontale: se riduci la capacità obiettivo desiderata, Amazon EC2 termina le istanze che non sono contrassegnate per il ribilanciamento fino a quando non viene raggiunta la capacità desiderata. Le istanze contrassegnate per il ribilanciamento non vengono conteggiate per la capacità evasa.

  Ad esempio, crei un parco istanze EC2 con una capacità obiettivo di 100 istanze spot. 10 istanze ricevono un suggerimento di ribilanciamento, quindi Amazon EC2 avvia 10 nuove istanze sostitutive, con una capacità soddisfatta di 110 istanze. Riduci quindi la capacità obiettivo a 50 (riduzione orizzontale), ma la capacità soddisfatta è in realtà di 60 istanze, perché le 10 istanze contrassegnate per il ribilanciamento non vengono terminate da Amazon EC2. È necessario terminare manualmente queste istanze oppure lasciarle in esecuzione.

- Aumento orizzontale: se aumenti la capacità desiderata obiettivo, Amazon EC2 avvia nuove istanze fino al raggiungimento della capacità desiderata. Le istanze contrassegnate per il ribilanciamento non vengono conteggiate per la capacità evasa.

  Ad esempio, crei un parco istanze EC2 con una capacità obiettivo di 100 istanze spot. 10 istanze ricevono un suggerimento di ribilanciamento, quindi il parco istanze avvia 10 nuove istanze sostitutive, con una capacità evasa di 110 istanze. Si aumenta quindi la capacità target a 200 (dimensionamento orizzontale), ma la capacità evasa effettiva è di 210 istanze, perché le 10 istanze contrassegnate per il ribilanciamento non vengono conteggiate dal parco istanze come parte della capacità target. È necessario terminare manualmente queste istanze oppure lasciarle in esecuzione.

Sostituzioni prezzo massimo

Ogni parco istanze EC2 può includere un prezzo massimo globale o utilizzare quello predefinito (il prezzo on demand). Il parco istanze utilizza questo come il prezzo massimo predefinito per ciascuna delle sue specifiche di avvio.

È anche possibile specificare un prezzo massimo in una o più specifiche di avvio. Questo prezzo è relativo alla specifica di avvio. Se una specifica di avvio include un prezzo specifico, EC2 Fleet utilizza tale prezzo massimo, sostituendo il prezzo massimo globale. Le altre specifiche di avvio che non comprendono un prezzo massimo specifico continuano a utilizzare il prezzo massimo globale.

Controllo delle spese

parco istanze EC2 interrompe l'avvio delle istanze quando ha raggiunto uno dei parametri seguenti: la `TotalTargetCapacity` o il `MaxTotalPrice` (l'importo massimo che sei disposto a pagare). Per controllare l'importo che paghi all'ora per il parco istanze, puoi specificare il parametro `MaxTotalPrice`. Quando viene raggiunto il prezzo totale massimo, parco istanze EC2 interrompe l'avvio delle istanze anche se non è stata raggiunta la capacità target.

I seguenti esempi illustrano due scenari diversi. Nel primo, parco istanze EC2 interrompe l'avvio delle istanze quando ha raggiunto la capacità target. Nel secondo, parco istanze EC2 interrompe l'avvio delle istanze quando ha raggiunto l'importo massimo che sei disposto a pagare (`MaxTotalPrice`).

Esempio: arresto dell'avvio delle istanze al raggiungimento della capacità target

Data una richiesta di Istanze on demand `m4.large`, dove:

- Prezzo on demand: 0,10 USD all'ora

- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 1,50 USD

EC2 Fleet parco istanze EC2 avvia 10 Istanze on demand perché il totale di 1 USD (10 istanze x 0,10 USD) non supera il `MaxTotalPrice` di 1,50 USD per le Istanze on demand.

Esempio: arresto dell'avvio delle istanze al raggiungimento del prezzo totale massimo

Data una richiesta di Istanze on demand `m4.large`, dove:

- Prezzo on demand: 0,10 USD all'ora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 0,80 USD

Se Parco istanze EC2 avvia la capacità target on demand (10 Istanze on demand), il costo totale all'ora è di 1 USD. ovvero un importo superiore rispetto a quello specificato (0,80 USD) per il parametro `MaxTotalPrice` per le Istanze on demand. Per evitare di spendere più di quello che ti sei prefissato, parco istanze EC2 avvia solo 8 Istanze on demand (al di sotto della capacità target on demand) perché avviarne di più significherebbe superare il `MaxTotalPrice` per le Istanze on demand.

Ponderazione istanza parco istanze EC2

Durante la creazione di un parco istanze EC2, è possibile definire le unità di capacità con cui ciascun tipo di istanza contribuirà alle prestazioni dell'applicazione. Puoi modificare quindi il prezzo massimo per ogni specifica di avvio tramite la ponderazione dell'istanza.

Per impostazione predefinita, il prezzo specificato è all'ora per istanza. Quando si utilizza la funzionalità di ponderazione di istanza, il prezzo specificato è all'ora per unità. È possibile calcolare il prezzo all'ora per unità dividendo il prezzo di un tipo di istanza per il numero di unità che essa rappresenta. Il parco istanze EC2 calcola il numero di istanze da avviare dividendo la capacità obiettivo per il peso dell'istanza. Se il risultato non è un numero intero, il parco istanze lo arrotonda al numero intero successivo, in modo che la dimensione del parco istanze non sia inferiore alla sua capacità di destinazione. Il parco istanze può selezionare qualsiasi pool specificato nella specifica di avvio, anche se la capacità delle istanze avviate supera la capacità di destinazione richiesta.

La tabella seguente include esempi di calcoli per determinare il prezzo per unità per un parco istanze EC2 con una capacità di destinazione di 10.

Tipo di istanza	Peso dell'istanza	Capacità di destinazione	Numero di istanze avviate	Prezzo all'ora per istanza	Prezzo all'ora per unità
`r3.xlarge`	2	10	5 (10 diviso 2)	0,05 USD	0,025 USD (0,05 diviso 2)
`r3.8xlarge`	8	10	2 (10 diviso 8, risultato arrotondato)	0,10 USD	0,0125 USD (0,10 diviso 8)

Utilizzare la ponderazione d'istanza parco istanze EC2 come segue per assegnare la capacità di destinazione desiderata nei pool con il prezzo più basso per unità al momento dell'adempimento:

1. Impostare la capacità di destinazione per il parco istanze EC2 sia nelle istanze (predefinite) sia nelle unità prescelte, come CPU virtuali, memoria, archiviazione o throughput.
2. Impostare il prezzo per unità.
3. Per ogni specifica di avvio, indicare il peso, ovvero il numero di unità che il tipo di istanza rappresenta per la capacità di destinazione.

Esempio di ponderazione istanza

Considerare una richiesta parco istanze EC2 con la configurazione seguente:

- Una capacità di destinazione di 24
- Una specifica di avvio con un tipo di istanza `r3.2xlarge` e un peso di 6
- Una specifica di avvio con un tipo di istanza `c3.xlarge` e un peso di 5

I pesi rappresentano il numero di unità che il tipo di istanza rappresenta per la capacità di destinazione. Se la prima specifica di avvio fornisce il prezzo più basso per unità (prezzo per `r3.2xlarge` all'ora per istanza diviso 6), EC2 Fleet lancerà quattro di tali istanze (24 diviso 6).

Se la seconda specifica di avvio fornisce il prezzo più basso per unità (prezzo per `c3.xlarge` all'ora per istanza diviso 5), EC2 Fleet lancerà cinque di tali istanze (24 diviso 5, risultato arrotondato).

Ponderazione d'istanza e strategia di allocazione

Considerare una richiesta Parco istanze EC2 con la configurazione seguente:

- Una capacità obiettivo di 30 Istanze spot
- Una specifica di avvio con un tipo di istanza `c3.2xlarge` e un peso di 8
- Una specifica di avvio con un tipo di istanza `m3.xlarge` e un peso di 8
- Una specifica di avvio con un tipo di istanza `r3.xlarge` e un peso di 8

EC2 Fleet avvierà quattro istanze (30 diviso 8, risultato arrotondato). Con la strategia `diversified`, il parco istanze avvia un'istanza in ognuno dei tre pool e la quarta istanza in qualsiasi dei tre pool che fornisce il prezzo più basso per unità.

Utilizzo di Parchi istanze EC2

Per utilizzare un parco istanze EC2, si crea una richiesta che include la capacità target totale, la capacità on demand, la capacità spot, una o più specifiche di avvio per le istanze e il prezzo massimo che si è disposti a pagare. La richiesta del parco istanze deve includere un modello di avvio che indichi le informazioni di cui il parco istanze ha bisogno per avviare un'istanza, come un'AMI, un tipo di istanza, una sottorete o una zona di disponibilità e uno o più gruppi di sicurezza. È possibile indicare le sostituzioni delle specifiche di avvio per il tipo di istanza, la sottorete, la zona di disponibilità e il prezzo massimo che si desidera pagare, nonché assegnare una capacità ponderata a ciascuna sostituzione delle specifiche di avvio.

Il parco istanze EC2 avvia le Istanze on demand quando c'è capacità disponibile e avvia le Istanze spot quando il prezzo massimo supera il prezzo Spot e la capacità è disponibile.

Se il parco istanze include Istanze spot, Amazon EC2 può tentare di mantenere la capacità di destinazione del parco istanze al variare dei prezzi Spot.

Una richiesta di parco istanze EC2 del tipo `maintain` o `request` rimane attiva fino a quando non scade o fino a quando non viene eliminata. Quando si elimina un parco istanze di tipo `maintain`

o `request`, è possibile specificare se l'eliminazione termina le istanze del parco istanze. In caso contrario, le istanze on demand rimangono in esecuzione finché non vengono terminate e le istanze spot rimangono in esecuzione finché non vengono interrotte o terminate.

Indice

Stati della richiesta parco istanze EC2

Una richiesta parco istanze EC2 può avere uno dei seguenti stati:

`submitted`

La richiesta parco istanze EC2 è in fase di valutazione ed Amazon EC2 si sta preparando ad avviare il numero previsto di istanze. La richiesta può includere Istanze on demand, Istanze spot o entrambe. Se una richiesta supera il limite del parco istanze, viene eliminata immediatamente.

`active`

La richiesta parco istanze EC2 è stata convalidata ed Amazon EC2 sta tentando di mantenere il numero previsto di istanze in esecuzione. La richiesta rimane in questo stato finché non viene modificata o eliminata.

`modifying`

La richiesta parco istanze EC2 è in fase di modifica. La richiesta rimane in questo stato finché la modifica non viene completamente elaborata o la richiesta non viene eliminata. È possibile modificare solo un tipo di parco istanze `maintain`. Questo stato non si applica ad altri tipi di richieste.

`deleted_running`

La richiesta parco istanze EC2 viene eliminata e non avvia istanze aggiuntive. Le sue istanze esistenti continuano a essere eseguite finché non vengono interrotte o terminate manualmente. La richiesta rimane in questo stato finché tutte le istanze non vengono interrotte o terminate. Solo un parco istanze EC2 del tipo `maintain` o `request` può avere istanze in esecuzione dopo l'eliminazione della richiesta del parco istanze EC2. Un parco istanze `instant` eliminato con istanze in esecuzione non è supportato. Questo stato non si applica ai parchi istanze `instant`.

`deleted_terminating`

La richiesta del parco istanze EC2 viene eliminata e le sue istanze vengono terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono terminate.

`deleted`

Il parco istanze EC2 viene eliminato e non dispone di istanze in esecuzione. La richiesta viene eliminata due giorni dopo e le sue istanze vengono terminate.

Prerequisiti di parco istanze EC2

Per creare un parco istanze EC2, devono esserci i prerequisiti seguenti:

- Modello di lancio
- Ruolo collegato al servizio per parco istanze EC2
- Concessione dell'accesso alle chiavi gestite dal cliente per l'uso con le AMI crittografate e gli snapshot EBS
- Autorizzazioni del parco istanze EC2 per gli utenti

Modello di lancio

Un modello di avvio include le informazioni riguardo alle istanze da avviare, come il tipo di istanza, la zona di disponibilità e il prezzo massimo che si è disposti a pagare. Per ulteriori informazioni, consulta Avvio di un'istanza da un modello di avvio.

Ruolo collegato al servizio per parco istanze EC2

Il ruolo `AWSServiceRoleForEC2Fleet` concede al parco istanze EC2 l'autorizzazione per richiedere, avviare e terminare le istanze, e applicarvi tag per tuo conto. Amazon EC2 utilizza questo ruolo collegato ai servizi per completare le operazioni seguenti:

- `ec2:RunInstances` – Avviare istanze.
- `ec2:RequestSpotInstances` – Richiesta Istanze spot.
- `ec2:TerminateInstances` – Terminare istanze
- `ec2:DescribeImages` – Descrizione di Amazon Machine Image (AMI) per le Istanze spot.
- `ec2:DescribeInstanceStatus` – Descrizione dello stato delle Istanze spot.
- `ec2:DescribeSubnets` – Descrizione di sottoreti per le Istanze spot.
- `ec2:CreateTags` – Aggiungere tag a parco istanze EC2, istanze e volumi.

Assicurati che questo ruolo esista prima di utilizzare AWS CLI o un'API per creare una flotta EC2.

> **Note**
>
> Un parco istanze EC2 `instant` non richiede questo ruolo.

Per creare il ruolo, utilizzare la console IAM nel modo seguente.

Per creare il AWSServiceRoleForEC2Fleet ruolo per EC2 Fleet

1. Apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.
3. Nella pagina Seleziona il tipo di entità affidabile, procedi come segue:
   a. Per Tipo di entità attendibile, scegli Servizio AWS .
   b. In Caso d'uso, per Servizio o caso d'uso, scegli EC2 - Fleet.

      > **Tip**
      >
      > Assicurati di scegliere EC2 - Fleet. Se scegli EC2, il caso d'uso EC2 - Fleet non viene visualizzato nell'elenco dei casi d'uso. Lo use case EC2 - Fleet creerà automaticamente una policy con le autorizzazioni IAM richieste e la suggerirà AWSServiceRoleForEC2Fleetcome nome del ruolo.

   c. Scegli Next (Successivo).
4. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).

5. Nella pagina Nomina, rivedi e crea scegli Crea ruolo.

Se non hai più bisogno di usare EC2 Fleet, ti consigliamo di eliminare il ruolo. AWSServiceRoleForEC2Fleet Dopo che questo ruolo è stato eliminato dal proprio account, è possibile creare di nuovo il ruolo se si crea un altro parco istanze.

Per ulteriori informazioni, consulta Utilizzo di ruoli collegati a servizi nella Guida per l'utente di IAM .

Concessione dell'accesso alle chiavi gestite dal cliente per l'uso con le AMI crittografate e gli snapshot EBS

Se specifichi un'AMI crittografata o uno snapshot Amazon EBS crittografato nella tua flotta EC2 e utilizzi una AWS KMS chiave per la crittografia, devi concedere al AWSServiceRoleForEC2Fleetruolo l'autorizzazione a utilizzare la chiave gestita dal cliente in modo che Amazon EC2 possa avviare istanze per tuo conto. Per farlo, occorre aggiungere una concessione alla chiave gestita dal cliente, come mostrato nella procedura seguente.

Nel processo di assegnazione delle autorizzazioni, le concessioni rappresentano un'alternativa alle policy delle chiavi. Per ulteriori informazioni, consulta Utilizzo delle concessioni e Utilizzo delle policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

Per concedere al AWSServiceRoleForEC2Fleet ruolo le autorizzazioni all'uso della chiave gestita dal cliente

- Utilizza il comando create-grant per aggiungere una concessione alla chiave gestita dal cliente e per specificare il principale (il ruolo AWSServiceRoleForEC2Fleetcollegato al servizio) a cui è concessa l'autorizzazione per eseguire le operazioni consentite dalla concessione. La chiave gestita dal cliente è specificata dal parametro `key-id` e dall'ARN della chiave gestita dal cliente. Il principale è specificato dal `grantee-principal` parametro e dall'ARN del ruolo collegato al AWSServiceRoleForEC2Fleetservizio.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Autorizzazioni del parco istanze EC2 per gli utenti

Se gli utenti creano o gestiscono un parco istanze EC2, assicurati di concedere loro le autorizzazioni richieste.

Per creare una policy per il parco istanze EC2

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), selezionare la scheda JSON, sostituire il testo con il seguente, quindi selezionare Review policy (Rivedi policy).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
        }
    ]
}
```

`ec2:*` concede a un utente l'autorizzazione per chiamare tutte le operazioni API Amazon EC2. Per limitare l'utente a specifiche operazioni API Amazon EC2, è necessario invece indicare tali azioni.

L'utente deve avere l'autorizzazione per chiamare l'operazione `iam:ListRoles` per enumerare i ruoli IAM esistenti, l'operazione `iam:PassRole` per specificare il ruolo del parco istanze EC2 e l'operazione `iam:ListInstanceProfiles` per enumerare i profili dell'istanza esistenti.

(Facoltativo) Per consentire a un utente di creare ruoli o profili dell'istanza utilizzando la console IAM, devi inoltre aggiungere le operazioni seguenti alla policy:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

5. Nella pagina Review policy (Rivedi policy), immettere un nome policy e una descrizione, poi selezionare Create policy (Crea policy).
6. Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

   - Utenti e gruppi in: AWS IAM Identity Center

     Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

   - Utenti gestiti in IAM tramite un provider di identità:

     Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

   - Utenti IAM:
     - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
     - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Controlli dello stato parco istanze EC2

parco istanze EC2 controlla lo stato delle istanze nel parco istanze ogni due minuti. Lo stato di un'istanza è `healthy` o `unhealthy`.

parco istanze EC2 determina lo stato di un'istanza utilizzando i controlli dello stato forniti da Amazon EC2. Un'istanza viene determinata come `unhealthy` quando lo stato del controllo dello stato dell'istanza o del controllo dello stato del sistema è `impaired` per tre controlli dello stato di integrità consecutivi. Per ulteriori informazioni, consulta Verifiche dello stato delle istanze.

È possibile configurare il parco istanze per sostituire le Istanze spot non integre. Dopo l'impostazione di `ReplaceUnhealthyInstances` su `true`, l'istanza spot viene sostituita quando viene segnalata come `unhealthy`. Durante la sostituzione di un'istanza spot non integra, il parco istanze può scendere al di sotto della sua capacità obiettivo.

Requisiti

- La sostituzione del controllo dello stato è supportata solo per Parchi istanze EC2 che mantengono una capacità target (parchi istanza del tipo `maintain`) e non con parchi istanza del tipo `request` o `instant`.
- La sostituzione del controllo dello stato è supportata solo per Istanze spot. Questa funzionalità non è supportata per Istanze on demand.
- È possibile configurare EC2 Fleet per sostituire le istanze non integre solo al momento della sua creazione.
- Gli utenti possono utilizzare la sostituzione del controllo dell'integrità solo se hanno l'autorizzazione a chiamare l'operazione `ec2:DescribeInstanceStatus`.

Per configurare un parco istanze EC2 per sostituire un Istanze spot non integro

1. Per creare un parco istanze EC2, procedi come indicato di seguito. Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.
2. Per configurare il parco istanze per sostituire un Istanze spot non integro, nel file JSON, per `ReplaceUnhealthyInstances` immettere `true`.

Generazione di un file di configurazione parco istanze EC2 JSON

Per visualizzare l'elenco completo dei parametri di configurazione del parco istanze EC2, è possibile generare un file JSON. Per una descrizione di ciascun parametro, consultare create-fleet nella Guida di riferimento ai comandi della AWS CLI .

Generare un file JSON con tutti i parametri parco istanze EC2 possibile utilizzando la riga di comando

- Utilizzare il comando create-fleet (AWS CLI) e il parametro `--generate-cli-skeleton` per generare un file JSON del parco istanze EC2 e indirizzare l'output in un file per salvarlo.

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

Output di esempio

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
```

```
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
                        "Tenancy": "dedicated",
                        "SpreadDomain": "",
                        "HostResourceGroupArn": ""
                    },
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "MemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        },
                        "CpuManufacturers": [
                            "amd"
                        ],
                        "MemoryGiBPerVCpu": {
                            "Min": 0.0,
                            "Max": 0.0
                        },
                        "ExcludedInstanceTypes": [
```

```
                    ""
                ],
                "InstanceGenerations": [
                    "previous"
                ],
                "SpotMaxPricePercentageOverLowestPrice": 0,
                "OnDemandMaxPricePercentageOverLowestPrice": 0,
                "BareMetal": "included",
                "BurstablePerformance": "required",
                "RequireHibernateSupport": true,
                "NetworkInterfaceCount": {
                    "Min": 0,
                    "Max": 0
                },
                "LocalStorage": "excluded",
                "LocalStorageTypes": [
                    "ssd"
                ],
                "TotalLocalStorageGB": {
                    "Min": 0.0,
                    "Max": 0.0
                },
                "BaselineEbsBandwidthMbps": {
                    "Min": 0,
                    "Max": 0
                },
                "AcceleratorTypes": [
                    "inference"
                ],
                "AcceleratorCount": {
                    "Min": 0,
                    "Max": 0
                },
                "AcceleratorManufacturers": [
                    "amd"
                ],
                "AcceleratorNames": [
                    "a100"
                ],
                "AcceleratorTotalMemoryMiB": {
                    "Min": 0,
                    "Max": 0
                }
            }
```

```
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 0,
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 0,
        "DefaultTargetCapacityType": "on-demand",
        "TargetCapacityUnitType": "memory-mib"
    },
    "TerminateInstancesWithExpiration": true,
    "Type": "instant",
    "ValidFrom": "1970-01-01T00:00:00",
    "ValidUntil": "1970-01-01T00:00:00",
    "ReplaceUnhealthyInstances": true,
    "TagSpecifications": [
        {
            "ResourceType": "fleet",
            "Tags": [
                {
                    "Key": "",
                    "Value": ""
                }
            ]
        }
    ],
    "Context": ""
}
```

Creazione di un parco istanze EC2

Per creare un parco istanze EC2, è necessario specificare solo i seguenti parametri:

- `LaunchTemplateId` o `LaunchTemplateName`: specifica il modello di avvio da utilizzare (che contiene i parametri per l'avvio delle istanze, come il tipo di istanza, la zona di disponibilità e il prezzo massimo che si è disposti a pagare)
- `TotalTargetCapacity`: specifica la capacità di destinazione totale per il parco istanze
- `DefaultTargetCapacityType`: specifica se l'opzione di acquisto di default è On demand o Spot

È possibile specificare più specifiche di avvio che sostituiscono il modello di avvio. Le specifiche di avvio possono variare a seconda del tipo di istanza, della zona di disponibilità, della sottorete e del prezzo massimo e possono includere una capacità ponderata diversa. In alternativa, è possibile specificare gli attributi che un'istanza deve avere e Amazon EC2 identificherà tutti i tipi di istanza con tali attributi. Per ulteriori informazioni, consulta Selezione del tipo di istanza basata su attributi per il parco istanze EC2.

Se non viene specificato un parametro, il parco istanze utilizzerà il valore di default.

Specificare i parametri del parco istanze in un file JSON. Per ulteriori informazioni, consulta Generazione di un file di configurazione parco istanze EC2 JSON.

Al momento non è disponibile il supporto per la console per la creazione di un parco istanze EC2.

Creazione di un parco istanze EC2 (AWS CLI)

- Utilizzare il comando create-fleet (AWS CLI) per creare un parco istanze EC2 e specifica il file JSON che contiene i parametri di configurazione del parco istanze.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Per i file di configurazione di esempio, consultare Configurazioni parco istanze EC2 di esempio.

Di seguito è riportato l'output di esempio per un parco istanze del tipo `request` o `maintain`.

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Di seguito è riportato l'output di esempio per un parco istanze del tipo `instant` che ha avviato la capacità target.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
```

```
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ]
  ]
}
```

Di seguito è riportato l'output di esempio per un parco istanze del tipo `instant` che ha avviato parte della capacità target con errori per le istanze che non erano state avviate.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
```

```
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ]
  ]
}
```

Di seguito è riportato l'output di esempio per un parco istanze del tipo `instant` che non ha avviato istanze.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
```

```
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": []
}
```

Tagging di un parco istanze EC2

Per categorizzare e gestire le richieste parco istanze EC2, è possibile contrassegnarle con tag contenenti metadati personalizzati. È possibile assegnare un tag a una richiesta parco istanze EC2 alla sua creazione o successivamente.

Quando si applica un tag a una richiesta del parco istanze, alle istanze e ai volumi che vengono avviati dal parco istanze non vengono automaticamente applicati tag. È necessario applicare esplicitamente tag alle istanze e ai volumi avviati dal parco istanze. È possibile scegliere di applicare tag solo alla richiesta del parco istanze o solo alle istanze avviate dal parco istanze oppure solo ai volumi collegati alle istanze avviate dal parco istanze o a tutti e tre.

> **Note**
>
> Per i tipi di parco istanze `instant`, è possibile applicare tag ai volumi collegati a Istanze on demand e Istanze spot. Per i tipi di parco istanze `request` o `maintain`, è possibile applicare tag ai volumi collegati a Istanze on demand.

Per ulteriori informazioni sul funzionamento dei tag, consultare Tagging delle risorse Amazon EC2..

Prerequisito

Concedi all'utente l'autorizzazione per taggare le risorse. Per ulteriori informazioni, consulta Esempio: aggiunta di tag alle risorse.

Per concedere a un utente l'autorizzazione per taggare le risorse

Creare una policy IAM che include quanto segue:

- L'operazione `ec2:CreateTags`. Ciò concede all'utente l'autorizzazione per creare tag.
- L'operazione `ec2:CreateFleet`. Ciò concede all'utente l'autorizzazione per creare una richiesta parco istanze EC2.
- Per `Resource`, si consiglia di specificare `"*"`. Ciò consente agli utenti di taggare tutti i tipi di risorse.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagEC2FleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:CreateFleet"
            ],
            "Resource": "*"
}
```

Important

Attualmente non sono supportate le autorizzazioni a livello di risorse per la risorsa `create-fleet`. Se si specifica `create-fleet` come risorsa, si otterrà un'eccezione non autorizzata quando si tenta di taggare il parco istanze. Nell'esempio seguente viene mostrato come non impostare la policy.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:CreateFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:create-fleet/*"
}
```

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Per applicare tag a una nuova richiesta parco istanze EC2

Per assegnare un tag a una richiesta parco istanze EC2 durante la sua creazione, specificare la coppia chiave-valore nel file JSON utilizzato per creare il parco istanze. Il valore di `ResourceType` deve essere `fleet`. Indicando un altro valore, la richiesta per il parco istanze fallisce.

Per applicare tag a istanze e volumi avviati da un parco istanze EC2

Per applicare tag alle istanze e ai volumi quando vengono avviate dal parco istanze, specificare i tag nel modello di lancio a cui fa riferimento la richiesta nel parco istanze EC2.

> **Note**
>
> Non è possibile applicare tag ai volumi collegati a Istanze spot che vengono avviati da un tipo di parco istanze `request` o `maintain`.

Per applicare tag a una richiesta di parco istanze EC2, un'istanza e un volume esistenti (AWS CLI)

Utilizzare il comando create-tags per aggiungere un tag alle risorse esistenti.

```
aws ec2 create-tags \
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

Descrivere il parco istanze EC2

Puoi descrivere la configurazione del tuo parco istanze EC2, le istanze nel tuo parco istanze EC2 e la cronologia degli eventi del tuo parco istanze EC2.

Per descrivere il tuo parco istanze EC2 (AWS CLI)

Utilizzare il comando describe-fleets per descrivere i Parchi istanze EC2.

```
aws ec2 describe-fleets
```

> **Important**
>
> Se un parco istanze è di tipo `instant`, devi specificare l'ID del parco istanze, altrimenti non viene visualizzato nella risposta. Includi `--fleet-ids` come riportato di seguito:

```
aws ec2 describe-fleets --fleet-ids fleet-8a22eee4-f489-ab02-06b8-832a7EXAMPLE
```

Output di esempio


```
{
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
```

```
}
```

Usa il describe-fleet-instancescomando per descrivere le istanze per il parco EC2 specificato. L'elenco delle istanze in esecuzione riportato viene aggiornato periodicamente e potrebbe essere obsoleto.

```
aws ec2 describe-fleet-instances  --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Output di esempio

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Usa il describe-fleet-historycomando per descrivere la cronologia del parco EC2 specificato per l'ora specificata.

```
aws ec2 describe-fleet-history --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE --
start-time 2018-04-10T00:00:00Z
```

Output di esempio

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
```

```
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2018-04-09T23:53:20.000Z"
}
```

Come modificare un parco istanze EC2

È possibile modificare un parco istanze EC2 che risulta nello stato `submitted` o `active`. Quando si modifica un parco istanze, esso acquisisce lo stato `modifying`.

È possibile modificare solo un parco istanze EC2 che sia di tipo `maintain`. Non è possibile modificare un parco istanze EC2 di tipo `request` o `instant`.

È possibile modificare i parametri seguenti di un parco istanze EC2:

- `target-capacity-specification` – Consente di aumentare o diminuire la capacità target di `TotalTargetCapacity`, `OnDemandTargetCapacity` e `SpotTargetCapacity`.
- `excess-capacity-termination-policy` – Indica se l'esecuzione delle istanze deve terminare quando la capacità target totale del parco istanze EC2 scende al di sotto della dimensione attuale del parco istanze. I valori validi sono `no-termination` e `termination`.

Quando si aumenta la capacità target, EC2 Fleet avvia le istanze aggiuntive in base all'opzione di acquisto delle istanze indicato da `DefaultTargetCapacityType`, che può essere Istanze on demand o Istanze spot.

In caso `DefaultTargetCapacityType` affermativo`spot`, il parco istanze EC2 avvia le istanze Spot aggiuntive in base alla propria strategia di allocazione.

Quando si diminuisce la capacità di destinazione, EC2 Fleet elimina qualsiasi richiesta aperta che supera la nuova capacità di destinazione. È possibile richiedere che il parco istanze termini le istanze finché la dimensione del parco istanze non raggiunge la nuova capacità di destinazione. Se la strategia di allocazione è `lowest-price`, il parco istanze termina le istanze con il prezzo più alto per unità. Se la strategia di allocazione è `diversified`, il parco istanze termina le istanze tra i pool. In alternativa, è possibile richiedere che EC2 Fleet mantenga il parco istanze alla sua dimensione attuale, ma che non sostituisca le Istanze spot che vengono interrotte o tutte le istanze che vengono terminate manualmente.

Quando un parco istanze EC2 termina un'istanza spot a seguito della diminuzione della capacità obiettivo, l'istanza riceve un avviso di interruzione dell'istanza spot.

Per modificare un parco istanze EC2 (AWS CLI)

Utilizzare il comando modify-fleet per aggiornare la capacità target del parco istanze EC2 specificato.

```
aws ec2 modify-fleet \
```

```
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

Se si diminuisce la capacità target, ma si desidera mantenere il parco istanze alla dimensione attuale, è possibile modificare il comando precedente come segue.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

Eliminazione di un parco istanze EC2

Se un parco istanze EC2 non è più necessario, è possibile eliminarlo. Dopo aver eliminato un parco istanze, tutte le richieste Spot associate al parco istanze vengono eliminate, in modo che nessuna istanza spot nuova venga avviata per tale parco.

Quando si elimina un parco istanze EC2, è necessario specificare se si desidera terminare tutte le relative istanze. Ciò include sia le istanze on demand che le istanze spot. Per le `instant` flotte, EC2 Fleet deve chiudere le istanze quando la flotta viene eliminata. Un parco istanze `instant` eliminato con istanze in esecuzione non è supportato.

Se specifichi che le istanze devono essere terminate quando elimini il parco istanze, quest'ultimo acquisisce lo stato `deleted_terminating`. Altrimenti, esso acquisisce lo stato `deleted_running` e l'esecuzione delle istanze continua finché esse non vengono interrotte o terminate manualmente.

Restrizioni

- Puoi eliminare fino a 25 flotte di tipi `instant` in un'unica richiesta.
- Puoi eliminare fino a 100 flotte di tipo `maintain` o `request` in una singola richiesta.
- Puoi eliminare fino a 125 flotte in una singola richiesta, a condizione che non superi la quota per ogni tipo di flotta, come specificato sopra.
- Se superi il numero specificato di flotte da eliminare, non viene eliminata alcuna flotta.
- È possibile terminare fino a 1.000 istanze in una singola richiesta di eliminazione di parchi istanze `instant`.

Per eliminare un parco istanze EC2 e terminare le relative istanze (AWS CLI)

Utilizza il comando delete-fleets e il parametro `--terminate-instances` per eliminare EC2 Fleet specificato e terminare le istanze associate.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Output di esempio

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

Per eliminare un parco istanze EC2 senza terminare le relative istanze (AWS CLI)

È possibile modificare il comando precedente utilizzando il parametro `--no-terminate-instances` per eliminare EC2 Fleet specificato senza terminare le istanze associate.

> **Note**
>
> `--no-terminate-instances` non è supportato per i parchi istanze `instant`.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Output di esempio

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
```

```
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

Risoluzione dei problemi di eliminazione di un parco istanze

Se un parco istanze EC2 non viene eliminato, `UnsuccessfulFleetDeletions` nell'output restituisce l'ID del parco istanze EC2, un codice di errore e un messaggio di errore.

I codici di errore sono:

- `ExceededInstantFleetNumForDeletion`
- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`
- `unexpectedError`

Risoluzione dei problemi relativi a **`ExceededInstantFleetNumForDeletion`**

Se si tenta di eliminare più di 25 parchi istanze `instant` in una singola richiesta, viene restituito l'errore `ExceededInstantFleetNumForDeletion`. Di seguito è riportato l'output di esempio per questo errore.

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
          "Error": {
                  "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                  "Code": "ExceededInstantFleetNumForDeletion"
           }
     },
     {
```

```
            "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
            "Error": {
                  "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                  "Code": "ExceededInstantFleetNumForDeletion"
             }
     }
     .
     .
     .
     ],
     "SuccessfulFleetDeletions": []
}
```

Risoluzione dei problemi di **`NoTerminateInstancesNotSupported`**

Se si specifica che le istanze di un parco istanze `instant` non devono essere terminate quando si elimina il parco istanze, viene restituito l'errore `NoTerminateInstancesNotSupported`. `--no-terminate-instances` non è supportato per i parchi istanze `instant`. Di seguito è riportato l'output di esempio per questo errore.

```
{
      "UnsuccessfulFleetDeletions": [
            {
                  "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                  "Error": {
                        "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                        "Code": "NoTerminateInstancesNotSupported"
                   }
            }
       ],
       "SuccessfulFleetDeletions": []
```

Risoluzione dei problemi di **`UnauthorizedOperation`**

Se non si dispone dell'autorizzazione per terminare le istanze, viene restituito l'errore `UnauthorizedOperation` quando si elimina un parco istanze che deve terminare le relative istanze. Di seguito è riportata la risposta di errore.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
 authorized to perform this
```

```
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>
```

Per risolvere l'errore, è necessario aggiungere l'operazione `ec2:TerminateInstances` alla policy IAM, come illustrato nell'esempio seguente.

```
{
       "Version": "2012-10-17",
       "Statement": [
            {
                "Sid": "DeleteFleetsAndTerminateInstances",
                "Effect": "Allow",
                "Action": [
                       "ec2:DeleteFleets"
                       "ec2:TerminateInstances"
                ],
                "Resource": "*"
            }
       ]
   }
```

parco istanze spot

Un parco istanze Spot è una serie di istanze Spot ed eventualmente di istanze on demand che viene avviata in base ai criteri da te specificati. Il parco istanze spot seleziona i pool di capacità spot che soddisfano le tue esigenze e avvia le istanze spot per soddisfare la capacità obiettivo per il parco istanze. Per impostazione predefinita, il Parchi istanze spot è impostato per mantenere la capacità target attraverso l'avvio di istanze sostitutive dopo che le Istanze spot nel parco istanze sono terminate. È possibile inviare un parco istanze spot come richiesta una tantum, che non persiste dopo che le istanze sono terminate. È possibile includere richieste di istanza on demand in una richiesta ddel parco istanze spot.

> **Note**
>
> Se desideri utilizzare una console per creare un parco istanze che includa istanze spot, consigliamo di utilizzare un gruppo con scalabilità automatica piuttosto che una serie di istanze spot. Per ulteriori informazioni, consultare la sezione relativa ai Gruppi con dimensionamento automatico con più tipi di istanze e opzioni di acquisto nella Guida per l'utente di Dimensionamento automatico Amazon EC2.
> Se desideri utilizzare il per AWS CLI creare una flotta che includa istanze Spot, ti consigliamo di utilizzare un gruppo di Auto Scaling o un parco veicoli EC2 anziché Spot Fleet. L'RequestSpotFleetAPI, su cui si basa Spot Fleet, è un'API legacy senza investimenti pianificati.
> Per ulteriori informazioni sulle API consigliate da utilizzare, consulta Qual è il metodo di richiesta Spot migliore da utilizzare?

Argomenti

Tipi di richiesta del parco istanze spot

Esistono due tipi di richieste del parco istanze spot:

`request`

Se configuri il tipo di richiesta come `request`, il parco istanze spot inserisce una richiesta una tantum asincrona per la capacità desiderata. Successivamente, se la capacità è diminuita a causa delle interruzioni di Spot, il parco istanze non tenta di rifornire Istanze spot e non invia nemmeno richieste in pool di capacità spot alternativi se la capacità non è disponibile.

`maintain`

Se configuri il tipo di richiesta come `maintain`, il parco istanze spot effettua una richiesta asincrona per la capacità desiderata e mantiene la capacità rifornendo automaticamente le Istanze spot interrotte.

Per specificare il tipo di richiesta nella console Amazon EC2, durante la creazione di una richiesta di un parco istanze spot, effettua le seguenti operazioni:

- Per creare un parco istanze spot di tipo `request`, deseleziona la casella di controllo Maintain target capacity (Mantieni capacità obiettivo).
- Per creare un parco istanze spot di tipo `maintain`, seleziona la casella di controllo Maintain target capacity (Mantieni capacità obiettivo).

Per ulteriori informazioni, consulta Creare una richiesta di parco istanze spot utilizzando parametri definiti (console).

Entrambi i tipi di richiesta traggono vantaggio dalla strategia di allocazione. Per ulteriori informazioni, consulta Strategie di allocazione per istanze spot.

Strategie di configurazione del parco istanze spot

Un parco istanze spot è una serie, o parco, di istanze spot ed eventualmente di istanze on demand.

Il parco istanze spot tenta di avviare il numero di istanze spot e istanze on demand per soddisfare la capacità obiettivo specificata nella richiesta del parco istanze spot. La richiesta di Istanze spot viene soddisfatta se è disponibile capacità sufficiente e il prezzo massimo specificato nella richiesta supera il prezzo Spot attuale. Il parco istanze spot tenta inoltre di mantenere la propria capacità obiettivo se le Istanze spot vengono interrotte.

Puoi inoltre impostare un importo massimo all'ora che sei disposto a pagare per il parco istanze: il parco istanze spot avvierà le istanze finché non raggiunge tale importo. A questo punto, il parco istanze interrompe l'avvio delle istanze, anche se non è stata raggiunta la capacità target.

Un pool di capacità spot è un insieme di istanze EC2 inutilizzate con lo stesso tipo di istanza (ad esempio, `m5.large`), lo stesso sistema operativo, la stessa zona di disponibilità e la stessa piattaforma di rete. Quando si effettua una richiesta di parco istanze spot, è possibile includere più specifiche di avvio, che variano a seconda del tipo di istanza, dell'AMI, della zona di disponibilità o della sottorete. Il parco istanze spot seleziona i pool di capacità spot utilizzati per soddisfare la richiesta in base alle specifiche di avvio incluse nella richiesta del parco istanze spot e alla configurazione della richiesta del parco istanze spot. Le Istanze spot provengono dai pool selezionati.

Indice

Pianificare una richiesta di parco istanze spot

Prima di creare una richiesta di parco istanze spot, rivedi le Best practice Spot. Quando si programmano le richieste di parco istanze spot, utilizzare queste best practice in modo da assegnare il tipo di istanza desiderato al prezzo più basso possibile. Consigliamo anche di fare quanto segue:

- Stabilire se si desidera creare un parco istanze spot che invii una richiesta una tantum per la capacità obiettivo desiderata o che mantenga una capacità obiettivo nel tempo.
- Indicare il tipo di istanza che soddisfa i propri requisiti in termini di applicazioni.
- Stabilire la capacità obiettivo per la richiesta del parco istanze spot. È possibile impostare la capacità target in istanze o in unità personalizzate. Per ulteriori informazioni, consulta Ponderazione delle istanze del parco istanze spot.
- Stabilire quale porzione della capacità obiettivo del parco istanze spot deve essere una capacità on demand. È possibile specificare 0 come capacità on-demand.
- Se si utilizza la ponderazione d'istanza, stabilire il prezzo per unità. Per calcolare il prezzo per unità, dividere il prezzo all'ora per istanza per il numero di unità (o peso) che tale istanza

rappresenta. Se non si utilizza la ponderazione d'istanza, il prezzo predefinito per unità è il prezzo all'ora per istanza.

- Rivedere le possibili opzioni per la propria richiesta di parco istanze spot. Per ulteriori informazioni, consulta il request-spot-fleetcomando nel AWS CLI Command Reference. Per ulteriori esempi, consulta Configurazioni del parco istanze spot di esempio.

Strategie di allocazione per istanze spot

La configurazione di avvio determina tutti i possibili pool di capacità spot (tipi di istanze e zone di disponibilità) da cui la serie di istanze Spot può avviare istanze spot. Tuttavia, al momento del lancio delle istanze, la serie di istanze spot utilizza la strategia di allocazione specificata per scegliere i pool specifici da tutti i pool possibili.

> **Note**
>
> (Solo istanze Linux) Se configuri l'istanza Spot per l'avvio con AMD SEV-SNP attivato, ti verrà addebitata una tariffa di utilizzo oraria aggiuntiva equivalente al 10% della tariffa oraria On-Demand per il tipo di istanza selezionato. Se la strategia di allocazione utilizza il prezzo come input, il parco istanze EC2 non include questa tariffa aggiuntiva; viene utilizzato solo il prezzo spot.

Strategie di allocazione

Puoi specificare una delle seguenti strategie di allocazione per le istanze spot:

`priceCapacityOptimized`(consigliato)

Il parco istanze spot identifica i pool con la massima capacità disponibile per il numero di istanze che vengono avviate. Ciò implica che richiederemo istanze spot dai pool che riteniamo avere le minori possibilità di interruzione nel breve termine. Dopodiché, il parco istanze spot chiede istanze spot dal pool con il prezzo più basso tra questi pool.

La strategia di allocazione `priceCapacityOptimized` è la scelta migliore per la maggior parte dei carichi di lavoro spot, come applicazioni containerizzate stateless, microservizi, applicazioni Web, processi di dati e analisi ed elaborazione in batch.

`capacityOptimized`

Il parco istanze spot identifica i pool con la massima capacità disponibile per il numero di istanze che vengono avviate. Ciò implica che richiederemo istanze spot dai pool che riteniamo avere le minori possibilità di interruzione nel breve termine. Facoltativamente, puoi impostare una priorità per ogni tipo di istanza del parco istanze utilizzando `capacityOptimizedPrioritized`. Il parco istanze spot ottimizzerà innanzitutto la capacità, ma rispetterà le priorità del tipo di istanza sulla base del miglior tentativo.

Con Istanze spot, i prezzi cambiano lentamente nel tempo in base ai trend a lungo termine dell'offerta e della domanda, ma la capacità fluttua in tempo reale. La strategia `capacityOptimized` avvia automaticamente Istanze spot nei pool più disponibili esaminando i dati di capacità in tempo reale e prevedendo quali sono le più disponibili. Questa strategia è ideale per carichi di lavoro che possono avere un costo più elevato di interruzione associato al riavvio del lavoro, ad esempio carichi di lavoro di integrazione continua (CI), rendering di immagini e media, deep learning e calcolo ad alte prestazioni (HPC), che possono avere un costo più elevato di interruzione associato al riavvio del lavoro. Offrendo la possibilità di ridurre il numero di interruzioni, la strategia `capacityOptimized` può ridurre il costo complessivo del carico di lavoro.

In alternativa, puoi utilizzare la strategia di allocazione di `capacityOptimizedPrioritized` con un parametro di priorità e quindi impostare l'ordine dei tipi di istanza dalla priorità più alta alla più bassa. Puoi impostare la stessa priorità per diversi tipi di istanza. Il parco istanze spot ottimizzerà innanzitutto la capacità, ma rispetterà le priorità del tipo di istanza sulla base del miglior tentativo (ad esempio, se il rispetto delle priorità non influirà in modo significativo sulla capacità del parco istanze spot di fornire capacità ottimale). Questa è una buona opzione per i carichi di lavoro in cui è necessario ridurre al minimo la possibilità di interruzioni e la preferenza per determinati tipi di istanza è importante. L'utilizzo delle priorità è supportato solo se la flotta utilizza un modello di avvio. Tieni presente che quando imposti la priorità per `capacityOptimizedPrioritized`, la stessa priorità viene applicata anche alle istanze on demand se la `AllocationStrategy` on demand è impostata su `prioritized`.

`diversified`

Le Istanze spot sono distribuite in tutti i pool.

Scegliere una strategia di allocazione adeguata

Puoi ottimizzare il tuo parco istanze in base al tuo caso d'uso scegliendo la strategia di allocazione spot appropriata. Per quanto riguarda la capacità target delle istanze On-Demand, Spot Fleet seleziona sempre il tipo di istanza meno costoso in base al prezzo pubblico on demand, seguendo al contempo la strategia di allocazione (o, o) per le istanze `priceCapacityOptimized` Spot. `capacityOptimized` `diversified`

Equilibrio tra prezzo più basso e capacità disponibile

Per bilanciare i compromessi tra i pool di capacità spot con il prezzo più basso e i pool di capacità spot con la massima capacità disponibile, ti consigliamo di utilizzare la strategia di allocazione `priceCapacityOptimized`. Questa strategia decide a quali pool richiedere le istanze spot tenendo conto sia del prezzo dei pool sia della capacità di istanze spot disponibile in tali pool. Ciò implica che richiederemo istanze spot dai pool che riteniamo avere le minori possibilità di interruzione nel breve termine, tenendo comunque conto del prezzo.

Se il tuo parco istanze esegue carichi di lavoro resilienti e stateless, tra cui applicazioni containerizzate, microservizi, applicazioni Web, processi di dati e analisi ed elaborazione in batch, utilizza la strategia di allocazione `priceCapacityOptimized` per risparmiare sui costi e disporre di una capacità ottimale.

Se il parco istanze esegue carichi di lavoro che possono avere un costo più elevato di interruzione associato al riavvio del lavoro, ti consigliamo implementare i checkpoint affinché le applicazioni possano riavviarsi da quel punto in caso di interruzione. Utilizzando i checkpoint, la strategia di allocazione `priceCapacityOptimized` è una buona scelta per questi carichi di lavoro perché alloca la capacità dai pool con il prezzo più basso che offrono anche una bassa frequenza di interruzione delle istanze spot.

Per una configurazione di esempio che utilizza la strategia di allocazione `priceCapacityOptimized`, consulta la pagina Esempio 9: avvia le istanze Spot in un parco istanze con priorità ottimizzate in termini di capacità.

Quando i carichi di lavoro hanno un costo di interruzione elevato

Facoltativamente, è possibile utilizzare la strategia `capacityOptimized` se si eseguono carichi di lavoro che utilizzano tipi di istanze con prezzi simili o in cui il costo dell'interruzione è così significativo che qualsiasi risparmio sui costi è inadeguato rispetto a un aumento marginale delle interruzioni. Questa strategia alloca la capacità dai pool di capacità spot con maggiore disponibilità che offrono una possibilità minore di interruzioni, il che può ridurre il costo complessivo del carico di lavoro.

Per una configurazione di esempio che utilizza la strategia di allocazione `capacityOptimized`, consulta la pagina Esempio 7: configura il ribilanciamento della capacità per avviare istanze Spot sostitutive.

Quando è necessario ridurre al minimo la possibilità di interruzione ma la preferenza per determinati tipi di istanza è importante, puoi esprimere le priorità dei pool utilizzando la strategia di allocazione `capacityOptimizedPrioritized` e quindi impostare l'ordine dei tipi di istanza da utilizzare dalla priorità più alta alla più bassa. Per un esempio di configurazione, consulta Esempio 8: avvio di istanze Spot in un parco istanze ottimizzato in termini di capacità.

L'utilizzo delle priorità è supportato solo se il parco istanze utilizza un modello di avvio. Inoltre, tieni presente che quando imposti le priorità per `capacityOptimizedPrioritized`, le stesse priorità vengono applicate anche alle istanze on demand se la `AllocationStrategy` on demand è impostata su `prioritized`.

Quando il carico di lavoro è flessibile in termini di tempo e la capacità disponibile non è un fattore rilevante

Se il parco istanze è piccolo o viene eseguito per un breve periodo di tempo, puoi utilizzare `priceCapacityOptimized` per massimizzare i risparmi sui costi pur tenendo conto della capacità disponibile.

Quando il parco istanze è grande o viene eseguito per un lungo periodo di tempo

Se il parco istanze è grande o funziona per un lungo periodo di tempo, puoi aumentare la disponibilità del parco istanze distribuendo la Istanze spot tra più pool utilizzando la strategia `diversified`. Ad esempio, se il parco istanze spot specifica 10 pool e una capacità obiettivo pari a 100 istanze, il parco istanze avvia 10 istanze spot in ogni pool. Se il prezzo Spot per un pool supera il prezzo massimo per tale pool, solo il 10% del parco istanze ne è interessato. L'utilizzo di questa strategia rende inoltre il parco istanze meno sensibile agli aumenti del prezzo Spot in ogni pool unico nel tempo. Con la strategia `diversified`, il parco istanze spot non avvia le istanze spot nei pool con un prezzo Spot uguale o maggiore del prezzo on demand.

Mantenere la capacità target

Dopo che le istanze spot vengono terminate a causa di una modifica del prezzo Spot o della capacità disponibile di un pool di capacità spot, una serie di istanze spot di tipo `maintain` avvia istanze spot sostitutive. La strategia di allocazione determina i pool da cui vengono avviate le istanze sostitutive, come segue:

- Se la strategia di allocazione è `priceCapacityOptimized`, il parco istanze avvia le istanze sostitutive nei pool che hanno la massima capacità disponibile di istanze spot tenendo in considerazione e identificando anche i pool con il prezzo più basso con una capacità disponibile elevata.
- Se la strategia di allocazione è `capacityOptimized`, il parco istanze avvia le istanze sostitutive nei pool che hanno la massima capacità disponibile di istanze spot.
- Se la strategia di allocazione è `diversified`, il parco istanze distribuisce le Istanze spot sostitutive nei pool rimanenti.

Selezione del tipo di istanza basata su attributi per serie di istanze spot

Quando si crea una serie di istanze spot, è necessario specificare uno o più tipi di istanza per la configurazione delle istanze on-demand e delle istanze spot nel parco istanze. In alternativa alla specifica manuale dei tipi di istanza, è possibile specificare gli attributi che un'istanza deve avere e Amazon EC2 identificherà tutti i tipi di istanza con tali attributi. Questo è noto come selezione del tipo di istanza basata su attributi. Ad esempio, puoi specificare il numero minimo e massimo di vCPU richieste per le istanze e la serie di istanze spot avvierà le istanze utilizzando qualsiasi tipo di istanza disponibile che soddisfi i requisiti di tali vCPU.

La selezione del tipo di istanza basata su attributi è ideale per carichi di lavoro e framework che possono essere flessibili sui tipi di istanza utilizzati, ad esempio quando si eseguono container o parchi istanze Web, elaborazione di Big Data e implementazione di strumenti CI/CD (Continuous Integration and Deployment).

Vantaggi

La selezione del tipo di istanza basata su attributi comporta i seguenti vantaggi:

- Usa facilmente i tipi di istanza giusti: con così tanti tipi di istanze disponibili, trovare i tipi di istanza giusti per il tuo carico di lavoro può richiedere molto tempo. Quando si specificano gli attributi dell'istanza, i tipi di istanza avranno automaticamente gli attributi richiesti per il carico di lavoro.
- Configurazione semplificata: per specificare manualmente più tipi di istanze per un parco istanze Spot, devi creare un override del modello di lancio separato per ogni tipo di istanza. Tuttavia, con la selezione del tipo di istanza basata su attributi, per fornire più tipi di istanza è necessario specificare solo gli attributi dell'istanza nel modello di avvio o in una sostituzione di un modello di avvio.

- Uso automatico di nuovi tipi di istanze: quando si specificano gli attributi delle istanze anziché i tipi di istanze, il parco istanze può utilizzare tipi di istanze di nuova generazione non appena vengono rilasciati, «a prova di futuro» della configurazione del parco istanze.
- Flessibilità del tipo di istanza: quando si specificano gli attributi dell'istanza anziché i tipi di istanza, Spot Fleet può scegliere tra un'ampia gamma di tipi di istanze per il lancio delle istanze Spot, in linea con le migliori pratiche Spot in materia di flessibilità dei tipi di istanze.

Argomenti

Come funziona la selezione del tipo di istanza basata su attributi

Per utilizzare la selezione del tipo di istanza basata su attributi nella configurazione del parco istanze, è necessario sostituire l'elenco dei tipi di istanza con un elenco di attributi di istanza richiesti dalle istanze. La serie di istanze spot avvierà le istanze su qualsiasi tipo di istanza disponibile con gli attributi di istanza specificati.

Argomenti

Tipi di attributi di istanza

Esistono diversi attributi di istanza che puoi specificare per esprimere i tuoi requisiti di calcolo, ad esempio:

- Numero di vCPU: il numero minimo e massimo di vCPU per istanza.
- Memoria: il numero minimo e massimo GiBs di memoria per istanza.

- Archiviazione locale: se utilizzare EBS o i volumi di Instance Store per l'archiviazione locale.
- Prestazioni affidabili: se utilizzare la famiglia di istanze T, inclusi i tipi T4g, T3a, T3 e T2.

Per una descrizione di ogni attributo e dei valori predefiniti, InstanceRequirementsconsulta Amazon EC2 API Reference.

Dove configurare la selezione del tipo di istanza basata su attributi

A seconda che utilizzi la console o la AWS CLI, puoi specificare gli attributi dell'istanza per la selezione del tipo di istanza basata sugli attributi come segue:

Nella console è possibile specificare gli attributi di istanza in uno o entrambi i seguenti componenti di configurazione del parco istanze:

- In un modello di avvio, facendo successivamente riferimento al modello di avvio nella richiesta del parco istanze
- Nella richiesta del parco istanze

In AWS CLI, è possibile specificare gli attributi dell'istanza in uno o tutti i seguenti componenti di configurazione della flotta:

- In un modello di avvio, facendo riferimento al modello di avvio nella richiesta del parco istanze
- In una sostituzione del modello di avvio

  Se si desidera un mix di istanze che utilizzano AMI diverse, è possibile specificare gli attributi di istanza in più sostituzioni di modelli di avvio. Ad esempio, diversi tipi di istanza possono utilizzare processori x86 e ARM.
- In una specifica di avvio

Come la serie di istanze spot utilizza la selezione del tipo di istanza basata su attributi durante il provisioning di un parco istanze

La serie di istanze spot fornisce un parco istanze nel seguente modo:

- La serie di istanze spot identifica i tipi di istanza che hanno gli attributi specificati.
- La serie di istanze spot utilizza la protezione dei prezzi per determinare quali tipi di istanza escludere.

- Spot Fleet determina i pool di capacità da cui prenderà in considerazione l'avvio delle istanze in base alle AWS regioni o alle zone di disponibilità con tipi di istanze corrispondenti.
- La serie di istanze spot applica la strategia di allocazione specificata per determinare da quali pool di capacità avviare le istanze.

  Notare che la selezione del tipo di istanza basata su attributi non sceglie i pool di capacità da cui effettuare il provisioning del parco istanze; questo è il compito delle strategie di allocazione. Potrebbe esserci un numero elevato di tipi di istanza con gli attributi specificati e alcuni di essi potrebbero essere costosi.

  Se si specifica una strategia di allocazione, la serie di istanze spot avvierà le istanze in base alla strategia di allocazione specificata.

  - Per le istanze spot, la selezione del tipo di istanza basata su attributi supporta le strategie di allocazione `capacityOptimizedPrioritized` e `capacityOptimized`.
  - Per le istanze On-Demand, la selezione del tipo di istanza basata sugli attributi supporta la strategia di `lowestPrice` allocazione, che garantisce che Spot Fleet lanci istanze On-Demand dai pool di capacità meno costosi.
- Se non è presente alcuna capacità per i tipi di istanza con gli attributi di istanza specificati, non è possibile avviare le istanze e il parco istanze restituisce un errore.

Protezione del prezzo

La protezione dei prezzi è una funzione che impedisce alla serie di istanze spot di utilizzare tipi di istanza troppo costosi anche se si adattano agli attributi specificati. Per utilizzare la protezione del prezzo, è necessario impostare una soglia di prezzo. Quindi, quando Amazon EC2 seleziona i tipi di istanza con i tuoi attributi, esclude i tipi di istanza con un prezzo superiore alla soglia.

Il modo in cui Amazon EC2 calcola la soglia di prezzo è il seguente:

- Amazon EC2 identifica innanzitutto il tipo di istanza con il prezzo più basso tra quelle che corrispondono ai tuoi attributi.
- Amazon EC2 prende quindi il valore (espresso in percentuale) specificato per il parametro di protezione del prezzo e lo moltiplica per il prezzo del tipo di istanza identificato. Il risultato è il prezzo utilizzato come soglia di prezzo.

Esistono soglie di prezzo separate per le istanze on demand e le istanze Spot.

Quando crei un parco istanze con selezione del tipo di istanza basata sugli attributi, la protezione del prezzo è abilitata per impostazione predefinita. Puoi mantenere i valori predefiniti oppure puoi specificarne uno personalizzato.

Puoi anche disattivare la protezione del prezzo. Per indicare l'assenza di una soglia di protezione del prezzo, specifica un valore percentuale elevato, ad esempio999999.

Argomenti

- Come viene identificato il tipo di istanza con il prezzo più basso
- Protezione del prezzo delle istanze On-Demand
- Protezione del prezzo delle istanze Spot
- Specificate la soglia di protezione del prezzo

Come viene identificato il tipo di istanza con il prezzo più basso

Amazon EC2 determina il prezzo su cui basare la soglia di prezzo identificando il tipo di istanza con il prezzo più basso tra quelle che corrispondono agli attributi specificati. Lo fa nel modo seguente:

- Innanzitutto esamina i tipi di istanza C, M o R dell'attuale generazione che corrispondono ai tuoi attributi. Se trova delle corrispondenze, identifica il tipo di istanza con il prezzo più basso.
- Se non c'è alcuna corrispondenza, esamina tutti i tipi di istanza della generazione corrente che corrispondono ai tuoi attributi. Se trova delle corrispondenze, identifica il tipo di istanza con il prezzo più basso.
- Se non c'è alcuna corrispondenza, esamina tutti i tipi di istanza della generazione precedente che corrispondono ai tuoi attributi e identifica il tipo di istanza con il prezzo più basso.

Protezione del prezzo delle istanze On-Demand

La soglia di protezione del prezzo per i tipi di istanze On-Demand viene calcolata come percentuale superiore al tipo di istanza On-Demand identificato con il prezzo più basso (). `OnDemandMaxPricePercentageOverLowestPrice` Specifichi la percentuale più alta che sei disposto a pagare. Se non specifichi questo parametro, `20` viene utilizzato un valore predefinito di per calcolare una soglia di protezione del prezzo del 20% superiore al prezzo identificato.

Ad esempio, se il prezzo dell'istanza On-Demand identificata è`0.4271`, e lo si specifica`25`, la soglia di prezzo è superiore del 25% rispetto a`0.4271`. Viene calcolato come segue:`0.4271 * 1.25 =`

0.533875. Il prezzo calcolato è il massimo che sei disposto a pagare per le istanze On-Demand e, in questo esempio, Amazon EC2 escluderà qualsiasi tipo di istanza On-Demand che costa più di. 0.533875

Protezione del prezzo delle istanze Spot

Per impostazione predefinita, Amazon EC2 applicherà automaticamente una protezione ottimale del prezzo delle istanze Spot per scegliere in modo coerente tra un'ampia gamma di tipi di istanze. Puoi anche impostare manualmente la protezione del prezzo. Tuttavia, lasciare che Amazon EC2 lo faccia per te può aumentare la probabilità che la tua capacità Spot venga soddisfatta.

Puoi specificare manualmente la protezione del prezzo utilizzando una delle seguenti opzioni. Se imposti manualmente la protezione del prezzo, ti consigliamo di utilizzare la prima opzione.

- Una percentuale del tipo di istanza On-Demand identificato con il prezzo più basso [] MaxSpotPriceAsPercentageOfOptimalOnDemandPrice

  Ad esempio, se il prezzo del tipo di istanza On-Demand identificato è0.4271, e lo si specifica60, la soglia di prezzo è pari al 60% di. 0.4271 Viene calcolato come segue:0.4271 * 0.60 = 0.25626. Il prezzo calcolato è il massimo che sei disposto a pagare per le istanze Spot e, in questo esempio, Amazon EC2 escluderà qualsiasi tipo di istanza Spot che costa più di. 0.25626
- Una percentuale superiore al tipo di istanza Spot identificato con il prezzo più basso [] SpotMaxPricePercentageOverLowestPrice

  Ad esempio, se il prezzo del tipo di istanza Spot identificato è0.1808, e lo si specifica25, la soglia di prezzo è superiore del 25% rispetto a0.1808. Viene calcolato come segue:0.1808 * 1.25 = 0.226. Il prezzo calcolato è il massimo che sei disposto a pagare per le istanze Spot e, in questo esempio, Amazon EC2 escluderà qualsiasi tipo di istanza Spot che costa più di. 0.266 Non consigliamo di utilizzare questo parametro perché i prezzi Spot possono variare e pertanto anche la soglia di protezione del prezzo potrebbe variare.

Specificate la soglia di protezione del prezzo

Per specificare la soglia di protezione del prezzo

Durante la creazione del parco istanze spot, configura il parco istanze per la selezione del tipo di istanza basata su attributi ed esegui le seguenti operazioni:

- Console

Per specificare la soglia di protezione del prezzo dell'istanza on demand, in Additional instance attribute (Attributo istanza aggiuntivo), scegli On-demand price protection (Protezione del prezzo on demand) e quindi Add attribute (Aggiungi attributo). Per On-Demand price protection percentage (Percentuale di protezione del prezzo on demand), inserisci la soglia di protezione del prezzo in percentuale.

Per specificare la soglia di protezione del prezzo dell'istanza spot, in Additional instance attribute (Attributo istanza aggiuntivo), scegli Spot price protection (Protezione del prezzo Spot) e quindi Add attribute (Aggiungi attributo). Scegliete un parametro e inserite la soglia di protezione del prezzo come percentuale.

- AWS CLI

  Per specificare la soglia di protezione del prezzo dell'istanza on demand, nel file di configurazione JSON, nella struttura `InstanceRequirements`, per `OnDemandMaxPricePercentageOverLowestPrice`, inserisci la soglia di protezione del prezzo in percentuale.

  Per specificare la soglia di protezione del prezzo dell'istanza Spot, nel file di configurazione JSON, nella `InstanceRequirements` struttura, specifica uno dei seguenti parametri:

  - Per`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, inserisci la soglia di protezione del prezzo come percentuale.
  - Per`SpotMaxPricePercentageOverLowestPrice`, inserite la soglia di protezione del prezzo in percentuale.

Per ulteriori informazioni sulla creazione del parco istanze, consulta Creazione di una serie di istanze spot con la selezione del tipo di istanza basata su attributi.

> **Note**
>
> Quando crei il parco istanze spot, se imposti il tipo Total target capacity (Capacità target totale) su vCPUs (vCPU) o Memory (MiB) (Memoria (MiB)) (console) o `TargetCapacityUnitType` su `vcpu` o `memory-mib` (AWS CLI), la soglia di protezione del prezzo viene applicata in base al prezzo per vCPU o per memoria, anziché al prezzo per istanza.

Considerazioni

- È possibile specificare i tipi di istanza o gli attributi di istanza in una serie di istanze spot, ma non entrambi nello stesso momento.

  Quando si utilizza la CLI, le sostituzioni del modello di avvio sovrascriveranno il modello di avvio. Ad esempio, se il modello di avvio contiene un tipo di istanza e la sostituzione del modello di avvio contiene attributi di istanza, le istanze identificate dagli attributi di istanza sostituiranno il tipo di istanza nel modello di avvio.
- Quando si utilizza la CLI e si specificano gli attributi di istanza come sostituzioni, non è possibile specificare pesi o priorità.
- In una configurazione di richiesta è possibile specificare un massimo di quattro strutture `InstanceRequirements`.

Creazione di una serie di istanze spot con la selezione del tipo di istanza basata su attributi

È possibile configurare un parco istanze in modo da utilizzare la selezione del tipo di istanza basata su attributi tramite la console Amazon EC2 o la AWS CLI.

Argomenti

- Creazione di una serie di istanze spot tramite la console
- Crea una flotta Spot utilizzando il AWS CLI

Creazione di una serie di istanze spot tramite la console

Come configurare una serie di istanze spot per la selezione del tipo di istanza basata su attributi (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione selezionare Spot Requests (Richieste Spot) e scegli Request Spot Instances (Istanze spot richiesta).
3. Seguire la procedura per creare una serie di istanze spot. Per ulteriori informazioni, consulta Creare una richiesta di parco istanze spot utilizzando parametri definiti (console).

   Durante la creazione della serie di istanze spot, configurare il parco istanze per la selezione del tipo di istanza basata su attributi come segue:

a. Per Instance type requirements (Requisiti per il tipo di istanza), scegliere Specify instance attributes that match your compute requirements (Specifica gli attributi di istanza che corrispondono ai requisiti di calcolo).

b. Per vCPUs (vCPU) inserire il numero minimo e massimo desiderato di vCPU. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.

c. Per Memory (GiB) (Memoria [GiB]) inserire la quantità minima e massima di memoria desiderata. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.

d. (Facoltativo) Per Additional instance attributes (Attributi istanza aggiuntivi), facoltativamente, è possibile specificare uno o più attributi per esprimere i requisiti di calcolo in modo più dettagliato. Ogni attributo aggiuntivo aggiunge ulteriori vincoli alla propria richiesta.

e. (Facoltativo) Espandere Preview matching instance types (Anteprima tipi di istanza corrispondenti) per visualizzare i tipi di istanza con gli attributi specificati.

Crea una flotta Spot utilizzando il AWS CLI

Configurazione di un parco istanze spot per la selezione del tipo di istanza basata su attributi (AWS CLI)

Usa il comando request-spot-fleet(AWS CLI) per creare una flotta Spot. Specificare la configurazione del parco istanze in un file JSON.

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

Esempio di file *file_name*.json

L'esempio seguente contiene i parametri che configurano un parco istanze spot in modo da utilizzare la selezione del tipo di istanza basata su attributi ed è seguito da una spiegazione.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
```

```
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

I parametri per la selezione del tipo di istanza basata su attributi sono specificati nella struttura `InstanceRequirements`. In questo esempio, vengono specificati due attributi:

- `VCpuCount`: viene specificato un minimo di 2 vCPU. Poiché non è specificato alcun massimo, non esiste un limite massimo.
- `MemoryMiB`: viene specificato un minimo di 4 MiB di memoria. Poiché non è specificato alcun massimo, non esiste un limite massimo.

Verranno identificati tutti i tipi di istanza con 2 o più vCPU e 4 MiB o più di memoria. Tuttavia, la protezione dei prezzi e la strategia di allocazione potrebbero escludere alcuni tipi di istanze quando il parco istanze spot alloca le istanze.

Per un elenco e le descrizioni di tutti i possibili attributi che puoi specificare, consulta InstanceRequirementsAmazon EC2 API Reference.

> **Note**
>
> Quando `InstanceRequirements` è incluso nella configurazione del parco istanze, `InstanceType` e `WeightedCapacity` devono essere esclusi; non possono determinare la configurazione del parco istanze contemporaneamente agli attributi di istanza.

Il JSON contiene anche la seguente configurazione del parco istanze:

- `"AllocationStrategy": "priceCapacityOptimized"`: la strategia di allocazione per le istanze spot nel parco istanze.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"`: il modello di avvio contiene alcune informazioni sulla configurazione delle istanze; tuttavia, se vengono specificati dei tipi di istanza, questi verranno sostituiti dagli attributi specificati in `InstanceRequirements`.
- `"TargetCapacity": 20`: la capacità obiettivo è di 20 istanze.
- `"Type": "request"`: il tipo di richiesta per il parco istanze è `request`.

Esempi di configurazioni valide e non valide

Se utilizzi il AWS CLI per creare una flotta Spot, devi assicurarti che la configurazione del tuo parco veicoli sia valida. I seguenti esempi mostrano configurazioni valide e non valide.

Le configurazioni sono considerate non valide quando contengono quanto segue:

- Una singola struttura `Overrides` con `InstanceRequirements` e `InstanceType`
- Due strutture `Overrides`, una con `InstanceRequirements` e l'altra con `InstanceType`
- Due strutture `InstanceRequirements` con valori di attributo sovrapposti all'interno dello stesso `LaunchTemplateSpecification`

Configurazioni di esempio

- Configurazione valida: modello di avvio singolo con sostituzioni
- Configurazione valida: modello di lancio singolo con più InstanceRequirements
- Configurazione valida: due modelli di avvio, ognuno con sostituzioni
- Configurazione valida: specificati solo InstanceRequirements, nessun valore di attributo sovrapposto
- Configurazione non valida: Overrides contiene InstanceRequirements e InstanceType
- Configurazione non valida: due Overrides contengono InstanceRequirements e InstanceType
- Configurazione non valida: valori di attributo sovrapposti

Configurazione valida: modello di avvio singolo con sostituzioni

La configurazione seguente è valida. Contiene un modello di avvio e una struttura `Overrides` contenente una struttura `InstanceRequirements`. Di seguito è riportata una spiegazione della configurazione di esempio.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
        "TargetCapacity": 5000,
            "OnDemandTargetCapacity": 0,
            "TargetCapacityUnitType": "vcpu"
    }
}
```

`InstanceRequirements`

Per utilizzare la selezione dell'istanza basata su attributi, è necessario includere la struttura `InstanceRequirements` nella configurazione del parco istanze e specificare gli attributi desiderati per le istanze nel parco istanze.

Nell'esempio precedente, vengono specificati i seguenti attributi di istanza:

- `VCpuCount`: i tipi di istanza devono avere un minimo di 2 e un massimo di 8 vCPU.
- `MemoryMiB`: i tipi di istanza devono avere un massimo di 10240 MiB di memoria. Un minimo di 0 indica nessun limite minimo.
- `MemoryGiBPerVCpu`: i tipi di istanza devono avere un massimo di 10.000 MiB di memoria per vCPU. Il parametro `Min` è facoltativo. Omettendolo, non si indica alcun limite minimo.

`TargetCapacityUnitType`

Il parametro `TargetCapacityUnitType` specifica l'unità per la capacità di destinazione. Nell'esempio, la capacità di destinazione è `5000` e il tipo di unità della capacità di destinazione è `vcpu`, che insieme specificano una capacità di destinazione desiderata di 5.000 vCPU. La serie di istanze spot avvierà un numero sufficiente di istanze in modo che il numero totale di vCPU nel parco istanze sia di 5.000.

Configurazione valida: modello di lancio singolo con più InstanceRequirements

La configurazione seguente è valida. Contiene un modello di avvio e una struttura `Overrides` contenente due strutture `InstanceRequirements`. Gli attributi specificati in `InstanceRequirements` sono validi perché i valori non si sovrappongono; la prima struttura `InstanceRequirements` specifica un `VCpuCount` di 0-2 vCPU, mentre la seconda struttura `InstanceRequirements` specifica 4-8 vCPU.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
```

```
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configurazione valida: due modelli di avvio, ognuno con sostituzioni

La configurazione seguente è valida. Contiene due modelli di avvio, ognuno con una struttura `Overrides` contenente una struttura `InstanceRequirements`. Questa configurazione è utile per il supporto delle architetture `arm` e `x86` nello stesso parco istanze.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
```

```
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configurazione valida: specificati solo **`InstanceRequirements`**, nessun valore di attributo sovrapposto

La configurazione seguente è valida. Contiene due strutture `LaunchTemplateSpecification`, ognuna con un modello di avvio e una struttura `Overrides` contenente una struttura `InstanceRequirements`. Gli attributi specificati in `InstanceRequirements` sono validi perché i valori non si sovrappongono; la prima struttura `InstanceRequirements` specifica un `VCpuCount` di 0-2 vCPU, mentre la seconda struttura `InstanceRequirements` specifica 4-8 vCPU.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
```

```
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configurazione non valida: **`Overrides`** contiene **`InstanceRequirements`** e **`InstanceType`**

La configurazione seguente non è valida. La struttura `Overrides` include sia `InstanceRequirements` che `InstanceType`. Per le `Overrides`, è possibile specificare `InstanceRequirements` o `InstanceType`, ma non entrambi.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configurazione non valida: due **`Overrides`** contengono **`InstanceRequirements`** e **`InstanceType`**

La configurazione seguente non è valida. Le strutture `Overrides` contengono sia `InstanceRequirements` che `InstanceType`. È possibile specificare `InstanceRequirements` o `InstanceType` ma non entrambi, anche se si trovano in strutture `Overrides` differenti.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configurazione non valida: valori di attributo sovrapposti

La configurazione seguente non è valida. Le due strutture `InstanceRequirements`, ognuna contenente `"VCpuCount": {"Min": 0, "Max": 2}`. I valori di questi attributi si sovrappongono, il che restituirà pool di capacità duplicati.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
```

```
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Anteprima di tipi di istanza con attributi specificati

È possibile utilizzare il AWS CLI comando get-instance-types-from-instance-requirements per visualizzare in anteprima i tipi di istanza che corrispondono agli attributi specificati. Ciò è particolarmente utile per capire quali attributi specificare nella configurazione della richiesta senza avviare alcuna istanza. Si noti che il comando non considera la capacità disponibile.

Per visualizzare in anteprima un elenco di tipi di istanze specificando gli attributi utilizzando il AWS CLI

1. (Facoltativo) Per generare tutti i possibili attributi che possono essere specificati, utilizzate il comando get-instance-types-from-instance-requirements e il parametro. `--generate-cli-skeleton` Facoltativamente, è possibile indirizzare l'output a un file per salvarlo tramite `input > attributes.json`.

```
aws ec2 get-instance-types-from-instance-requirements \
    --region us-east-1 \
    --generate-cli-skeleton input > attributes.json
```

Output previsto

```
{
    "DryRun": true,
    "ArchitectureTypes": [
        "i386"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
```

```
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
```

```
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Creare un file di configurazione JSON utilizzando l'output del passaggio precedente e configurarlo come segue:

> **Note**
>
> È necessario fornire valori per `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. È possibile omettere gli altri attributi, nel qual caso saranno utilizzati i valori di default.
> Per una descrizione di ogni attributo e dei relativi valori predefiniti, consulta get-instance-types-from-instance-requirements in Amazon EC2 Command Line Reference.

   a. Per `ArchitectureTypes`, specificare uno o più tipi di architettura del processore.
   b. Per `VirtualizationTypes`, specificare uno o più tipi di virtualizzazione.
   c. Per `VCpuCount`, specificare il numero minimo e massimo di vCPU. Per non specificare un limite minimo, per `Min`, specificare `0`. Per non specificare alcun limite massimo, omettere il parametro `Max`.
   d. Per `MemoryMiB`, specificare la quantità minima e massima di memoria in MiB. Per non specificare un limite minimo, per `Min`, specificare `0`. Per non specificare alcun limite massimo, omettere il parametro `Max`.
   e. Facoltativamente, è possibile specificare uno o più altri attributi per limitare ulteriormente l'elenco di tipi di istanza restituiti.

3. Per visualizzare in anteprima i tipi di istanza con gli attributi specificati nel file JSON, usa il comando get-instance-types-from-instance-requirements e specifica il nome e il percorso del file JSON utilizzando il parametro. `--cli-input-json` Facoltativamente, è possibile formattare l'output in modo che venga visualizzato in un formato tabella.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
```

```
    --output table
```

Esempio di file *attributes.json*

In questo esempio gli attributi richiesti sono inclusi nel file JSON. Tali attributi sono `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. Inoltre, è incluso anche l'attributo facoltativo `InstanceGenerations`. Tenere presente che per `MemoryMiB`, il valore `Max` può essere omesso per indicare che non c'è alcun limite.

```
{
    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

Output di esempio

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
||             InstanceType              ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
```

```
||  c5ad.xlarge                          ||
||  c5d.xlarge                           ||
||  c5n.xlarge                           ||
||  c6a.xlarge                            ||
...
```

4. Dopo aver identificato i tipi di istanza che soddisfano le proprie esigenze, prendere nota degli attributi di istanza utilizzati in modo da poterli utilizzare durante la configurazione della richiesta del parco istanze.

Richieste on demand nel parco istanze spot

Per assicurarsi di avere sempre capacità di istanza, è possibile includere una richiesta di capacità on demand nella richiesta del parco istanze spot. Nella richiesta del parco istanze spot, specificare la capacità obiettivo desiderata e la quantità di tale capacità che deve essere on demand. Il saldo comprende la capacità spot, che viene avviata se sono disponibili la capacità e la disponibilità di Amazon EC2. Ad esempio, se nella richiesta del parco istanze spot si specifica la capacità obiettivo pari a 10 e la capacità on demand pari a 8, Amazon EC2 avvia 8 unità di capacità come on demand e 2 unità di capacità (10-8=2) come Spot.

Dare priorità ai tipi di istanze per la capacità on demand

Quando il parco istanze spot cerca di soddisfare la capacità on demand, per impostazione predefinita avvia come primo tipo di istanza quello con il prezzo più basso. Se `OnDemandAllocationStrategy` è impostata su `prioritized`, la serie di istanze spot utilizza la priorità per stabilire quale tipo di istanza utilizzare per primo per soddisfare la capacità on demand.

La priorità è assegnata alla sostituzione del modello di avvio e la priorità più alta viene lanciata per prima.

Esempio: assegnare priorità ai tipi di istanza

Ad esempio, hai configurato tre sostituzioni dei modelli di avvio, ognuna con un tipo di istanza diversa.

Il prezzo on demand per i tipi di istanze varia nel prezzo. Di seguito sono riportati i tipi di istanza utilizzati in questo esempio, elencati in ordine di prezzo, a partire dal tipo di istanza più economico:

- `m4.large`: più economico
- `m5.large`

- `m5a.large`

Se non usi la priorità per stabilire l'ordine, il parco istanze utilizza la capacità on demand partendo dal tipo di istanza più economico.

Tuttavia, poniamo che tu non abbia utilizzato le istanze riservate `m5.large` che vuoi utilizzare per prime. È possibile impostare la priorità di sostituzione del modello di avvio in modo che i tipi di istanze vengano utilizzati nell'ordine di priorità, come segue:

- `m5.large`: priorità 1
- `m4.large`: priorità 2
- `m5a.large`: priorità 3

Ribilanciamento della capacità

È possibile configurare il parco istanze spot per l'avvio di un'istanza spot sostitutiva quando Amazon EC2 emette un suggerimento di ribilanciamento per notificare che un'istanza spot è a rischio elevato di interruzione. Il ribilanciamento della capacità consente di mantenere la disponibilità del carico di lavoro aumentando proattivamente il parco istanze con una nuova istanza spot prima che un'istanza in esecuzione venga interrotta da Amazon EC2. Per ulteriori informazioni, consulta Raccomandazioni per il ribilanciamento delle istanze EC2.

Per configurare la serie di istanze spot in modo che avvii un'istanza spot sostitutiva, puoi usare la console Amazon EC2 o la AWS CLI.

- Console Amazon EC2: è necessario selezionare la casella di controllo Capacity rebalance (Ribilanciamento capacità) quando si crea un parco istanze spot. Per ulteriori informazioni, consulta la fase 6.d in Creare una richiesta di parco istanze spot utilizzando parametri definiti (console).
- AWS CLI: Utilizza il comando e i parametri pertinenti nella struttura. request-spot-fleet`SpotMaintenanceStrategies` Per ulteriori informazioni, vedere l' esempio di configurazione di avvio.

Limitazioni

- Il ribilanciamento della capacità è disponibile solo per i parchi istanza di tipo `maintain`.

- Quando il parco istanze è in esecuzione, non è possibile modificare l'impostazione di ribilanciamento della capacità. Per modificare l'impostazione di ribilanciamento capacità, è necessario eliminare il parco istanze e crearne uno nuovo.

Opzioni di configurazione

`ReplacementStrategy` per la serie di istanze spot supporta i due seguenti valori:

`launch-before-terminate`

Amazon EC2 termina le istanze spot che ricevono una notifica di ribilanciamento dopo avere avviato le nuove istanze spot sostitutive. Se si specifica `launch-before-terminate`, occorre specificare un valore anche per `termination-delay`. Dopo l'avvio delle nuove istanze sostitutive, Amazon EC2 attende la durata di `termination-delay`, quindi termina le vecchie istanze. Per `termination-delay`, il minimo è 120 secondi (2 minuti) e il massimo è di 7200 secondi (2 ore).

Consigliamo di utilizzare `launch-before-terminate` solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza. Ciò garantirà che le vecchie istanze vengano terminate solo dopo il completamento delle procedure di arresto. Tenere presente che Amazon EC2 può interrompere le vecchie istanze con un avviso di due minuti prima di `termination-delay`.

`launch`

Amazon EC2 avvia le istanze spot sostitutive quando viene emessa una notifica di ribilanciamento per le istanze spot esistenti. Amazon EC2 non termina le istanze che ricevono una notifica di ribilanciamento. È possibile terminare le vecchie istanze o lasciarle in esecuzione. Saranno addebitati i costi per entrambe le istanze durante la loro esecuzione.

Considerazioni

Se si configura un parco istanze spot per il ribilanciamento della capacità, è necessario considerare quanto segue:

Fornisci il maggior numero possibile di pool di capacità spot nella richiesta

È possibile configurare il parco istanze spot affinché utilizzi diversi tipi di istanza e zone di disponibilità. Ciò fornisce la flessibilità necessaria per avviare Istanze spot in vari pool di capacità

spot. Per ulteriori informazioni, consulta Essere flessibili riguardo tipi di istanza e zone di disponibilità.

Evitare un rischio elevato di interruzione delle istanze spot sostitutive

Per evitare un rischio elevato di interruzione, consigliamo la strategia di `capacityOptimizedPrioritized` allocazione `capacityOptimized` o. Queste strategie garantiscono che le Spot Instances (Istanze spot) sostitutive vengano avviate nei pool di capacità spot ottimali per cui è meno probabile che vengano interrotte nel prossimo futuro. Per ulteriori informazioni, consulta Utilizzo della strategia di allocazione ottimizzata per prezzo e capacità.

Amazon EC2 avvierà una nuova istanza solo se la disponibilità è uguale o migliore

Uno degli obiettivi del ribilanciamento della capacità è migliorare la disponibilità di un'istanza spot. Se un'istanza spot esistente riceve una raccomandazione di ribilanciamento, Amazon EC2 avvierà una nuova istanza solo se la nuova istanza fornisce una disponibilità uguale o migliore rispetto all'istanza esistente. Se il rischio di interruzione di una nuova istanza è peggiore di quello dell'istanza esistente, Amazon EC2 non avvierà una nuova istanza. Tuttavia, Amazon EC2 continuerà a valutare i pool di capacità spot e avvierà una nuova istanza se la disponibilità migliorerà.

È possibile che l'istanza esistente venga interrotta senza che Amazon EC2 avvii in modo proattivo una nuova istanza. In questo caso, Amazon EC2 tenterà di avviare una nuova istanza indipendentemente dal fatto che la nuova istanza presenti un rischio elevato di interruzione.

Il ribilanciamento della capacità non aumenta il tasso di interruzione dell'istanza Spot

Quando si abilita il ribilanciamento della capacità, non aumenta il tasso di interruzione dell'istanza spot (il numero di istanze Spot che vengono recuperate quando Amazon EC2 ha bisogno di capacità). Tuttavia, se il ribilanciamento della capacità rileva che un'istanza è a rischio di interruzione, Amazon EC2 tenterà immediatamente di avviare una nuova istanza. Il risultato è che potrebbero essere sostituite più istanze di quelle che sarebbero state sostituite se avessi aspettato che Amazon EC2 avviasse una nuova istanza dopo l'interruzione di quella a rischio.

Sebbene sia possibile sostituire più istanze mediante l'abilitazione del ribilanciamento delle capacità, è meglio prendersi più tempo per agire prima che le istanze vengano interrotte. Con un Avviso di interruzione dell'istanza Spot, in genere hai solo fino a due minuti per interrompere l'istanza. Con il ribilanciamento della capacità che avvia una nuova istanza in anticipo, offri ai processi esistenti maggiori possibilità di completamento sull'istanza a rischio, puoi avviare le procedure di chiusura dell'istanza e impedire la pianificazione di nuovi lavori sull'istanza a rischio. Puoi anche iniziare a preparare l'istanza appena avviata per assumere il controllo

dell'applicazione. Con la sostituzione proattiva offerta dal ribilanciamento della capacità, puoi beneficiare di una continuità regolare.

Come esempio teorico per dimostrare i rischi e i benefici dell'utilizzo del ribilanciamento della capacità, osserviamo il seguente scenario:

- 14:00: viene ricevuto un suggerimento di ribilanciamento per l'istanza A e Amazon EC2 inizia immediatamente a tentare di avviare un'istanza sostitutiva B, dandoti il tempo di iniziare le procedure di arresto.*
- 14:30: viene ricevuto un suggerimento di ribilanciamento per l'istanza B, sostituita dall'istanza C dandoti il tempo di iniziare le procedure di arresto.*
- 14:32: se il ribilanciamento della capacità non fosse abilitato e se un avviso di interruzione dell'istanza Spot fosse stato ricevuto alle 14:32 per l'istanza A, avresti avuto solo fino a due minuti per agire, ma l'istanza A sarebbe stata in esecuzione fino a questo momento.

* Se `launch-before-terminate` è specificato, Amazon EC2 terminerà l'istanza a rischio dopo che l'istanza sostitutiva sarà online.

Amazon EC2 può avviare nuove Istanze spot sostitutive fino a quando la capacità soddisfatta non è il doppio della capacità obiettivo

Quando un parco istanze spot è configurato per il ribilanciamento della capacità, Amazon EC2 tenta di avviare una nuova istanza spot sostitutiva per ogni istanza spot che riceve un suggerimento di ribilanciamento. Dopo che un'istanza spot riceve un suggerimento di ribilanciamento, non viene più conteggiata come parte della capacità evasa. A seconda della strategia di sostituzione, Amazon EC2 termina l'istanza dopo un ritardo di terminazione preconfigurato o la lascia in esecuzione. In questo modo è possibile eseguire operazioni di ribilanciamento sull'istanza.

Se il parco istanze raggiunge il doppio della capacità target, smette di lanciare nuove istanze sostitutive anche se le istanze sostitutive stesse ricevono una raccomandazione di ribilanciamento.

Ad esempio, se crei un parco istanze spot con una capacità obiettivo di 100 istanze spot. Tutte le istanze spot ricevono un suggerimento di ribilanciamento, cosicché Amazon EC2 avvia 100 istanze spot sostitutive. In questo modo il numero di istanze spot evase sale a 200, che è il doppio della capacità target. Alcune istanze sostitutive ricevono una raccomandazione di ribilanciamento, ma non vengono più avviate istanze sostitutive perché il parco istanze non può superare il doppio della capacità target.

Tenere presente che tutte le istanze vengono addebitate mentre sono in esecuzione.

Si consiglia di configurare la serie di istanze spot in modo che termini le istanze spot che ricevono un suggerimento di ribilanciamento

Se si configura la serie di istanze spot per il ribilanciamento della capacità, si consiglia di scegliere `launch-before-terminate` con un ritardo di terminazione appropriato solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza. Ciò garantirà che le vecchie istanze vengano terminate solo dopo il completamento delle procedure di arresto.

Se si decide di terminare autonomamente le istanze suggerite per il ribilanciamento, si consiglia di monitorare il segnale di suggerimento del ribilanciamento ricevuto dalle istanze spot nel parco istanze. Monitorando il segnale, puoi eseguire rapidamente le operazioni di ribilanciamento sulle istanze interessate prima che Amazon EC2 le interrompa; poi potrai terminarle manualmente. Se non si terminano le istanze, verranno addebitati i relativi costi fintantoché sono in esecuzione. Amazon EC2 non termina automaticamente le istanze che ricevono un suggerimento di ribilanciamento.

Puoi configurare le notifiche utilizzando Amazon EventBridge o i metadati delle istanze. Per ulteriori informazioni, consulta Monitorare i segnali di raccomandazione di ribilanciamento.

La serie di istanze spot non conteggia le istanze che ricevono un suggerimento di ribilanciamento quando calcola la capacità evasa durante il dimensionamento orizzontale o verticale

Se il parco istanze spot è configurato per il ribilanciamento della capacità e si modifica la capacità obiettivo per il dimensionamento orizzontale o verticale, la il parco istanze non conteggia le istanze contrassegnate per il ribilanciamento come parte della capacità evasa, come indicato di seguito:

- Riduzione orizzontale: se riduci la capacità obiettivo desiderata, Amazon EC2 termina le istanze che non sono contrassegnate per il ribilanciamento fino a quando non viene raggiunta la capacità desiderata. Le istanze contrassegnate per il ribilanciamento non vengono conteggiate per la capacità evasa.

  Ad esempio, crei un parco istanze spot con una capacità obiettivo di 100 istanze spot. 10 istanze ricevono un suggerimento di ribilanciamento, quindi Amazon EC2 avvia 10 nuove istanze sostitutive, con una capacità soddisfatta di 110 istanze. Riduci quindi la capacità obiettivo a 50 (riduzione orizzontale), ma la capacità soddisfatta è in realtà di 60 istanze, perché le 10 istanze contrassegnate per il ribilanciamento non vengono terminate da Amazon EC2. È necessario terminare manualmente queste istanze oppure lasciarle in esecuzione.

- Aumento orizzontale: se aumenti la capacità desiderata obiettivo, Amazon EC2 avvia nuove istanze fino al raggiungimento della capacità desiderata. Le istanze contrassegnate per il ribilanciamento non vengono conteggiate per la capacità evasa.

  Ad esempio, crei un parco istanze spot con una capacità obiettivo di 100 istanze spot. 10 istanze ricevono un suggerimento di ribilanciamento, quindi Amazon EC2 avvia 10 nuove istanze sostitutive, con una capacità soddisfatta di 110 istanze. Si aumenta quindi la capacità target a 200 (dimensionamento orizzontale), ma la capacità evasa effettiva è di 210 istanze, perché le 10 istanze contrassegnate per il ribilanciamento non vengono conteggiate dal parco istanze come parte della capacità target. È necessario terminare manualmente queste istanze oppure lasciarle in esecuzione.

Sostituzioni prezzo Spot

Ogni richiesta di parco istanze spot può includere un prezzo massimo globale o utilizzare quello predefinito (il prezzo on demand). Il parco istanze spot utilizza questo come il prezzo massimo predefinito per ciascuna delle sue specifiche di avvio.

È anche possibile specificare un prezzo massimo in una o più specifiche di avvio. Questo prezzo è relativo alla specifica di avvio. Se una specifica di avvio include un prezzo specifico, il parco istanze spot utilizza tale prezzo massimo, sostituendo il prezzo massimo globale. Le altre specifiche di avvio che non comprendono un prezzo massimo specifico continuano a utilizzare il prezzo massimo globale.

Controllo delle spese

Il parco istanze spot interrompe l'avvio delle istanze quando ha raggiunto la capacità e l'importo massimo che sei disposto a pagare. Per controllare l'importo che paghi all'ora per il parco istanze, puoi specificare il parametro `SpotMaxTotalPrice` per Istanze spot e il parametro `OnDemandMaxTotalPrice` per Istanze on demand. Quando viene raggiunto il prezzo totale massimo, il parco istanze spot interrompe l'avvio delle istanze anche se non è stata raggiunta la capacità obiettivo.

I seguenti esempi illustrano due scenari diversi. Nel primo, il parco istanze spot interrompe l'avvio delle istanze quando ha raggiunto la capacità obiettivo. Nel secondo, il parco istanze spot interrompe l'avvio delle istanze quando ha raggiunto l'importo massimo che sei disposto a pagare.

Esempio: arresto dell'avvio delle istanze al raggiungimento della capacità target

Data una richiesta di Istanze on demand `m4.large`, dove:

- Prezzo on demand: 0,10 USD all'ora
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 1,50 USD

La serie di istanze spot avvia 10 istanze on demand perché il totale di 1 USD (10 istanze x 0,10 USD) non supera il `OnDemandMaxTotalPrice` di 1,50 USD.

Esempio: arresto dell'avvio delle istanze al raggiungimento del prezzo totale massimo

Data una richiesta di Istanze on demand `m4.large`, dove:

- Prezzo on demand: 0,10 USD all'ora
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 0,80 USD

Se la serie di istanze spot avvia la capacità obiettivo on demand (10 Istanze on demand), il costo totale all'ora è di 1 USD, ovvero un importo superiore rispetto a quello specificato (0,80 USD) per il parametro `OnDemandMaxTotalPrice`. Per evitare di spendere più di quello che ti sei prefissato, la serie di istanze spot avvia solo 8 Istanze on demand (al di sotto della capacità obiettivo on demand) perché avviarne di più significherebbe superare il `OnDemandMaxTotalPrice`.

Ponderazione delle istanze del parco istanze spot

Quando richiedi un parco istanze di Istanze spot, puoi definire le unità di capacità con cui ogni tipo di istanza contribuirebbe alle prestazioni dell'applicazione e regolare il prezzo massimo per ogni pool di capacità spot di conseguenza, utilizzando la ponderazione di istanza.

Per impostazione predefinita, il prezzo specificato è all'ora per istanza. Quando si utilizza la funzionalità di ponderazione di istanza, il prezzo specificato è all'ora per unità. È possibile calcolare il prezzo all'ora per unità dividendo il prezzo di un tipo di istanza per il numero di unità che essa rappresenta. Il parco istanze spot calcola il numero di istanze spot da avviare dividendo la capacità obiettivo per il peso dell'istanza. Se il risultato non è un numero intero, il parco istanze spot lo arrotonda al numero intero successivo, in modo che la dimensione del parco istanze non sia inferiore alla sua capacità obiettivo. Il parco istanze spot può selezionare qualsiasi pool specificato nella specifica di avvio, anche se la capacità delle istanze avviate supera la capacità obiettivo richiesta.

Le tabelle seguenti includono esempi di calcoli per determinare il prezzo per unità per una richiesta di istanza spot con una capacità obiettivo di 10.

Tipo di istanza	Peso dell'istanza	Prezzo all'ora per istanza	Prezzo all'ora per unità	Numero di istanze avviate
`r3.xlarge`	2	0,05 $	0,025 (0,05 diviso 2)	5 (10 diviso 2)

Tipo di istanza	Peso dell'istanza	Prezzo all'ora per istanza	Prezzo all'ora per unità	Numero di istanze avviate
`r3.8xlarge`	8	0,10 $	0,0125 (0,10 diviso 8)	2 (10 diviso 8, risultato arrotondato)

Utilizzare la ponderazione d'istanza del parco istanze spot come segue per assegnare la capacità obiettivo desiderata nei pool con il prezzo più basso per unità al momento dell'evasione:

1. Impostare la capacità obiettivo per il parco istanze spot sia nelle istanze (predefinite) sia nelle unità prescelte, come CPU virtuali, memoria, archiviazione o velocità effettiva.
2. Impostare il prezzo per unità.
3. Per ogni configurazione di avvio, specificare il peso, ovvero il numero di unità che il tipo di istanza rappresenta verso la capacità target.

Esempio di ponderazione istanza

Considerare una richiesta del parco istanze spot con la configurazione seguente:

- Una capacità di destinazione di 24
- Una specifica di avvio con un tipo di istanza `r3.2xlarge` e un peso di 6

- Una specifica di avvio con un tipo di istanza `c3.xlarge` e un peso di 5

I pesi rappresentano il numero di unità che il tipo di istanza rappresenta per la capacità di destinazione. Se la prima specifica di avvio fornisce il prezzo più basso per unità (prezzo all'`r3.2xlarge`ora per istanza diviso 6), il parco istanze spot avvierà quattro di tali istanze (24 diviso 6).

Se la seconda specifica di avvio fornisce il prezzo più basso per unità (prezzo per `c3.xlarge` all'ora per istanza diviso 5), la serie di istanze spot avvierà cinque di tali istanze (24 diviso 5, risultato arrotondato per eccesso).

Ponderazione d'istanza e strategia di allocazione

Considerare una richiesta del Parco istanze spot con la configurazione seguente:

- Una capacità target di 30
- Una specifica di avvio con un tipo di istanza `c3.2xlarge` e un peso di 8
- Una specifica di avvio con un tipo di istanza `m3.xlarge` e un peso di 8
- Una specifica di avvio con un tipo di istanza `r3.xlarge` e un peso di 8

Il parco istanze spot avvierà quattro istanze (30 diviso 8, risultato arrotondato per eccesso). Con la strategia `diversified`, la serie di istanze spot avvia una istanza in ognuno dei tre pool e la quarta istanza in quello dei tre pool che fornisce il prezzo più basso per unità.

Utilizzo del parco istanze spot

Per iniziare a utilizzare un parco istanze spot, puoi creare una richiesta di istanze spot che includa la capacità target, la parte on demand facoltativa, una o più specifiche di avvio per le istanze e il prezzo massimo che sei disposto a pagare. La richiesta del parco deve includere una specifica di avvio che indichi le informazioni di cui il parco istanze ha bisogno per avviare un'istanza, come un'AMI, un tipo di istanza, una sottorete o una zona di disponibilità e uno o più gruppi di sicurezza.

Se il parco istanze include Istanze spot, Amazon EC2 può tentare di mantenere la capacità di destinazione del parco istanze al variare dei prezzi Spot.

Non è possibile modificare la capacità target di una richiesta una tantum dopo che essa è stata inviata. Per modificare la capacità target, annullare la richiesta e inviarne una nuova.

Una richiesta di parco istanze spot rimane attiva fino a quando non scade o fino a quando non la si annulla. Quando annulli una richiesta di parco istanze, puoi specificare se l'annullamento della richiesta interrompe le istanze spot nel rispettivo parco istanze.

Indice

Stati della richiesta di parco istanze spot

Una richiesta di parco istanze spot può avere uno dei seguenti stati:

- `submitted` - La richiesta della serie di istanze spot è in fase di valutazione e Amazon EC2 si sta preparando ad avviare il numero di istanze previsto. Se la tua richiesta supera il limite della serie di istanze spot, viene annullata immediatamente.
- `active` - La richiesta della serie di istanze spot è stata convalidata e Amazon EC2 sta tentando di mantenere il numero previsto di istanze spot in esecuzione. La richiesta rimane in questo stato finché non viene modificata o annullata.
- `modifying` - La richiesta della serie di istanze spot è in fase di modifica. La richiesta rimane in questo stato finché la modifica non viene completamente elaborata o il parco istanze spot non viene annullato. Una `request` una tantum non può essere modificata e questo stato non è valido per tali richieste Spot.
- `cancelled_running` - La serie di istanze spot viene annullato e non avvia istanze spot aggiuntive. Le sue Istanze spot esistenti continuano a essere eseguite finché non vengono interrotte o terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono interrotte o terminate.
- `cancelled_terminating` - La serie di istanze spot viene annullato e le istanze spot vengono terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono terminate.

- `cancelled` - La serie di istanze spot viene annullato e non ha istanze spot in esecuzione. La richiesta di parco istanze spot viene eliminata due giorni dopo che le sue istanze sono state terminate.

Controlli dell'integrità del parco istanze spot

Il parco istanze spot controlla lo stato di integrità delle istanze nel parco istanze ogni due minuti. Lo stato di un'istanza è `healthy` o `unhealthy`.

Il parco istanze spot determina lo stato di integrità un'istanza utilizzando i controlli dello stato forniti da Amazon EC2. Un'istanza viene determinata come `unhealthy` quando lo stato del controllo dello stato dell'istanza o del controllo dello stato del sistema è `impaired` per tre controlli di integrità consecutivi. Per ulteriori informazioni, consulta Verifiche dello stato delle istanze.

È possibile configurare il parco istanze per sostituire le Istanze spot non integre. Dopo avere abilitato la sostituzione del controllo di integrità, un'istanza spot viene sostituita quando viene segnalata come `unhealthy`. Durante la sostituzione di un'istanza spot non integra, il parco istanze può scendere al di sotto della sua capacità obiettivo.

Requisiti

- La sostituzione del controllo dello stato è supportata solo per i Parchi istanze spot che mantengono una capacità target (parchi istanza del tipo `maintain`) e non per i Parchi istanze spot una tantum (ossia del tipo `request`).
- La sostituzione del controllo dello stato è supportata solo per Istanze spot. Questa funzionalità non è supportata per Istanze on demand.
- È possibile configurare il parco istanze spot per sostituire le istanze non integre solo al momento della sua creazione.
- Gli utenti possono utilizzare la sostituzione del controllo dell'integrità solo se hanno l'autorizzazione a chiamare l'operazione `ec2:DescribeInstanceStatus`.

Console

Per configurare un parco istanze spot per sostituire le istanze spot non integre utilizzando la Console

1. Seguire i passaggi per creare un parco istanze spot. Per ulteriori informazioni, consulta Creare una richiesta di parco istanze spot utilizzando parametri definiti (console).

2. Per configurare il parco al fine di sostituire le istanze spot non integre, per Health check (Controllo integrità) scegliere Replace unhealthy instances (Sostituisci istanze non integre). Per abilitare questa opzione, è necessario innanzitutto scegliere Maintain target capacity (Mantieni capacità target).

AWS CLI

Per configurare una serie di istanze spot per sostituire le istanze spot non integre utilizzando AWS CLI

1. Seguire i passaggi per creare un Parco istanze spot. Per ulteriori informazioni, consulta Crea una flotta Spot utilizzando il AWS CLI.
2. Per configurare il parco in modo da sostituire le Istanze spot non integre, per `ReplaceUnhealthyInstances`, immettere `true`.

Autorizzazioni del parco istanze spot

Se gli utenti IAM creano o gestiscono una serie di istanze spot, occorre concedere loro le autorizzazioni richieste.

Se utilizzi la console Amazon EC2 per creare una serie di istanze spot, viene creato un ruolo collegato ai due servizi denominato `AWSServiceRoleForEC2SpotFleet` e `AWSServiceRoleForEC2Spot` e un ruolo denominato `aws-ec2-spot-fleet-tagging-role` che concede al serie di istanze spot le autorizzazioni per richiedere, avviare, terminare e assegnare tag alle risorse per tuo conto. Se utilizzi AWS CLI o un'API, devi assicurarti che questi ruoli esistano.

Utilizzare le istruzioni seguenti per concedere le autorizzazioni necessarie e creare i ruoli.

Autorizzazioni e ruoli

- Concessione di autorizzazioni a un utente per la serie di istanze spot
- Ruolo collegato al servizio per il parco istanze spot
- Ruolo collegato ai servizi per le istanze spot
- Ruolo IAM per l'assegnazione di tag a un parco istanze spot

Concessione di autorizzazioni a un utente per la serie di istanze spot

Se gli utenti creano o gestiscono una serie di istanze spot, assicurati di concedere loro le autorizzazioni richieste.

Per creare una policy per la serie di istanze spot

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, selezionare Policies (Policy), quindi Create policy (Crea policy).
3. Nella pagina Crea policy scegliere JSON e sostituire il testo con il seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

La policy di esempio precedente concede a un utente le autorizzazioni richieste dalla maggior parte dei casi d'uso della serie di istanze spot. Per limitare l'utente a operazioni API specifiche, specificare solo tali operazioni API.

EC2 e API IAM obbligatorie

Le API seguenti devono essere incluse nella policy:

- `ec2:RunInstances` - Obbligatorio per avviare istanze in una serie di istanze spot
- `ec2:CreateTags` - Obbligatorio per applicare tag alla richiesta della serie di istanze spot, alle istanze o ai volumi
- `iam:PassRole` - Obbligatorio per specificare il ruolo della serie di istanze spot
- `iam:CreateServiceLinkedRole` - Obbligatorio per creare il ruolo collegato ai servizi
- `iam:ListRoles` - Obbligatorio per enumerare i ruoli IAM esistenti
- `iam:ListInstanceProfiles` - Obbligatorio per enumerare i profili delle istanze esistenti

> **Important**
>
> Se specifichi un ruolo per il profilo dell'istanza IAM nella specifica di avvio o nel modello di avvio, devi concedere all'utente l'autorizzazione per passare il ruolo al servizio. A tale scopo, nella policy IAM includere "`arn:aws:iam::*:role/`*`IamInstanceProfile-role`*" come risorsa per l'operazione `iam:PassRole`. Per ulteriori informazioni, consulta Concedere a un utente le autorizzazioni per passare un ruolo a un AWS servizio nella Guida per l'utente IAM.

API della serie di istanze spot

Aggiungere le operazioni API del parco istanze spot seguenti alla policy, se necessario:

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`

- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

API IAM opzionali

(Facoltativo) Per consentire a un utente di creare ruoli o profili delle istanze utilizzando la console IAM, è anche necessario aggiungere le operazioni seguenti alla policy:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Scegliere Review policy (Esamina policy).
5. Nella pagina Review policy (Rivedi policy), immettere un nome policy e una descrizione, poi selezionare Create policy (Crea policy).
6. Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

   - Utenti e gruppi in: AWS IAM Identity Center

     Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

   - Utenti gestiti in IAM tramite un provider di identità:

     Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

   - Utenti IAM:
     - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
     - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Ruolo collegato al servizio per il parco istanze spot

Amazon EC2 utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri servizi AWS per tuo conto. Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente a un AWS servizio. I ruoli collegati ai servizi forniscono un modo sicuro per delegare le autorizzazioni ai AWS servizi perché solo il servizio collegato può assumere un ruolo collegato al servizio. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati a servizi nella Guida per l'utente di IAM .

Amazon EC2 utilizza il ruolo collegato al servizio denominato AWSServiceRoleForEC2SpotFleetper avviare e gestire le istanze per tuo conto.

> **Important**
>
> Se specifichi un'AMI crittografata o uno snapshot Amazon EBS crittografato nella tua flotta Spot, devi concedere al AWSServiceRoleForEC2SpotFleetruolo l'autorizzazione a utilizzare la CMK in modo che Amazon EC2 possa avviare istanze per tuo conto. Per ulteriori informazioni, consulta Concessione dell'accesso alle CMK per l'uso con le AMI crittografate e gli snapshot EBS.

Autorizzazioni concesse da AWSServiceRoleForEC2SpotFleet

Amazon EC2 utilizza AWSServiceRoleForEC2SpotFleetper completare le seguenti azioni:

- `ec2:RequestSpotInstances` – Richiesta di Istanze spot
- `ec2:RunInstances` - Avviare istanze
- `ec2:TerminateInstances` - Terminare istanze
- `ec2:DescribeImages` - Descrivere le immagini Amazon Machine (AMI) per le istanze
- `ec2:DescribeInstanceStatus` - Monitorare lo stato delle istanze.
- `ec2:DescribeSubnets` - Descrivere le sottoreti per le istanze
- `ec2:CreateTags` - Aggiungere tag alla richiesta della serie di istanze spot, alle istanze e ai volumi
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` - Aggiungere le istanze specificate al load balancer specificato
- `elasticloadbalancing:RegisterTargets` - Registrare le destinazioni specificate nel gruppo di destinazioni specificato

Creazione del ruolo collegato ai servizi

In gran parte dei casi, non è necessario creare manualmente un ruolo collegato ai servizi. Amazon EC2 crea il ruolo AWSServiceRoleForEC2SpotFleetcollegato ai servizi la prima volta che crei una flotta Spot utilizzando la console.

Se hai ricevuto una richiesta Spot Fleet attiva prima di ottobre 2017, quando Amazon EC2 ha iniziato a supportare questo ruolo collegato al servizio, Amazon EC2 ha creato il ruolo nel tuo account. AWSServiceRoleForEC2SpotFleet AWS Per ulteriori informazioni, consulta A new role appeared in my AWS account nella IAM User Guide.

Se utilizzi AWS CLI o un'API per creare una flotta Spot, devi prima assicurarti che questo ruolo esista.

Per creare AWSServiceRoleForEC2SpotFleet utilizzando la console

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella pagina Seleziona un'entità attendibile, esegui le operazioni seguenti:
    a. Per Tipo di entità attendibile, scegli Servizio AWS .
    b. In Caso d'uso, per Servizio o caso d'uso, scegli EC2.
    c. Per Caso d'uso, scegli EC2 - Spot Fleet.
    d. Scegli Next (Successivo).
5. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).
6. Nella pagina Nomina, rivedi e crea scegli Crea ruolo.

Per creare AWSServiceRoleForEC2SpotFleet utilizzando AWS CLI

Utilizza il comando create-service-linked-role come riportato di seguito.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Se non hai più bisogno di utilizzare Spot Fleet, ti consigliamo di eliminare il AWSServiceRoleForEC2SpotFleetruolo. Dopo che questo ruolo è stato eliminato dall'account, Amazon EC2 creerà di nuovo il ruolo se viene richiesto un parco istanze spot utilizzando la console.

Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Concessione dell'accesso alle CMK per l'uso con le AMI crittografate e gli snapshot EBS

Se specifichi un AMI crittografato o uno snapshot Amazon EBS crittografato nella tua richiesta Spot Fleet e utilizzi una chiave gestita dal cliente per la crittografia, devi concedere al AWSServiceRoleForEC2SpotFleetruolo l'autorizzazione a utilizzare la CMK in modo che Amazon EC2 possa avviare istanze per tuo conto. Per farlo, occorre aggiungere una concessione alla chiave CMK, come mostrato nella procedura seguente.

Nel processo di assegnazione delle autorizzazioni, le concessioni rappresentano un'alternativa alle policy delle chiavi. Per ulteriori informazioni, consulta Utilizzo delle concessioni e Utilizzo delle policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

Per concedere al AWSServiceRoleForEC2SpotFleet ruolo le autorizzazioni per utilizzare la CMK

- Utilizzate il comando create-grant per aggiungere una concessione alla CMK e per specificare il principale (il ruolo AWSServiceRoleForEC2SpotFleetcollegato al servizio) a cui viene concessa l'autorizzazione per eseguire le operazioni consentite dalla concessione. La CMK è specificata dal parametro `key-id` e dal relativo ARN. Il principale è specificato dal `grantee-principal` parametro e dall'ARN del ruolo collegato al AWSServiceRoleForEC2SpotFleetservizio.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/
AWSServiceRoleForEC2SpotFleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Ruolo collegato ai servizi per le istanze spot

Amazon EC2 utilizza il ruolo collegato al servizio denominato AWSServiceRoleForEC2Spotper avviare e gestire le istanze Spot per tuo conto. Per ulteriori informazioni, consulta Ruolo collegato ai servizi per le richieste di istanza spot.

Ruolo IAM per l'assegnazione di tag a un parco istanze spot

Il ruolo IAM `aws-ec2-spot-fleet-tagging-role` concede l'autorizzazione al serie di istanze spot per assegnare tag alla richiesta, alle istanze e ai volumi della serie di istanze spot. Per ulteriori informazioni, consulta Assegnare tag a un parco istanze spot.

> **Important**
>
> Se scegli di applicare tag alle istanze nel parco istanze e scegli anche di mantenere la capacità obiettivo (la richiesta della serie di istanze spot è di tipo `maintain`), le differenze nelle autorizzazioni impostate per l'utente e il `IamFleetRole` potrebbero generare un comportamento incoerente nell'assegnazione di tag alle istanze nel parco istanze. Se l'autorizzazione `CreateTags` `IamFleetRole` non include, alcune delle istanze lanciate dal parco istanze potrebbero non essere taggate. Mentre stiamo lavorando per risolvere questa incoerenza, per garantire che tutte le istanze lanciate dal parco istanze siano taggate, si consiglia di utilizzare il ruolo `aws-ec2-spot-fleet-tagging-role` per `IamFleetRole`. In alternativa, per utilizzare un ruolo esistente, collega la `AmazonEC2SpotFleetTaggingRole` AWS Managed Policy al ruolo esistente. In caso contrario, è necessario aggiungere manualmente l'autorizzazione `CreateTags` alla policy esistente.

Per creare il ruolo IAM per l'assegnazione di tag a un parco istanze spot

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella pagina Select trusted entity (Seleziona entità attendibile) in Trusted entity type (Tipo di entità attendibile), scegli AWS service (Servizio).
5. In Caso d'uso, da Casi d'uso per altri AWS servizi, scegli EC2, quindi scegli EC2 - Spot Fleet Tagging.
6. Scegli Next (Successivo).
7. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).
8. Nella pagina Name, review, and create (Nome, revisione e creazione), per Role name (Nome ruolo) inserisci un nome per il ruolo (ad esempio **`aws-ec2-spot-fleet-tagging-role`**).
9. Rivedi le informazioni presenti nella pagina, quindi scegli Create role (Crea ruolo).

Prevenzione del confused deputy tra servizi

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. Si consiglia di utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` nelle policy di attendibilità `aws-ec2-spot-fleet-tagging-role` per limitare le autorizzazioni con cui la serie di istanze spot fornisce un altro servizio alla risorsa.

Per aggiungere le chiavi aws: SourceArn e aws: SourceAccount condition alla policy di fiducia **`aws-ec2-spot-fleet-tagging-role`**

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Individuare la policy `aws-ec2-spot-fleet-tagging-role` creata in precedenza e scegliere il collegamento (non la casella di controllo).
4. In Summary (Riepilogo), scegliere la scheda Trust relationships (Relazioni di attendibilità), quindi scegliere Edit trust policy (Modifica policy di attendibilità).
5. Nell'istruzione JSON, aggiungere un elemento `Condition` contenente le proprie chiavi di contesto delle condizioni globali `aws:SourceAccount` e `aws:SourceArn` per prevenire il problema del “deputy confused”, come segue:

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
```

> **Note**
>
> Se si utilizzano entrambe le chiavi di contesto delle condizioni globali e il valore `aws:SourceArn` contiene l'ID account, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account quando viene utilizzato nella stessa dichiarazione di policy.

La policy di attendibilità finale sarà la seguente:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
    }
  }
}
```

6. Scegli Aggiorna policy.

La tabella seguente fornisce valori potenziali affinché `aws:SourceArn` limiti l'ambito di `aws-ec2-spot-fleet-tagging-role` secondo diversi gradi di specificità.

Operazione API	Servizio chiamato	Ambito	**`aws:SourceArn`**
RequestSpotFleet	AWS STS (`AssumeRole`)	Limita la `AssumeRole` funzionalità `aws-ec2-spot-fleet-tagging-role` spot-fleet-requests all'account specificato.	`arn:aws:ec2:*: 123456789012 :spot-fleet-request/sfr-*`

Operazione API	Servizio chiamato	Ambito	**aws:SourceArn**
RequestSpotFleet	AWS STS (AssumeRole)	Limita la AssumeRole capacità aws-ec2-spot-fleet-tagging-role spot-fleet-requests all'account e alla regione specificati. Questo ruolo non sarà utilizzabile in altre regioni.	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Limita la capacità di AssumeRole in aws-ec2-spot-fleet-tagging-role alle sole operazioni che interessano il parco istanze sfr-11111111-1111-1111-1111-111111111111. Questo ruolo potrebbe non essere utilizzabile per altre serie di istanze spot. Inoltre, questo ruolo non può essere utilizzato per lanciare nuove flotte Spot tramiterequest-spot-fleet.	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*11111111-1111-1111-1111-111111111111*

Creare una richiesta di parco istanze spot

Utilizzando AWS Management Console, crea rapidamente una richiesta Spot Fleet scegliendo solo l'applicazione o l'attività di cui hai bisogno e le specifiche di calcolo minime. Amazon EC2 configura un parco istanze più appropriato alle tue esigenze e segue le best practice Spot. Per ulteriori informazioni, consulta Creare rapidamente una richiesta di parco istanze spot (console). In caso contrario, puoi modificare le impostazioni predefinite che preferisci. Per ulteriori informazioni, consulta Creare una richiesta di parco istanze spot utilizzando parametri definiti (console) e Crea una flotta Spot utilizzando il AWS CLI.

Opzioni per creare un parco istanze spot

- Creare rapidamente una richiesta di parco istanze spot (console)
- Creare una richiesta di parco istanze spot utilizzando parametri definiti (console)
- Crea una flotta Spot utilizzando il AWS CLI

Creare rapidamente una richiesta di parco istanze spot (console)

Per creare rapidamente una richiesta di parco istanze spot, segui la procedura descritta di seguito.

Per creare una richiesta di parco istanze spot utilizzando le impostazioni consigliate (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Se è la prima volta che viene utilizzato lo Spot, verrà visualizzata una pagina di benvenuto; selezionare Get started (Inizia). Altrimenti, selezionare Request Istanze spot (Richiedi Istanze spot).
4. Sotto Launch parameters (Parametri di avvio), scegliere Manually configure launch parameters (Configura manualmente i parametri di avvio).
5. Per AMI, scegliere un'AMI.
6. Sotto Target capacity (Capacità di destinazione), per Total target capacity (Capacità di destinazione totale), specificare il numero di unità da richiedere. Per il tipo di unità, è possibile scegliere Instances (Istanze), vCPU oppure Memory (MiB) (Memoria (MiB)).
7. Per Your fleet request at a glance (La tua richiesta immediata per il parco istanze), controllare la configurazione del tuo parco istanze e scegliere Launch (Avvia).

Creare una richiesta di parco istanze spot utilizzando parametri definiti (console)

È possibile creare un parco istanze spot utilizzando i parametri che si definiscono.

Per creare una richiesta di parco istanze spot utilizzando parametri definiti (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Se è la prima volta che viene utilizzato lo Spot, verrà visualizzata una pagina di benvenuto; selezionare Get started (Inizia). Altrimenti, selezionare Request Istanze spot (Richiedi Istanze spot).
4. Per Launch parameters (Parametri di avvio), effettuare le seguenti operazioni:

   a. Per definire i parametri di avvio nella console Spot, scegliere Manually configure launch parameters (Configura manualmente i parametri di avvio).

   b. Per l'AMI, scegli una delle AMI di base fornite da AWS oppure scegli Cerca AMI per utilizzare un'AMI della nostra comunità di utenti Marketplace AWS, o di una tua.

      > **Note**
      >
      > Se un'AMI specificata nei parametri di avvio viene annullata o disattivata, non è possibile avviare nuove istanze dall'AMI. Per le flotte impostate per mantenere la capacità target, tale capacità non verrà mantenuta.

   c. (Facoltativo) Per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o crearne una nuova.

      [Coppia di chiavi esistente] Scegliere la coppia di chiavi.

      [Nuova coppia di chiavi] Scegliere Create new key pair (Crea nuova coppia di chiavi) per accedere alla pagina Key Pairs (Coppie di chiavi). Una volta terminato, tornare alla pagina Spot Requests (Richieste Spot) e aggiornare l'elenco.

   d. (Facoltativo) Espandere Additional launch parameters (Parametri di avvio aggiuntivi) ed effettuare le seguenti operazioni.

      i. (Facoltativo) Per abilitare l'ottimizzazione Amazon EBS, per EBS-optimized (Ottimizzato per EBS), scegliere Launch EBS-optimized instances (Avvia istanze ottimizzate per EBS).

ii. (Facoltativo) Per aggiungere archiviazione a livello di blocchi temporaneo per le istanze, per Instance store, scegliere Attach at launch (Collega all'avvio).

iii. (Facoltativo) Per aggiungere archiviazione, scegli Add new volume (Aggiungi nuovo volume) e specifica volumi di archivio istanza aggiuntivi o volumi Amazon EBS, a seconda del tipo di istanza.

iv. (Facoltativo) Per impostazione predefinita, per le proprie istanze è attivo il monitoraggio base. Per abilitare il monitoraggio dettagliato, per Monitoraggio, seleziona Abilita monitoraggio CloudWatch dettagliato.

v. (Facoltativo) Per eseguire un'istanza spot dedicata, per Tenancy selezionare Dedicated - run a dedicated instance (Dedicata: esegui un'istanza dedicata).

vi. (Facoltativo) Per Security groups (Gruppi di sicurezza), scegliere uno o più gruppi di sicurezza o crearne uno nuovo.

[Gruppo di sicurezza esistente] Scegliere uno o più gruppi di sicurezza.

[Nuovo gruppo di sicurezza] Scegliere Create new security group (Crea nuovo gruppo di sicurezza) per accedere alla pagina Security Groups (Gruppi di sicurezza). Una volta terminato, tornare alla pagina Spot Requests (Richieste Spot) e aggiornare l'elenco.

vii. (Facoltativo) Per rendere le istanze raggiungibili da Internet, per Auto-assign IPv4 Public IP (Assegna IP pubblico IPv4 in modo automatico), scegliere Enable (Abilita).

viii. (Facoltativo) Per avviare le Istanze spot con un ruolo IAM, selezionare il ruolo per IAM instance profile (Profilo dell'istanza IAM).

ix. (Facoltativo) Per eseguire uno script di avvio, copiarlo su User data (Dati utente).

x. (Facoltativo) Per aggiungere un tag, scegliere Create tag (Crea tag) e inserire la chiave e il valore per il tag, quindi scegliere Create (Crea). Ripetere per ogni tag.

Per ogni tag, per assegnare alle richieste di istanze e serie di istanze spot lo stesso tag, assicurarsi che siano selezionati sia Instance (Istanza) che Fleet (parco istanze). Per assegnare tag solo alle istanze avviate dal parco istanze, deseleziona Fleet (parco istanze). Per assegnare tag solo alla richiesta della serie di istanze spot, deselezionare Instances (Istanze).

5. Per Additional request details (Dettagli richiesta aggiuntivi), procedere come segue:

a. Esaminare i dettagli aggiuntivi della richiesta. Per apportare modifiche, deselezionare Apply defaults (Applica impostazioni predefinite).

b. (Facoltativo) Per IAM fleet role (Ruolo parco istanze IAM), è possibile utilizzare il ruolo predefinito o scegliere un ruolo diverso. Per utilizzare il ruolo predefinito dopo aver modificato il ruolo, scegliere Use default role (Usa ruolo predefinito).

c. (Facoltativo) Per Maximum price (Prezzo massimo), è possibile utilizzare il prezzo massimo predefinito (il prezzo on demand) o specificare il prezzo massimo che si è disposti a pagare. Se il prezzo massimo è inferiore al prezzo Spot per i tipi di istanza che sono stati selezionati, le Istanze spot non vengono avviate.

d. (Facoltativo) Per creare una richiesta valida soltanto per un periodo di tempo specifico, modificare Request valid from (Richiesta valida da) e Request valid until (Richiesta valida fino a).

e. (Facoltativo) Per impostazione predefinita, interrompiamo le Istanze spot quando la richiesta della serie di istanze spot scade. Per tenerle in esecuzione dopo la scadenza della richiesta, deselezionare Terminate the instances when the request expires (Termina istanze alla scadenza della richiesta).

f. (Facoltativo) Per registrare le proprie Istanze Spot con un load balancer, selezionare Receive traffic from one or more load balancers (Ricevi traffico da uno o più load balancer) e scegliere uno o più Classic Load Balancer o gruppi di destinazione.

6. Per Minimum compute unit (Unità minima di elaborazione) scegliere le specifiche hardware minime (vCPU, memoria e archiviazione) necessarie per l'applicazione o l'attività, as specs (come specifiche) o as an instance type (come tipo di istanza).

   - Per as specs (come specifiche), specificare il numero richiesto di vCPU la quantità di memoria.
   - Per as an instance type (come tipo di istanza), accettare il tipo di istanza predefinito o scegliere Change instance type (Cambia tipo di istanza) per scegliere un tipo di istanza diverso.

7. In Target capacity (Capacità target), effettuare le operazioni seguenti:

   a. Per Total target capacity (Capacità di destinazione totale), specificare il numero di unità da richiedere. Per il tipo di unità, è possibile scegliere Instances (Istanze), vCPU oppure Memory (MiB) (Memoria (MiB)). Per specificare una capacità target pari a 0 per aggiungere la capacità in un secondo momento, scegliere Maintain target capacity (Mantieni capacità target).

   b. (Facoltativo) Per Include On-Demand base capacity (Includi capacità di base on demand), specificare il numero di unità on demand da richiedere. Il numero deve essere inferiore alla

Capacità obiettivo totale. Amazon EC2 calcola la differenza e la assegna alle unità Spot da richiedere.

> **Important**
>
> Per specificare una capacità on demand facoltativa, è necessario prima scegliere un modello di avvio.

c. (Facoltativo) Per impostazione predefinita, Amazon EC2 termina le istanze Spot quando vengono interrotte. Per mantenere la capacità target, selezionare Maintain target capacity (Mantieni capacità target). È quindi possibile specificare che Amazon EC2 interrompa, arresta o iberna le istanze Spot quando vengono interrotte. Per procedere in questo senso, selezionare l'opzione corrispondente da Interruption behavior (Comportamento di interruzione).

> **Note**
>
> Se un'AMI specificata nei parametri di avvio viene annullata o disattivata, non è possibile avviare nuove istanze dall'AMI. Per le flotte impostate per mantenere la capacità target, tale capacità non verrà mantenuta.

d. (Facoltativo) Per consentire alla serie di istanze spot di avviare un'istanza spot sostitutiva quando viene emessa una notifica di ribilanciamento dell'istanza per un'istanza spot esistente nel parco istanze, selezionare Capacity rebalance (Ribilanciamento capacità), quindi scegliere una strategia di sostituzione istanze. Se si sceglieLaunch before terminate (Avviare prima di terminare), specificare il ritardo (in secondi) prima che la serie di istanze spot chiuda le vecchie istanze. Per ulteriori informazioni, consulta Ribilanciamento della capacità.

e. (Facoltativo) Per controllare l'importo che paghi all'ora per tutte le istanze spot del parco istanze, seleziona Set maximum cost for Spot Instances (Imposta il costo massimo per le istanze spot) e quindi inserisci l'importo totale massimo che sei disposto a pagare all'ora. Quando viene raggiunto l'importo totale massimo, il parco istanze spot interrompe l'avvio di istanze spot, anche se non è stata raggiunta la capacità obiettivo. Per ulteriori informazioni, consulta Controllo delle spese.

8. In Network (Rete), procedere come segue:

a. (Facoltativo) Per Rete, scegliere un VPC esistente o crearne uno nuovo.

[VPC esistente] Scegliere il VPC.

[VPC nuovo] Scegliere Create new VPC (Crea nuovo VPC) per accedere alla console Amazon VPC. Una volta terminato, tornare alla procedura guidata e aggiornare l'elenco.

b. (Facoltativo) Per Availability Zone (Zona di disponibilità), l'impostazione predefinita è lasciare che AWS scelga le zone di disponibilità per le istanze spot o specificare una o più zone di disponibilità.

Se si ha più di una sottorete in una zona di disponibilità, scegliere la sottorete appropriata da Subnet (Sottorete). Per aggiungere sottoreti, scegliere Create new subnet (Crea nuova sottorete) per accedere alla console Amazon VPC. Una volta terminato, tornare alla procedura guidata e aggiornare l'elenco.

9. Per Instance type requirements (Requisiti per il tipo di istanza), puoi specificare gli attributi dell'istanza e consentire ad Amazon EC2 di identificare i tipi di istanza ottimali con questi attributi, oppure puoi specificare un elenco di istanze. Per ulteriori informazioni, consulta Selezione del tipo di istanza basata su attributi per serie di istanze spot.

a. Se si sceglie Specify instance attributes that match your compute requirements (Specifica gli attributi di istanza che corrispondono ai requisiti di calcolo), specificare gli attributi di istanza nel modo seguente:

i. Per vCPUs (vCPU) inserire il numero minimo e massimo desiderato di vCPU. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.

ii. Per Memory (GiB) (Memoria [GiB]) inserire la quantità minima e massima di memoria desiderata. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.

iii. (Facoltativo) Per Additional instance attributes (Attributi istanza aggiuntivi), facoltativamente, è possibile specificare uno o più attributi per esprimere i requisiti di calcolo in modo più dettagliato. Ogni attributo aggiuntivo aggiunge ulteriori vincoli alla tua richiesta. È possibile omettere gli attributi aggiuntivi, nel qual caso saranno utilizzati i valori di default. Per una descrizione di ogni attributo e dei relativi valori predefiniti, consulta get-spot-placement-scoresAmazon EC2 Command Line Reference.

iv. (Facoltativo) Per visualizzare i tipi di istanza con gli attributi specificati, espandere Preview matching instance types (Anteprima tipi di istanza corrispondenti). Per

escludere i tipi di istanza utilizzati nella richiesta, selezionare le istanze e quindi scegliere Exclude selected instance types (Escludi tipi di istanze selezionati).

b. Se si sceglie Manually select instance types (Seleziona manualmente i tipi di istanza), la serie di istanze spot fornisce un elenco di tipi di istanza di default. Per selezionare più tipi di istanza, scegliere Add instance types (Aggiungi tipi di istanza), selezionare i tipi di istanza da utilizzare nella tua richiesta e scegliere Select (Seleziona). Per eliminare i tipi di istanza, selezionarli e scegliere Delete (Elimina).

10. Per Allocation strategy (Strategia di allocazione), scegliere la strategia che risponde alle proprie esigenze. Per ulteriori informazioni, consulta Strategie di allocazione per istanze spot.
11. Per Your fleet request at a glance (La tua richiesta immediata per il parco istanze), rivedere la configurazione del parco istanze e, se necessario, apportare eventuali modifiche.
12. (Facoltativo) Per scaricare una copia della configurazione di avvio da utilizzare con AWS CLI, scegli JSON config.
13. Scegliere Launch (Avvia).

    Il tipo di richiesta della serie di istanze spot è `fleet`. Quando la richiesta viene soddisfatta, vengono aggiunte delle richieste di tipo `instance`, che hanno come condizione `active` e come stato `fulfilled`.

Crea una flotta Spot utilizzando il AWS CLI

Per creare una richiesta Spot Fleet utilizzando il AWS CLI

- Utilizza il request-spot-fleetcomando per creare una richiesta Spot Fleet.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Per i file di configurazione di esempio, consultare Configurazioni del parco istanze spot di esempio.

Di seguito è riportato un output di esempio:

```
{
    "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Assegnare tag a un parco istanze spot

Per categorizzare e gestire le richieste del parco istanze spot, è possibile assegnarvi tag contenenti metadati personalizzati. È possibile assegnare un tag a una richiesta di parco istanze spot alla sua creazione o successivamente. È possibile assegnare tag utilizzando la console Amazon EC2 o lo strumento da riga di comando.

Quando si assegna un tag a una richiesta del parco istanze spot, alle istanze e ai volumi che vengono avviati dal parco istanze spot non vengono automaticamente applicati tag. È necessario applicare esplicitamente tag alle istanze e ai volumi avviati dal parco istanze spot. È possibile scegliere di applicare tag solo alla richiesta del parco istanze spot o solo alle istanze avviate dal parco istanze oppure solo ai volumi collegati alle istanze avviate dal parco istanze o a tutti e tre.

> **Note**
>
> I tag associati ai volumi sono supportati solo per i volumi collegati a Istanze on demand. Non è possibile applicare tag ai volumi collegati a Istanze spot.

Per ulteriori informazioni sul funzionamento dei tag, consultare Tagging delle risorse Amazon EC2..

Indice

Prerequisito

Concedi all'utente l'autorizzazione per taggare le risorse. Per ulteriori informazioni, consulta Esempio: aggiunta di tag alle risorse.

Per concedere a un utente l'autorizzazione per taggare le risorse

Creare una policy IAM che include quanto segue:

- L'operazione `ec2:CreateTags`. Ciò concede all'utente l'autorizzazione per creare tag.

- L'operazione `ec2:RequestSpotFleet`. Ciò concede all'utente l'autorizzazione per creare una richiesta di serie di istanze spot.
- Per `Resource`, è necessario specificare `"*"`. Ciò consente agli utenti di taggare tutti i tipi di risorse.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
        }
    ]
}
```

Important

Attualmente non sono supportate le autorizzazioni a livello di risorse per la risorsa `spot-fleet-request`. Se si specifica `spot-fleet-request` come risorsa, si otterrà un'eccezione non autorizzata quando si tenta di taggare il parco istanze. Nell'esempio seguente viene mostrato come non impostare la policy.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Assegnare tag a un nuovo parco istanze spot

Per assegnare tag a una nuova richiesta di parco istanze spot utilizzando la console

1. Seguire la procedura Creare una richiesta di parco istanze spot utilizzando parametri definiti (console).
2. Per aggiungere un tag, espandere Additional configurations (Configurazioni aggiuntive), scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore per il tag. Ripetere per ogni tag.

   Per ogni tag, è possibile assegnare lo stesso tag alla richiesta del parco istanze spot e alle istanze. Per taggare entrambi, assicurarsi che siano selezionati sia i tag di istanza che i tag del parco istanze . Per assegnare tag soltanto alla richiesta del parco istanze spot, deselezionare i tag di istanza. Per taggare solo le istanze lanciate dal parco istanze, cancellare i tag del parco istanze.
3. Completare i campi obbligatori per creare una richiesta di parco istanze spot, quindi scegliere Launch (Avvia). Per ulteriori informazioni, consulta Creare una richiesta di parco istanze spot utilizzando parametri definiti (console).

Per taggare una nuova richiesta Spot Fleet utilizzando il AWS CLI

Per assegnare tag a una richiesta di parco istanze spot al momento della creazione, impostare la configurazione della richiesta di parco istanze spot nel modo seguente:

- Specificare i tag per la richiesta di serie di istanze spot in `SpotFleetRequestConfig`.
- Per `ResourceType`, specificare `spot-fleet-request`. Indicando un altro valore, la richiesta per il parco istanze fallisce.
- Per `Tags`, specificare la coppia chiave-valore. È possibile specificare più coppie chiave-valore.

Nel seguente esempio, la richiesta di parco istanze spot è taggata con due tag: Key=Environment e Value=Production, e Key=Cost-Center e Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large"
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
```

```
                    }
                ]
            }
        ]
    }
}
```

Applicare un tag a un nuovo parco istanze spot e alle istanze e ai volumi che avvia

Per etichettare una nuova richiesta Spot Fleet e le istanze e i volumi che avvia, utilizza il AWS CLI

Per applicare tag a una richiesta di parco istanze spot al momento della creazione e per applicare tag alle istanze e ai volumi quando vengono avviati dal parco istanze, impostare la configurazione della richiesta di parco istanze spot nel modo seguente:

Tag della richiesta di parco istanze spot:

- Specificare i tag per la richiesta di serie di istanze spot in `SpotFleetRequestConfig`.
- Per `ResourceType`, specificare `spot-fleet-request`. Indicando un altro valore, la richiesta per il parco istanze fallisce.
- Per `Tags`, specificare la coppia chiave-valore. È possibile specificare più coppie chiave-valore.

Tag di istanza:

- Specificare i tag per le istanze in `LaunchSpecifications`.
- Per `ResourceType`, specificare `instance`. Indicando un altro valore, la richiesta per il parco istanze fallisce.
- Per `Tags`, specificare la coppia chiave-valore. È possibile specificare più coppie chiave-valore.

  In alternativa, è possibile specificare i tag per l'istanza nel modello di avvio al quale si fa riferimento nella richiesta di parco istanze spot.

Tag associati ai volumi:

- Specificare i tag per i volumi nel modello di avvio al quale si fa riferimento nella richiesta di parco istanze spot. Il tagging del volume in `LaunchSpecifications` non è supportato.

Nel seguente esempio, la richiesta di Parco istanze spot è taggata con due tag: Key=Environment e Value=Production, e Key=Cost-Center e Value=123. Le istanze avviate dal parco istanze sono taggate con un tag (che è lo stesso di uno dei tag per la richiesta di parco istanze spot): Key=Cost-Center e Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
```

```
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Per etichettare le istanze lanciate da una flotta Spot utilizzando il AWS CLI

Per applicare tag alle istanze quando vengono avviate dal parco istanze, è possibile specificare i tag nel modello di avvio a cui si fa riferimento nella richiesta del parco istanze spot oppure specificare i tag nella configurazione della richiesta del parco istanze spot come segue:

- Specificare i tag per le istanze in `LaunchSpecifications`.
- Per `ResourceType`, specificare `instance`. Indicando un altro valore, la richiesta per il parco istanze fallisce.
- Per `Tags`, specificare la coppia chiave-valore. È possibile specificare più coppie chiave-valore.

Nell'esempio seguente, le istanze avviate dal parco istanze sono taggate con un tag: Key=Cost-Center e Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
```

```
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

Per applicare tag ai volumi collegati alle istanze on demand avviate da una serie di istanze spot utilizzando la AWS CLI

Per applicare tag ai volumi quando vengono avviati dal parco istanze, specificare i tag nel modello di avvio a cui si fa riferimento nella richiesta del parco istanze spot.

> **Note**
>
> I tag associati ai volumi sono supportati solo per i volumi collegati a Istanze on demand. Non è possibile applicare tag ai volumi collegati a Istanze spot.
> Il tagging del volume in `LaunchSpecifications` non è supportato.

Assegnazione di tag a un parco istanze spot esistente

Per assegnare tag a una richiesta di parco istanze spot esistente utilizzando la console

Dopo aver creato una richiesta di parco istanze spot, è possibile aggiungere tag alla richiesta del parco istanze utilizzando la console.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.
4. Scegliere la scheda Tags e scegliere Create Tag (Crea tag).

Per etichettare una richiesta Spot Fleet esistente utilizzando il AWS CLI

Utilizzare il seguente comando create-tags per aggiungere un tag alle risorse esistenti. Nell'esempio seguente, la richiesta di parco istanze spot esistente è taggata con Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
    --tags Key=purpose,Value=test
```

Visualizzare i tag della richiesta di parco istanze spot

Per visualizzare i tag della richiesta di parco istanze spot utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare la richiesta di parco istanze spot e scegliere la scheda Tags.

Per descrivere i tag della richiesta del parco istanze spot

Utilizzare il comando describe-tags per visualizzare i tag per la risorsa specificata. Nell'esempio seguente vengono descritti i tag per la richiesta di parco istanze spot specificata.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
```

```
}
```

Puoi visualizzare i tag di una richiesta di parco istanze spot anche descrivendo la richiesta di parco istanze spot.

Utilizza il describe-spot-fleet-requestscomando per visualizzare la configurazione della richiesta Spot Fleet specificata, che include tutti i tag specificati per la richiesta della flotta.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
```

```
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
}
```

Descrivere il parco istanze spot

Il parco istanze spot avvia le istanze spot quando il prezzo massimo supera il prezzo Spot e la capacità è disponibile. Le Istanze spot vengono eseguite fino a quando non vengono interrotte o terminate.

Per descrivere il parco istanze spot (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di Parco istanze spot. Per vedere i dettagli di configurazione, scegliere Description (Descrizione).
4. Per elencare le istanze spot per il parco istanze spot, scegliere Instances (Istanze).
5. Per visualizzare la cronologia per il parco istanze spot, scegliere History (Cronologia).

Per descrivere il parco istanze spot (AWS CLI)

Usa il describe-spot-fleet-requestscomando per descrivere le tue richieste Spot Fleet.

```
aws ec2 describe-spot-fleet-requests
```

Utilizza il describe-spot-fleet-instancescomando per descrivere le istanze Spot per il parco istanze Spot specificato.

```
aws ec2 describe-spot-fleet-instances \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Utilizza il comando describe-spot-fleet-request-history per descrivere la cronologia della richiesta Spot Fleet specificata.

```
aws ec2 describe-spot-fleet-request-history \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2015-05-18T00:00:00Z
```

Modificare una richiesta di parco istanze spot

È possibile modificare una richiesta di parco istanze spot attiva per completare le attività seguenti:

- Incremento della capacità target e della porzione on demand
- Riduzione della capacità target e della porzione on demand

> **Note**
>
> Non è possibile modificare una richiesta di parco istanze spot una tantum. È possibile modificare una richiesta di parco istanze spot solo se è stata selezionata Maintain target capacity (Mantieni capacità obiettivo) quando la richiesta è stata creata.

Quando si aumenta la capacità obiettivo, il parco istanze spot avvia istanze spot aggiuntive. Quando si incrementa la porzione on demand, il parco istanze spot avvia istanze on demand aggiuntive.

Quando aumenti la capacità target, il parco istanze Spot avvia le istanze Spot aggiuntive in base alla strategia di allocazione per la sua richiesta Spot Fleet.

Quando si diminuisce la capacità obiettivo, il parco istanze spot annulla qualsiasi richiesta aperta che supera la nuova capacità obiettivo. È possibile richiedere che il parco istanze spot termini le istanze spot finché la dimensione del parco istanze non raggiunge la nuova capacità obiettivo. Se la strategia di allocazione è `diversified`, la serie di istanze spot termina le istanze tra i pool. In alternativa, è possibile richiedere che il parco istanze spot mantenga il parco istanze alla sua dimensione attuale, ma che non sostituisca le istanze spot che vengono interrotte o tutte le istanze che vengono terminate manualmente.

Quando un parco istanze spot termina un'istanza spot a seguito della diminuzione della capacità obiettivo, l'istanza riceve un avviso di interruzione dell'istanza spot.

Per modificare una richiesta di parco istanze spot (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).

3. Seleziona la richiesta di parco istanze spot.
4. Scegliere Actions (Operazioni), quindi Modify target capacity (Modifica capacità target).
5. In Modify target capacity (Modifica capacità target), effettuare le operazioni seguenti:

    a. Immettere la nuova capacità target e la porzione on demand.

    b. (Facoltativo) Se si diminuisce la capacità target ma si desidera mantenere il parco istanze alla dimensione attuale, deselezionare Terminate instances (Termina istanze).

    c. Seleziona Submit (Invia).

Per modificare una richiesta Spot Fleet utilizzando il AWS CLI

Utilizza il modify-spot-fleet-requestcomando per aggiornare la capacità target della richiesta Spot Fleet specificata.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 20
```

È possibile modificare il comando precedente come segue per diminuire la capacità obiettivo del parco istanze spot specificata senza di conseguenza terminare le istanze spot.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

Annullare una richiesta di parco istanze spot

Se non hai più bisogno di una serie di istanze spot, puoi annullare la richiesta della serie di istanze spot. Dopo aver annullato la richiesta di un parco istanze, anche tutte le richieste di istanze spot associate al parco istanze vengono eliminate, in modo che nessuna istanza spot nuova venga avviata per tale parco.

Quando si annulla una richiesta di una serie di istanze spot, è necessario specificare se si desidera terminare tutte le relative istanze. Ciò include sia le istanze on demand che le istanze spot.

Se specifichi che le istanze devono essere terminate quando annulli la richiesta del parco istanze, quest'ultima acquisisce lo stato `cancelled_terminating`. Altrimenti, la richiesta del parco istanze

acquisisce lo stato `cancelled_running` e l'esecuzione delle istanze continua finché non viene interrotta o terminata manualmente.

Restrizioni

- Puoi eliminare fino a 100 flotte in una singola richiesta. Se si supera il numero specificato, non viene eliminato alcun parco veicoli.

Per annullare una richiesta di parco istanze spot (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.
4. Scegli Operazioni e Annulla richiesta.
5. Nella finestra di dialogo Annulla richiesta di istanze spot, esegui una delle operazioni indicate di seguito:

   a. Per terminare le istanze associate contemporaneamente all'annullamento della richiesta della serie di istanze spot, lascia selezionata la casella di controllo Termina istanze. Per annullare la richiesta della serie di istanze spot senza terminare le istanze associate, deseleziona la casella di controllo Termina istanze.

   b. Scegli Conferma.

Per annullare una richiesta Spot Fleet e terminarne le istanze, utilizza il AWS CLI

Utilizza il cancel-spot-fleet-requestscomando per annullare la richiesta Spot Fleet specificata e terminarne le istanze On-Demand e Spot.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Output di esempio

```
{
    "SuccessfulFleetRequests": [
        {
```

```
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Per annullare una richiesta di serie di istanze spot senza terminare le relative istanze utilizzando la AWS CLI

Puoi modificare il comando precedente utilizzando il parametro `--no-terminate-instances` per annullare la richiesta della serie di istanze spot specificata senza terminare le relative istanze on demand e le istanze spot.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Output di esempio

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

CloudWatch metriche per Spot Fleet

Amazon EC2 fornisce CloudWatch parametri Amazon che puoi utilizzare per monitorare la tua flotta Spot.

> **Important**
>
> Per garantire l'accuratezza, consigliamo di attivare il monitoraggio dettagliato durante l'utilizzo di tali parametri. Per ulteriori informazioni, consulta Abilitazione o disabilitazione del monitoraggio dettagliato per le istanze.

Per ulteriori informazioni sui CloudWatch parametri forniti da Amazon EC2, consulta. Monitora le tue istanze utilizzando CloudWatch

Parametri del parco istanze spot

Il `AWS/EC2Spot` namespace include le seguenti metriche, oltre alle metriche per le istanze Spot del CloudWatch tuo parco istanze. Per ulteriori informazioni, consulta Parametri dell'istanza.

Parametro	Descrizione
`AvailableInstancePoolsCount`	I pool di capacità spot specificati nella richiesta di parco istanze spot. Unità: numero
`BidsSubmittedForCapacity`	La capacità per cui Amazon EC2 ha inviato richieste di parco istanze spot. Unità: numero
`EligibleInstancePoolCount`	I pool di capacità spot specificati nella richiesta di parco istanze spot in cui Amazon EC2 può evadere le richieste . Amazon EC2 non soddisfa le richieste nei pool quando il prezzo massimo che si desidera pagare per le istanze spot è inferiore al prezzo Spot o quando il prezzo Spot è superiore al prezzo delle istanze on demand. Unità: numero
`FulfilledCapacity`	La capacità soddisfatta da Amazon EC2.

Parametro	Descrizione
	Unità: numero
`MaxPercentCapacityAllocation`	Il valore massimo di `PercentCapacityAllocation` in tutti i pool della serie di istanze spot specificati nella richiesta di serie di istanze spot. Unità: percentuale
`PendingCapacity`	La differenza tra `TargetCapacity` e `FulfilledCapacity`. Unità: numero
`PercentCapacityAllocation`	La capacità allocata per il pool di capacità spot per le dimensioni specificate. Per ottenere il valore massimo registrato in tutti i pool di capacità spot, utilizza `MaxPercentCapacityAllocation`. Unità: percentuale
`TargetCapacity`	La capacità obiettivo di una richiesta di parco istanze spot. Unità: numero
`TerminatingCapacity`	La capacità che si sta terminando perché la capacità di cui si è effettuato il provisioning supera quella di destinazione. Unità: numero

Se un'unità di misura per un parametro è `Count`, la statistica più utile è `Average`.

Dimensioni del parco istanze spot

Per filtrare i dati relativi al parco istanze spot, usa le seguenti dimensioni.

Dimensioni	Descrizione
`AvailabilityZone`	Consente di filtrare i dati per zona di disponibilità.
`FleetRequestId`	Consente di filtrare i dati in base alla richiesta di istanze spot.
`InstanceType`	Consente di filtrare i dati per tipo di istanza.

Visualizza le metriche per il tuo parco veicoli Spot CloudWatch

Puoi visualizzare le CloudWatch metriche per la tua flotta Spot utilizzando la CloudWatch console Amazon. Tali parametri vengono visualizzati come grafici di monitoraggio. Tali grafici mostrano i punti dati se il parco istanze spot è attivo.

I parametri sono raggruppati in primo luogo in base allo spazio dei nomi e in secondo luogo in base alle diverse combinazioni delle dimensioni all'interno di ciascuno spazio dei nomi. Ad esempio, è possibile visualizzare tutti i parametri del parco istanze spot o i gruppi di parametri del parco istanze spot in base all'ID richiesta del parco istanze spot, al tipo di istanza o alla zona di disponibilità.

Per visualizzare i parametri del parco istanze spot

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Scegliere lo spazio dei nomi Spot EC2.

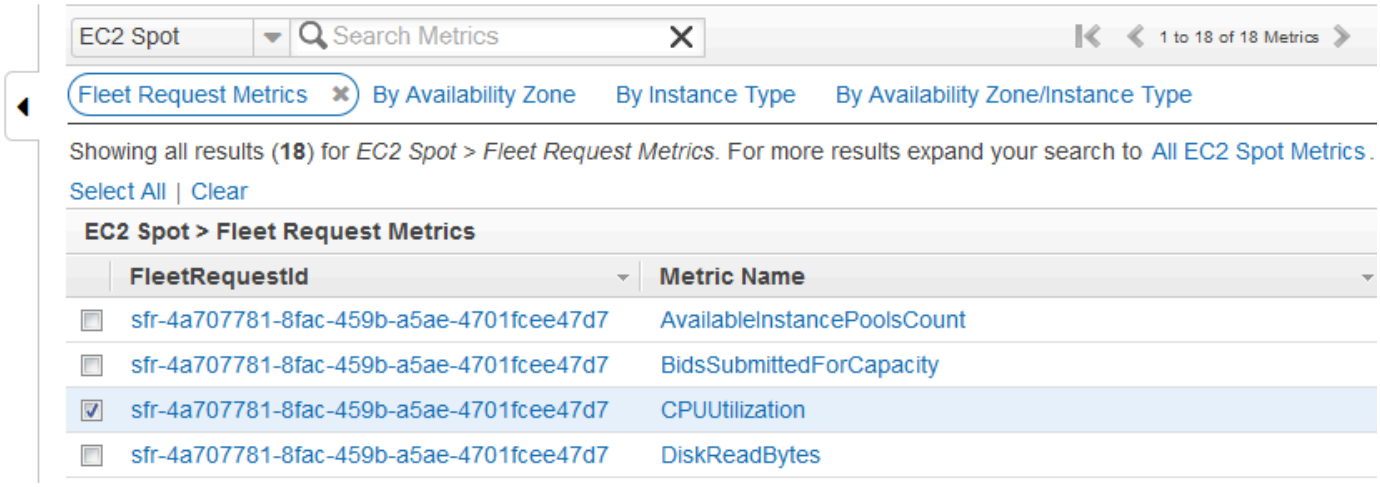
   > **Note**
   >
   > Se lo spazio dei nomi Spot EC2 non viene visualizzato, i motivi possono essere due. O non hai ancora utilizzato Spot Fleet, ma solo i AWS servizi che utilizzi inviano i parametri ad Amazon. CloudWatch Oppure, se non si è utilizzato il parco istanze spot nelle ultime due settimane, lo spazio dei nomi non viene visualizzato.

4. (Facoltativo) Per filtrare i parametri per dimensione, selezionare una delle opzioni seguenti:

   - Parametri di richiesta di parco istanze - Raggruppare per richiesta di parco istanze spot

- Per zona di disponibilità - Raggruppare per richiesta di parco istanze spot e zona di disponibilità
- Per tipo di istanza - Raggruppare per richiesta di parco istanze spot e tipo di istanza
- Per zona di disponibilità/tipo di istanza - Raggruppare per richiesta di parco istanze spot, zona di disponibilità e tipo di istanza

5. Per visualizzare i dati di un parametro, selezionare la casella di controllo accanto al parametro.



Scalabilità automatica per il parco istanze spot

La scalabilità automatica è la capacità di aumentare o diminuire automaticamente la capacità obiettivo del proprio parco istanze spot on demand. Un parco istanze spot può sia avviare le istanze sia terminarle (dimensionamento orizzontale) entro l'intervallo prescelto in risposta a uno o più policy di dimensionamento.

Il parco istanze spot supporta i seguenti tipi di scalabilità automatica:

- Target tracking scaling (Dimensionamento di monitoraggio degli obiettivi): aumenta o riduce la capacità attuale del parco istanze in base a un valore obiettivo per un parametro specifico. Questa operazione può essere paragonata al modo in cui il termostato regola la temperatura di una casa: si seleziona la temperatura e il termostato fa il resto.
- Step scaling (Dimensionamento per fasi): aumenta o diminuisce la capacità attuale del parco istanze in base a una serie di regolazioni del dimensionamento, chiamate regolazioni per fasi, che variano in base alla dimensione dell'utilizzo fuori limite segnalato dall'allarme.
- Scheduled scaling (Dimensionamento pianificato): aumenta o riduce la capacità corrente del parco istanze in base alla data e all'ora.

Se si utilizza la ponderazione delle istanze, tenere presente che il parco istanze spot può superare la capacità obiettivo in base alle necessità. La capacità soddisfatta può essere un numero a virgola mobile, ma la capacità obiettivo deve essere un numero intero, pertanto il parco istanze spot esegue l'arrotondamento fino al numero intero successivo. È necessario tenere conto di questi comportamenti quando si esamina l'esito di una policy di dimensionamento quando viene attivato un allarme. Per esempio, supponiamo che la capacità di destinazione sia 30, la capacità soddisfatta 30,1 e che la policy di dimensionamento sottragga 1. Quando si attiva l'allarme, il processo di scalabilità automatica sottrae 1 da 30,1 ottenendo 29,1, che viene arrotondato a 30, quindi non viene intrapresa alcuna operazione di dimensionamento. Come altro esempio, supponiamo di aver selezionato i pesi di istanza 2, 4 e 8 e una capacità obiettivo di 10 ma non erano disponibili istanze di peso 2, così il parco istanze spot ha fornito in provisioning istanze di peso 4 e 8 per una capacità soddisfatta di 12. Se la policy di dimensionamento riduce la capacità di destinazione del 20% e si attiva un allarme, il processo di scalabilità automatica sottrae 12 x 0,2 da 12 ottenendo 9,6, che viene arrotondato a 10, quindi non viene intrapresa alcuna operazione di dimensionamento.

Le policy di dimensionamento create per il parco istanze spot supportano un tempo di raffreddamento. Si tratta del numero di secondi dopo il completamento di un'attività di dimensionamento in cui le precedenti attività di dimensionamento correlate all'attivazione possono influenzare gli eventi di dimensionamento futuri. Per le policy di dimensionamento, mentre è attivo il periodo di attesa, la capacità aggiunta all'evento di dimensionamento precedente che ha innescato l'attesa viene calcolata come parte della capacità desiderata per il dimensionamento successivo. L'intenzione è di aumentare di continuo (ma non in eccesso). Per le policy di riduzione, il periodo di attesa viene utilizzato per bloccare le richieste di riduzione ulteriori finché non è scaduto. L'intenzione è quella di ridurre in modo conservativo per proteggere la disponibilità dell'applicazione. Tuttavia, se un altro allarme attiva una policy di dimensionamento durante il periodo di attesa dopo un ridimensionamento, la scalabilità automatica aumenta immediatamente il target scalabile.

Ti consigliamo di dimensionare in base a parametri di istanze con intervalli di 1 minuto, poiché questo garantisce una risposta più rapida alle variazioni di utilizzo. Il dimensionamento sui parametri a intervalli di 5 minuti potrebbe rallentare il tempo di risposta e causare il dimensionamento su dati di parametro obsoleti. Per inviare i dati metrici relativi alle istanze CloudWatch in periodi di 1 minuto, devi abilitare specificamente il monitoraggio dettagliato. Per ulteriori informazioni, consulta Abilitazione o disabilitazione del monitoraggio dettagliato per le istanze e Creare una richiesta di parco istanze spot utilizzando parametri definiti (console).

Per ulteriori informazioni sull'adattamento della configurazione per il parco istanze spot, consulta le risorse seguenti:

- La sezione application-autoscaling di Riferimento ai comandi AWS CLI .
- Riferimento API di Application Auto Scaling
- Application Auto Scaling User Guide

Autorizzazioni IAM richieste per la scalabilità automatica del parco istanze spot

La scalabilità automatica per Spot Fleet è resa possibile da una combinazione delle API Amazon EC2, CloudWatch Amazon e Application Auto Scaling. Le richieste Spot Fleet vengono create con Amazon EC2, gli allarmi vengono creati e le politiche di scalabilità vengono create con CloudWatch Application Auto Scaling.

In aggiunta alle autorizzazioni IAM per una serie di istanze spot e ad Amazon EC2, l'utente che accede alle impostazioni di dimensionamento del parco istanze deve avere le autorizzazioni appropriate per i servizi che supportano il dimensionamento dinamico. Gli utenti devono avere l'autorizzazione per utilizzare le operazioni nella seguente policy di esempio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Puoi anche creare le tue policy IAM che consentono autorizzazioni più granulari per chiamate alle API Application Auto Scaling. Per ulteriori informazioni, consulta Autenticazione e controllo degli accessi nella Guida per l'utente di Application Auto Scaling.

Il servizio Application Auto Scaling necessita inoltre dell'autorizzazione per descrivere la tua flotta Spot e gli CloudWatch allarmi e delle autorizzazioni per modificare la capacità target della tua flotta Spot per tuo conto. Se abiliti il dimensionamento automatico per la serie di istanze spot, viene creato un ruolo collegato ai servizi denominato `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest`. Questo ruolo concede a Application Auto Scaling l'autorizzazione per descrivere gli allarmi per le policy, per monitorare la capacità attuale del parco istanze e modificare la capacità del parco istanze. Il ruolo originale della serie di istanze spot gestito per Application Auto Scaling era `aws-ec2-spot-fleet-autoscale-role`, ma non è più richiesto. Il ruolo collegato al servizio è il ruolo predefinito per Application Auto Scaling. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di Application Auto Scaling.

Dimensionare il parco istanze spot utilizzando una policy di monitoraggio degli obiettivi

Con le policy di dimensionamento con monitoraggio degli obiettivi, puoi scegliere un parametro e impostare un valore obiettivo. Spot Fleet crea e gestisce gli CloudWatch allarmi che attivano la politica di scalabilità e calcola l'aggiustamento della scalabilità in base alla metrica e al valore target. La policy di dimensionamento aggiunge o rimuove la capacità in base alle necessità, per mantenere il parametro al valore di destinazione specificato o vicino a esso. Oltre a mantenere il parametro vicino al valore di destinazione, una policy di dimensionamento di monitoraggio dei target si adatta anche alle fluttuazioni del parametro dovute a un modello di carico fluttuante e riduce al minimo le fluttuazioni rapide nella capacità del parco istanze.

È possibile creare più policy di dimensionamento con monitoraggio degli obiettivi per un parco istanze spot, purché ciascuna di esse utilizzi parametri diversi. Il parco istanze si dimensiona in base alla policy che fornisce la capacità di parco istanze più ampia. Ciò ti permette di coprire più scenari e assicurarti che vi sia sempre una capacità sufficiente per elaborare i carichi di lavoro delle applicazioni.

Per garantire la disponibilità delle applicazioni, il parco istanze aumenta in proporzione al parametro il più veloce possibile, ma si riduce in modo più graduale.

Quando un parco istanze spot termina un'istanza spot a seguito della diminuzione della capacità obiettivo, l'istanza riceve un avviso di interruzione dell'istanza spot.

Non modificare o eliminare gli CloudWatch allarmi gestiti da Spot Fleet per una politica di scalabilità di tracciamento degli obiettivi. Il parco istanze spot elimina gli allarmi automaticamente quando elimini la policy di dimensionamento con monitoraggio degli obiettivi.

Limitazione

La richiesta della serie di istanze spot deve avere un tipo di richiesta di `maintain`. La scalabilità automatica non è supportata per le richieste del tipo `request`.

Per configurare una policy di monitoraggio dei target (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare la richiesta del parco istanze spot e scegliere Auto Scaling.
4. Se la scalabilità automatica non è configurata, selezionare Configure (Configurare).
5. Utilizzare Scale capacity between (Dimensionare capacità tra) per impostare la capacità minima e massima per il parco istanze. La scalabilità automatica non dimensiona il parco istanze al di sotto della capacità minima o al di sopra della capacità massima.
6. In Policy name (Nome policy), immettere un nome per la policy.
7. Selezionare un Target metric (Parametro di destinazione).
8. Immettere un Target value (Valore di destinazione) per il parametro.
9. Per il tempo di raffreddamento, specifica un nuovo valore (in secondi) o mantieni il valore predefinito.
10. (Facoltativo) Selezionare Disable scale-in (Disattiva dimensionamento) per omettere la creazione di una policy di ridimensionamento in base alla configurazione attuale. È possibile creare una policy di dimensionamento utilizzando una configurazione diversa.
11. Scegliere Save (Salva).

Per configurare una politica di tracciamento degli obiettivi utilizzando il AWS CLI

1. Registra la richiesta Spot Fleet come target scalabile utilizzando il register-scalable-targetcomando.
2. Crea una politica di scalabilità utilizzando il put-scaling-policycomando.

Dimensionare il parco istanze spot utilizzando le policy di dimensionamento a fasi

Con le politiche di scalabilità graduale, si specificano gli CloudWatch allarmi per attivare il processo di ridimensionamento. Per esempio, se si vuole aumentare quando l'utilizzo della CPU raggiunge un determinato livello, creare un allarme utilizzando il parametro `CPUUtilization` fornito da Amazon EC2.

Quando si crea una policy di dimensionamento a fasi, bisogna specificare uno dei seguenti tipi di adeguamento dimensionamento:

- Add (Aggiungi) – Aumenta la capacità obiettivo del parco istanze di un numero specifico di unità di capacità o di una percentuale specifica della capacità attuale.
- Remove (Rimuovi) – Diminuisce la capacità obiettivo del parco istanze di un numero specifico di unità di capacità o di una percentuale specifica della capacità attuale.
- Set to (Imposta su) – Imposta la capacità obiettivo del parco istanze sul numero di unità di capacità specificato.

Quando viene innescato un allarme, il processo di scalabilità automatica calcola la nuova capacità target utilizzando la capacità soddisfatta e la policy di dimensionamento, quindi aggiorna la capacità target di conseguenza. Per esempio, supponiamo che la capacità di destinazione e quella soddisfatta siano 10 e che la policy di dimensionamento aggiunga 1. Quando si attiva l'allarme, il processo di scalabilità automatica aggiunge 1 a 10 per ottenere 11, quindi il parco istanze spot avvia 1 istanza.

Quando un Parco istanze spot termina un'istanza spot a seguito della diminuzione della capacità obiettivo, l'istanza riceve un avviso di interruzione dell'istanza spot.

Limitazione

La richiesta della serie di istanze spot deve avere un tipo di richiesta di `maintain`. La scalabilità automatica non è supportata per le richieste del tipo `request` o i blocchi Spot.

Prerequisiti

- Considerate quali CloudWatch metriche sono importanti per la vostra applicazione. Puoi creare CloudWatch allarmi in base a metriche fornite da AWS o a metriche personalizzate.
- Per le AWS metriche che utilizzerai nelle tue politiche di scalabilità, abilita la raccolta delle CloudWatch metriche se il servizio che fornisce le metriche non la abilita per impostazione predefinita.

Per creare un allarme CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, seleziona Alarms (Allarmi).
3. Selezionare Create Alarm (Crea allarme).
4. Nella pagina Specify metric and conditions (Specifica parametro e condizioni), scegliere Select metric (Seleziona parametro).
5. Scegli EC2 Spot, Fleet Request Metrics, seleziona una metrica (ad esempio TargetCapacity), quindi scegli Seleziona metrica.

   Viene visualizzata la pagina Specify metric and conditions (Specifica parametro e condizioni) contenente un grafico e altre informazioni sul parametro selezionato.
6. In Period (Periodo), scegliere il periodo di valutazione per l'allarme, ad esempio 1 minuto. Durante la valutazione dell'allarme, ogni periodo è aggregato in un punto dati.

   > **Note**
   >
   > Un periodo più breve crea un allarme più sensibile.
7. In Conditions (Condizioni), definire l'allarme specificando la condizione di soglia. Ad esempio, è possibile definire una soglia per attivare l'allarme ogni volta che il valore del parametro è maggiore o uguale all'80%.
8. In Additional configuration (Configurazione aggiuntiva), per Datapoints to alarm (Punto di dati per allarme), specificare il numero di punti di dati (periodi di valutazione) che devono trovarsi nello stato ALLARME per attivare l'allarme, ad esempio, 1 periodo di valutazione su 2 di 3 periodi di valutazione. Questo consente di creare un allarme che passa allo stato ALARM se si verifica un superamento durante tali periodi consecutivi. Per ulteriori informazioni, consulta Evaluating an alarm nella Amazon CloudWatch User Guide.
9. Per Missing data treatment (Trattamento dati mancanti), selezionare una delle opzioni (o lasciare il valore di default di Treat missing data as missing (Tratta i dati mancanti come mancanti)). Per ulteriori informazioni, consulta Configurazione del modo in cui gli CloudWatch allarmi trattano i dati mancanti nella Amazon CloudWatch User Guide.
10. Seleziona Successivo.
11. (Facoltativo) Per ricevere la notifica di un evento di dimensionamento, per Notification (Notifica), è possibile scegliere o creare l'argomento Amazon SNS da utilizzare per ricevere notifiche.

Altrimenti, è possibile eliminare ora le notifiche e aggiungerne una in un secondo momento ove necessario.

12. Seleziona Successivo.
13. In Add a description (Aggiungere una descrizione), immettere un nome e una descrizione per l'allarme e scegliere Next (Successivo).
14. Selezionare Create Alarm (Crea allarme).

Per configurare una policy di dimensionamento per fasi per il parco istanze spot (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare la richiesta del parco istanze spot e scegliere Auto Scaling.
4. Se la scalabilità automatica non è configurata, selezionare Configure (Configurare).
5. Utilizzare Scale capacity between (Dimensionare capacità tra) per impostare la capacità minima e massima per il parco istanze. Le policy di dimensionamento non dimensionano il parco istanze al di sotto della capacità minima o al di sopra della capacità massima.
6. In Policy di dimensionamento, Tipo di policy scegli Policy di dimensionamento a fasi.
7. Inizialmente, le Policy di dimensionamento contengono policy di dimensionamento a fasi denominate ScaleUp e ScaleDown. È possibile completare tali policy o selezionare Remove policy (Rimuovi policy) per eliminarle. È possibile anche scegliere Add policy (Aggiungi policy).
8. Per definire una policy, effettuare le operazioni seguenti:

    a. In Policy name (Nome policy), immettere un nome per la policy.

    b. Per Policy trigger, seleziona un allarme esistente o scegli Crea allarme per aprire la CloudWatch console Amazon e creare un allarme.

    c. Per Modifica capacità, definisci la quantità in base alla quale dimensionare e il limite inferiore e superiore della regolazione del livello. È possibile aggiungere o rimuovere un numero specifico di istanze o una percentuale della dimensione del parco istanze esistente, oppure impostare il parco istanze su una dimensione specifica.

    Ad esempio, per creare una policy di dimensionamento graduale che aumenti la capacità del parco istanze del 30 percento, scegli `Add`, digita `30` nel campo successivo e quindi scegli `percent`. Per impostazione predefinita, il limite inferiore per una policy di aggiunta è la soglia di allarme e il limite superiore è positivo (+) infinito. Per impostazione predefinita,

il limite superiore per una policy di rimozione è la soglia di allarme e il limite inferiore è negativo (-) infinito.

d. (Facoltativo) Per aggiungere un'altra fase, seleziona Aggiungi fase.

e. Per il tempo di raffreddamento, specifica un nuovo valore (in secondi) o mantieni il valore predefinito.

9. Selezionare Salva.

Per configurare le politiche di scalabilità graduale per la tua flotta Spot, utilizza il AWS CLI

1. Registra la richiesta Spot Fleet come target scalabile utilizzando il register-scalable-targetcomando.
2. Crea una politica di scalabilità utilizzando il put-scaling-policycomando.
3. Crea un allarme che attiva la politica di ridimensionamento utilizzando il comando. put-metric-alarm

Dimensionare il parco istanze spot utilizzando il dimensionamento pianificato

Il dimensionamento basato su una pianificazione consente di dimensionare le applicazioni in relazione alle variazioni di domanda prevedibili. Per utilizzare il dimensionamento pianificato, è possibile creare operazioni pianificate che indicano al parco istanze spot di eseguire attività di dimensionamento a orari specifici. Al momento della creazione di un'operazione pianificata, è necessario specificare un parco istanze spot esistente, quando l'attività di dimensionamento dovrà verificarsi, la capacità minima e la capacità massima. È possibile creare operazioni pianificate una tantum oppure ricorrenti.

È possibile creare operazioni pianificate solo per la Parchi istanze spot che già esiste. Non è possibile creare operazioni pianificate contemporaneamente alla creazione di un parco istanze spot.

Limitazione

La richiesta della serie di istanze spot deve avere un tipo di richiesta di `maintain`. La scalabilità automatica non è supportata per le richieste del tipo `request` o i blocchi Spot.

Per creare un'operazione pianificata una tantum

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).

3. Selezionare la richiesta del parco istanze spot e scegliere la scheda Scheduled Scaling (Dimensionamento pianificato) nella parte inferiore dello schermo.
4. Scegliere Create Scheduled Action (Crea operazione pianificata).
5. In Name (Nome), specificare un nome per l'operazione pianificata.
6. Immettere un valore per Minimum capacity (Capacità minima), Maximum capacity (Capacità massima) o per entrambi i campi.
7. Per Recurrence (Ricorrenza), scegliere Once (Una tantum).
8. (Facoltativo) Scegliere una data e un'ora per Start time (Ora di inizio), End time (Ora di fine) o per entrambi i campi.
9. Seleziona Submit (Invia).

Per eseguire il dimensionamento in base a una pianificazione ricorrente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare la richiesta del Parco istanze spot e scegliere la scheda Scheduled Scaling (Dimensionamento pianificato) nella parte inferiore dello schermo.
4. Per Recurrence (Ricorrenza), scegliere uno dei piani predefiniti (ad esempio, Every day (Ogni giorno)), oppure scegliere Custom (Personalizzato) e immettere un'espressione cron. Per ulteriori informazioni sulle espressioni cron supportate dalla scalabilità pianificata, consulta Cron Expressions nella Amazon CloudWatch Events User Guide.
5. (Facoltativo) Scegliere una data e un'ora per Start time (Ora di inizio), End time (Ora di fine) o per entrambi i campi.
6. Seleziona Submit (Invia).

Per modificare un'operazione pianificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare la richiesta del Parco istanze spot e scegliere la scheda Scheduled Scaling (Dimensionamento pianificato) nella parte inferiore dello schermo.
4. Selezionare l'operazione pianificata e scegliere Actions (Operazioni), Edit (Modifica).
5. Apportare le modifiche necessarie e scegliere Invia.

Per eliminare un'operazione pianificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare la richiesta del Parco istanze spot e scegliere la scheda Scheduled Scaling (Dimensionamento pianificato) nella parte inferiore dello schermo.
4. Selezionare l'operazione pianificata e scegliere Actions (Operazioni), Elimina.
5. Quando viene richiesta la conferma, seleziona Elimina.

Per gestire il ridimensionamento pianificato utilizzando AWS CLI

Utilizza il seguente comando:

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

Monitora gli eventi della flotta utilizzando Amazon EventBridge

Quando lo stato di un parco istanze EC2 o del parco istanze spot viene modificato, il parco istanze emette una notifica. La notifica viene resa disponibile come evento inviato ad Amazon EventBridge (precedentemente noto come Amazon CloudWatch Events). Gli eventi vengono emessi secondo il principio del massimo sforzo.

Con Amazon EventBridge, puoi creare regole che attivano azioni programmatiche in risposta a un evento. Ad esempio, puoi creare due EventBridge regole, una che viene attivata quando lo stato di una flotta cambia e l'altra che viene attivata quando un'istanza del parco veicoli viene terminata. Se lo stato del parco istanze cambia, puoi configurare la prima regola in modo che richiami un argomento SNS per inviare una notifica via e-mail. Se un'istanza viene terminata, puoi configurare la seconda regola in modo che richiami una funzione Lambda per avviare una nuova istanza.

Argomenti

- Tipi di eventi parco istanze EC2
- Tipi di eventi del parco istanze spot
- Crea EventBridge regole Amazon

Tipi di eventi parco istanze EC2

> **Note**
>
> Solo flotte di tipo `maintain` ed `request` emettono eventi. I parchi istanze del tipo `instant` non emettono eventi perché inviano richieste sincrone una tantum e lo stato del parco istanze è noto immediatamente nella risposta.

Esistono cinque tipi di eventi parco istanze EC2. Per ogni tipo di evento, ci sono diversi sottotipi.

Gli eventi vengono inviati EventBridge in formato JSON. I campi riportati di seguito nell'evento costituiscono il modello di evento definito nella regola e che attivano un'operazione:

`"source": "aws.ec2fleet"`

Identifica che l'evento proviene da parco istanze EC2.

`"detail-type": "EC2 Fleet State Change"`

Identifica il tipo di evento.

`"detail": { "sub-type": "submitted" }`

Identifica il sottotipo di evento.

Tipi di eventi

- Cambiamento di stato del parco istanze EC2
- Richiesta di modifica dell'istanza spot del parco istanze EC2
- Modifica dell'istanza del parco istanze EC2
- Informazioni sul parco istanze EC2
- Errore parco istanze EC2

Cambiamento di stato del parco istanze EC2

EC2 Fleet invia un `EC2 Fleet State Change` evento ad Amazon EventBridge quando un parco veicoli EC2 cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

I valori possibili per `sub-type` sono:

`active`

La richiesta parco istanze EC2 è stata convalidata ed Amazon EC2 sta tentando di mantenere il numero previsto di istanze in esecuzione.

`deleted`

Il parco istanze EC2 viene eliminato e non ha istanze in esecuzione. La richiesta parco istanze EC2 viene eliminata due giorni dopo e le sue istanze vengono terminate.

`deleted_running`

La richiesta Parco istanze EC2 viene eliminata e non avvia istanze aggiuntive. Le sue istanze esistenti continuano a essere eseguite finché non vengono interrotte o terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono interrotte o terminate.

`deleted_terminating`

La richiesta del parco istanze EC2 viene eliminata e le sue istanze vengono terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono terminate.

`expired`

La richiesta parco istanze EC2 è scaduta. Se la richiesta è stata creata con un set `TerminateInstancesWithExpiration`, un evento successivo `terminated` indica che le istanze sono terminate.

`modify_in_progress`

La richiesta parco istanze EC2 è in fase di modifica. La richiesta rimane in questo stato finché la modifica non viene completamente elaborata.

`modify_succeeded`

La richiesta parco istanze EC2 è stata modificata.

`submitted`

La richiesta parco istanze EC2 è in fase di valutazione ed Amazon EC2 si sta preparando ad avviare il numero previsto di istanze.

`progress`

La richiesta parco istanze EC2 è in procinto di essere soddisfatta.

Richiesta di modifica dell'istanza spot del parco istanze EC2

EC2 Fleet invia un `EC2 Fleet Spot Instance Request Change` evento ad Amazon EventBridge quando una richiesta di istanza Spot nel parco veicoli cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
```

```
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

I valori possibili per `sub-type` sono:

`active`

La richiesta è stata soddisfatta e ha un'istanza spot associata.

`cancelled`

Hai annullato la richiesta dell'istanza spot o la richiesta dell'istanza spot è scaduta.

`disabled`

Hai arrestato l'istanza spot.

`submitted`

La richiesta dell'istanza spot viene inviata.

Modifica dell'istanza del parco istanze EC2

EC2 Fleet invia un `EC2 Fleet Instance Change` evento ad Amazon EventBridge quando un'istanza nel parco veicoli cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
```

```
        "instance-id": "i-0c594155dd5ff1829",
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
    }
}
```

I valori possibili per `sub-type` sono:

`launched`

È stata lanciata una nuova istanza.

`terminated`

L'istanza è stata terminata.

`termination_notified`

Una notifica di terminazione dell'istanza è stata inviata quando un'istanza spot è stata terminata da Amazon EC2 durante la riduzione orizzontale, quando la capacità target del parco istanze è stata modificata, ad esempio, da una capacità target di 4 a una capacità target di 3.

Informazioni sul parco istanze EC2

EC2 Fleet invia un `EC2 Fleet Information` evento ad Amazon EventBridge in caso di errore durante l'adempimento. L'evento informativo non impedisce al parco istanze di tentare di raggiungere la sua capacità target.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
```

```
    "detail": {
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
        "sub-type": "launchSpecUnusable"
    }
}
```

I valori possibili per `sub-type` sono:

`fleetProgressHalted`

Il prezzo in ogni specifica di avvio non è valido perché è inferiore al prezzo istanza spot (tutte le specifiche di avvio hanno prodotto eventi `launchSpecUnusable`). Una specifica di avvio potrebbe diventare valida se il prezzo Spot cambia.

`launchSpecTemporarilyBlacklisted`

La configurazione non è valida e vari tentativi di avvio delle istanze non sono riusciti. Per ulteriori informazioni, consultare la descrizione dell'evento.

`launchSpecUnusable`

Il prezzo in una specifica di avvio non è valido perché è inferiore al prezzo istanza spot o il prezzo istanza spot è inferiore al prezzo on demand.

`registerWithLoadBalancersFailed`

Tentativo di registrazione di istanze con bilanciamento del carico non riuscito. Per ulteriori informazioni, consultare la descrizione dell'evento.

Errore parco istanze EC2

EC2 Fleet invia un `EC2 Fleet Error` evento ad Amazon EventBridge in caso di errore durante l'adempimento. L'evento di errore impedisce al parco istanze di tentare di raggiungere la sua capacità target.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
```

```
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not
 supported for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

I valori possibili per `sub-type` sono:

`iamFleetRoleInvalid`

Il parco istanze EC2 non include le autorizzazioni necessarie per avviare o terminare un'istanza.

`allLaunchSpecsTemporarilyBlacklisted`

Nessuna delle configurazioni è valida e vari tentativi di avvio delle istanze non sono riusciti. Per ulteriori informazioni, consultare la descrizione dell'evento.

`spotInstanceCountLimitExceeded`

Hai raggiunto il limite del numero di istanze spot che puoi avviare.

`spotFleetRequestConfigurationInvalid`

La configurazione non è valida. Per ulteriori informazioni, consultare la descrizione dell'evento.

Tipi di eventi del parco istanze spot

Esistono cinque tipi di eventi del parco istanze spot Per ogni tipo di evento, ci sono diversi sottotipi.

Gli eventi vengono inviati EventBridge in formato JSON. I campi riportati di seguito nell'evento costituiscono il modello di evento definito nella regola e che attivano un'operazione:

`"source": "aws.ec2spotfleet"`

Identifica che l'evento proviene da un parco istanze spot.

`"detail-type": "EC2 Spot Fleet State Change"`

Identifica il tipo di evento.

`"detail": { "sub-type": "submitted" }`

Identifica il sottotipo di evento.

Tipi di eventi

- Cambiamento dello stato del parco istanze spot di EC2
- Modifica della richiesta del parco istanze spot EC2
- Modifica dell'istanza del parco istanze spot di EC2
- Informazioni sul parco istanze spot di EC2
- Errore del parco istanze spot EC2

Cambiamento dello stato del parco istanze spot di EC2

Spot Fleet invia un `EC2 Spot Fleet State Change` evento ad Amazon EventBridge quando una flotta Spot cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
    "detail": {
        "sub-type": "submitted"
    }
}
```

I valori possibili per `sub-type` sono:

`active`

La richiesta del parco istanze spot è stata convalidata e Amazon EC2 sta tentando di mantenere il numero previsto di istanze in esecuzione.

`cancelled`

La richiesta del parco istanze spot viene annullata e non contiene istanze in esecuzione. Il parco istanze spot verrà eliminato due giorni dopo la chiusura delle istanze.

`cancelled_running`

La richiesta del parco istanze spot viene annullata e non avvia istanze aggiuntive. Le sue istanze esistenti continuano a essere eseguite finché non vengono interrotte o terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono interrotte o terminate.

`cancelled_terminating`

La richiesta del parco istanze spot viene annullata e le sue istanze sono in terminazione. La richiesta rimane in questo stato finché tutte le istanze non vengono terminate.

`expired`

La richiesta del parco istanze spot è scaduta. Se la richiesta è stata creata con un set `TerminateInstancesWithExpiration`, un evento successivo `terminated` indica che le istanze sono terminate.

`modify_in_progress`

La richiesta del parco istanze spot è in fase di modifica. La richiesta rimane in questo stato finché la modifica non viene completamente elaborata.

`modify_succeeded`

La richiesta del parco istanze spot è stata modificata.

`submitted`

La richiesta del parco istanze spot è in fase di valutazione e Amazon EC2 si sta preparando ad avviare il numero previsto di istanze.

`progress`

La richiesta del parco istanze spot sta per essere evasa.

Modifica della richiesta del parco istanze spot EC2

Spot Fleet invia un `EC2 Spot Fleet Spot Instance Request Change` evento ad Amazon EventBridge quando una richiesta di istanza Spot nel parco veicoli cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

I valori possibili per `sub-type` sono:

`active`

La richiesta è stata soddisfatta e ha un'istanza spot associata.

`cancelled`

Hai annullato la richiesta dell'istanza spot o la richiesta dell'istanza spot è scaduta.

`disabled`

Hai arrestato l'istanza spot.

`submitted`

La richiesta dell'istanza spot viene inviata.

Modifica dell'istanza del parco istanze spot di EC2

Spot Fleet invia un `EC2 Spot Fleet Instance Change` evento ad Amazon EventBridge quando un'istanza del parco veicoli cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":
\"ami-032930428bf1abbff\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":
\"us-east-1a\"}",
        "sub-type": "launched"
    }
}
```

I valori possibili per `sub-type` sono:

`launched`

È stata lanciata una nuova istanza.

`terminated`

L'istanza è stata terminata.

`termination_notified`

Una notifica di terminazione dell'istanza è stata inviata quando un'istanza spot è stata terminata da Amazon EC2 durante la riduzione orizzontale, quando la capacità target del parco istanze è stata modificata, ad esempio, da una capacità target di 4 a una capacità target di 3.

Informazioni sul parco istanze spot di EC2

Spot Fleet invia un `EC2 Spot Fleet Information` evento ad Amazon EventBridge in caso di errore durante l'adempimento. L'evento informativo non impedisce al parco istanze di tentare di raggiungere la sua capacità target.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot
 bid price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
}
```

I valori possibili per `sub-type` sono:

`fleetProgressHalted`

Il prezzo in ogni specifica di avvio non è valido perché è inferiore al prezzo istanza spot (tutte le specifiche di avvio hanno prodotto eventi `launchSpecUnusable`). Una specifica di avvio potrebbe diventare valida se il prezzo Spot cambia.

`launchSpecTemporarilyBlacklisted`

La configurazione non è valida e vari tentativi di avvio delle istanze non sono riusciti. Per ulteriori informazioni, consultare la descrizione dell'evento.

`launchSpecUnusable`

Il prezzo in una specifica di avvio non è valido perché è inferiore al prezzo istanza spot o il prezzo istanza spot è inferiore al prezzo on demand.

`registerWithLoadBalancersFailed`

Tentativo di registrazione di istanze con bilanciamento del carico non riuscito. Per ulteriori informazioni, consultare la descrizione dell'evento.

Errore del parco istanze spot EC2

Spot Fleet invia un `EC2 Spot Fleet Error` evento ad Amazon EventBridge in caso di errore durante l'adempimento. L'evento di errore impedisce al parco istanze di tentare di raggiungere la sua capacità target.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface
 with DeviceIndex 0. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

I valori possibili per `sub-type` sono:

`iamFleetRoleInvalid`

La serie di istanze spot non include le autorizzazioni necessarie per avviare o terminare un'istanza.

`allLaunchSpecsTemporarilyBlacklisted`

Nessuna delle configurazioni è valida e vari tentativi di avvio delle istanze non sono riusciti. Per ulteriori informazioni, consultare la descrizione dell'evento.

`spotInstanceCountLimitExceeded`

Hai raggiunto il limite del numero di istanze spot che puoi avviare.

`spotFleetRequestConfigurationInvalid`

La configurazione non è valida. Per ulteriori informazioni, consultare la descrizione dell'evento.

Crea EventBridge regole Amazon

Quando viene emessa una notifica di modifica dello stato per una flotta EC2 o una flotta Spot, l'evento relativo alla notifica viene inviato ad Amazon. EventBridge Se EventBridge rileva uno schema di evento che corrisponde a uno schema definito in una regola, EventBridge richiama uno o più obiettivi specificati nella regola.

È possibile scrivere una EventBridge regola e automatizzare le azioni da intraprendere quando il modello di evento corrisponde alla regola.

Argomenti

- Crea EventBridge regole Amazon per monitorare gli eventi della flotta EC2
- Crea EventBridge regole Amazon per monitorare gli eventi della flotta Spot

Crea EventBridge regole Amazon per monitorare gli eventi della flotta EC2

Quando viene emessa una notifica di modifica dello stato per una flotta EC2, l'evento relativo alla notifica viene inviato ad Amazon EventBridge sotto forma di file JSON. Puoi scrivere una EventBridge regola per automatizzare le azioni da intraprendere quando un pattern di eventi corrisponde alla regola. Se EventBridge rileva un pattern di eventi che corrisponde a uno schema definito in una regola, EventBridge richiama l'obiettivo (o i target) specificati nella regola.

I campi seguenti costituiscono il modello di evento definito nella regola:

`"source": "aws.ec2fleet"`

Identifica che l'evento proviene da Parco istanze EC2.

`"detail-type": "EC2 Fleet State Change"`

Identifica il tipo di evento.

`"detail": { "sub-type": "submitted" }`

Identifica il sottotipo di evento.

Per l'elenco degli eventi del parco istanze EC2 e dei dati relativi agli eventi di esempio, consulta the section called “Tipi di eventi parco istanze EC2”.

Esempi

- Crea una EventBridge regola per inviare una notifica
- Crea una EventBridge regola per attivare una funzione Lambda

Crea una EventBridge regola per inviare una notifica

L'esempio seguente crea una EventBridge regola per inviare un'e-mail, un messaggio di testo o una notifica push mobile ogni volta che Amazon EC2 emette una notifica di modifica dello stato della flotta EC2. Il segnale in questo esempio viene emesso come evento `EC2 Fleet State Change`, che attiva l'azione definita dalla regola.

Prima di creare la EventBridge regola, devi creare l'argomento Amazon SNS per l'e-mail, il messaggio di testo o la notifica push per dispositivi mobili.

Per creare una EventBridge regola per inviare una notifica quando lo stato di una flotta EC2 cambia

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.
3. Per Define rule detail (Definisci dettagli della regola), effettua le seguenti operazioni:
   a. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.

      Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso bus di eventi.
   b. Per Event bus (Bus di eventi), scegli default. Quando un servizio AWS nell'account genera un evento, passa sempre al bus di eventi di default dell'account.
   c. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).

d. Seleziona Successivo.

4. Per Build event pattern (Crea modello di eventi), procedi come segue:

   a. Per Event source, scegli AWS eventi o eventi EventBridge partner.

   b. Per Event pattern (Modello di eventi), ai fini di questo esempio specificherai il seguente modello di eventi in modo che corrisponda all'evento `EC2 Fleet Instance Change`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"]
}
```

      Per aggiungere il modello di eventi, puoi utilizzare un modello scegliendo Event pattern form (Formato del modello di eventi) o specificare il tuo modello scegliendo Custom pattern (JSON editor) (Modello personalizzato (editor JSON)), come segue:

      i. Per utilizzare un modello per creare il modello di eventi, procedi come segue:

         A. Scegli Event pattern form (Formato del modello di eventi).

         B. Per Event source (Origine evento), scegli AWS services (Servizi).

         C. In AWS Service, scegli parco istanze EC2.

         D. Per Event type (Tipo di evento), scegli EC2 Fleet Instance Change (Modifica dell'istanza del parco istanze EC2).

         E. Per personalizzare il modello, scegli Edit pattern (Modifica modello) e apporta le modifiche in modo che corrisponda al modello di eventi di esempio.

      ii. (Alternativa) Per specificare un modello di eventi personalizzato, procedi come segue:

         A. Scegli Custom pattern (JSON editor) (Modello personalizzato (editor JSON)).

         B. Nella casella Event pattern (Modello di eventi), aggiungi il modello di eventi per questo esempio.

   c. Seleziona Successivo.

5. Per Select target(s) (Seleziona destinazione/i), esegui queste operazioni:

   a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).

b. Per Select a target (Seleziona una destinazione, scegli SNS topic (Argomento SNS) per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando si verifica l'evento.

c. Per Argomento, scegliere un argomento esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) nella Amazon Simple Notification Service Developer Guide.

d. (Facoltativo) In Additional settings (Impostazioni aggiuntive), facoltativamente puoi configurare impostazioni aggiuntive. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi (passaggio 16) nella Amazon EventBridge User Guide.

e. Seleziona Successivo.

6. (Opzionale) Per Tags (Tag), se desideri puoi assegnare uno o più tag alla regola, quindi scegli Next (Successivo).
7. Per Review and create (Verifica e crea), procedi come segue:

a. Verifica i dettagli della regola e modificali se necessario.

b. Scegli Crea regola.

Per ulteriori informazioni, consulta EventBridge le regole di Amazon e i modelli di EventBridge eventi di Amazon nella Amazon EventBridge User Guide

Crea una EventBridge regola per attivare una funzione Lambda

L'esempio seguente crea una EventBridge regola per attivare una funzione Lambda ogni volta che Amazon EC2 emette una notifica di modifica dell'istanza EC2 Fleet per l'avvio di un'istanza. Il segnale in questo esempio viene emesso come evento `EC2 Fleet Instance Change`, sottotipo `launched`, che attiva l'azione definita dalla regola.

Prima di creare la EventBridge regola, è necessario creare la funzione Lambda.

Per creare la funzione Lambda da utilizzare nella regola EventBridge

1. Apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Selezionare Create function (Crea funzione).
3. Immettere un nome per la funzione, configurare il codice, quindi scegliere Create function (Crea funzione).

Per ulteriori informazioni sull'utilizzo di Lambda, consulta Creare una funzione Lambda con la console nella Guida per gli sviluppatori di AWS Lambda .

Per creare una EventBridge regola per attivare una funzione Lambda quando un'istanza in un parco EC2 cambia stato

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.
3. Per Define rule detail (Definisci dettagli della regola), effettua le seguenti operazioni:
   a. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.

      Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso bus di eventi.
   b. Per Event bus (Bus di eventi), scegli default. Quando un servizio AWS nell'account genera un evento, passa sempre al bus di eventi di default dell'account.
   c. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
   d. Seleziona Successivo.
4. Per Build event pattern (Crea modello di eventi), procedi come segue:
   a. Per Event source, scegli AWS eventi o eventi EventBridge partner.
   b. Per Event pattern (Modello di eventi), ai fini di questo esempio specificherai il seguente modello di eventi in modo che corrisponda all'evento `EC2 Fleet Instance Change` e al sottotipo `launched`.

      ```
      {
       "source": ["aws.ec2fleet"],
       "detail-type": ["EC2 Fleet Instance Change"],
       "detail": {
         "sub-type": ["launched"]
      }
      ```

      Per aggiungere il modello di eventi, puoi utilizzare un modello scegliendo Event pattern form (Formato del modello di eventi) o specificare il tuo modello scegliendo Custom pattern (JSON editor) (Modello personalizzato (editor JSON)), come segue:

i. Per utilizzare un modello per creare il modello di eventi, procedi come segue:

A. Scegli Event pattern form (Formato del modello di eventi).

B. Per Event source (Origine evento), scegli AWS services (Servizi).

C. In AWS Service, scegli parco istanze EC2.

D. Per Event type (Tipo di evento), scegli EC2 Fleet Instance Change (Modifica dell'istanza del parco istanze EC2).

E. Scegli Edit pattern (Modifica modello) e aggiungi `"detail": {"sub-type": ["launched"]` per creare una corrispondenza con il modello di evento di esempio. Per il corretto formato JSON, inserisci una virgola (`,`) dopo la parentesi quadrata precedente (`]`).

ii. (Alternativa) Per specificare un modello di eventi personalizzato, procedi come segue:

A. Scegli Custom pattern (JSON editor) (Modello personalizzato (editor JSON)).

B. Nella casella Event pattern (Modello di eventi), aggiungi il modello di eventi per questo esempio.

c. Seleziona Successivo.

5. Per Select target(s) (Seleziona destinazione/i), esegui queste operazioni:

a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).

b. Per Select a target (Seleziona una destinazione, scegli SNS topic (Argomento SNS) per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando si verifica l'evento.

c. Per Target, scegli Lambda function (Funzione Lambda), e in Function (Funzione), scegli la funzione creata per rispondere quando si verifica l'evento.

d. (Facoltativo) In Additional settings (Impostazioni aggiuntive), facoltativamente puoi configurare impostazioni aggiuntive. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi (passaggio 16) nella Amazon EventBridge User Guide.

e. Seleziona Successivo.

6. (Opzionale) Per Tags (Tag), se desideri puoi assegnare uno o più tag alla regola, quindi scegli Next (Successivo).

7. Per Review and create (Verifica e crea), procedi come segue:

a. Verifica i dettagli della regola e modificali se necessario.
b. Scegli Crea regola.

Per un tutorial su come creare una funzione Lambda e una EventBridge regola che esegua la funzione Lambda, consulta Tutorial: Log the State of an Amazon EC2 Instance Using in the Developer Guide. EventBridge AWS Lambda

Crea EventBridge regole Amazon per monitorare gli eventi della flotta Spot

Quando viene emessa una notifica di modifica dello stato per una flotta Spot, l'evento relativo alla notifica viene inviato ad Amazon EventBridge sotto forma di file JSON. Puoi scrivere una EventBridge regola per automatizzare le azioni da intraprendere quando un modello di evento corrisponde alla regola. Se EventBridge rileva un pattern di eventi che corrisponde a uno schema definito in una regola, EventBridge richiama l'obiettivo (o i target) specificati nella regola.

I campi seguenti costituiscono il modello di evento definito nella regola:

`"source": "aws.ec2spotfleet"`

Identifica che l'evento proviene da un parco istanze spot.

`"detail-type": "EC2 Spot Fleet State Change"`

Identifica il tipo di evento.

`"detail": { "sub-type": "submitted" }`

Identifica il sottotipo di evento.

Per l'elenco degli eventi della serie di istanze spot e dei dati degli eventi di esempio, vedere the section called “Tipi di eventi del parco istanze spot”.

Esempi

- Crea una EventBridge regola per inviare una notifica
- Crea una EventBridge regola per attivare una funzione Lambda

Crea una EventBridge regola per inviare una notifica

L'esempio seguente crea una EventBridge regola per inviare un'e-mail, un messaggio di testo o una notifica push mobile ogni volta che Amazon EC2 emette una notifica di modifica dello stato della flotta

Spot. Il segnale in questo esempio viene emesso come evento `EC2 Spot Fleet State Change`, che attiva l'azione definita dalla regola. Prima di creare la EventBridge regola, devi creare l'argomento Amazon SNS per l'e-mail, il messaggio di testo o la notifica push per dispositivi mobili.

Per creare una EventBridge regola per inviare una notifica quando lo stato di una flotta Spot cambia

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.
3. Per Define rule detail (Definisci dettagli della regola), effettua le seguenti operazioni:
   a. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.

      Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso bus di eventi.
   b. Per Event bus (Bus di eventi), scegli default. Quando un servizio AWS nell'account genera un evento, passa sempre al bus di eventi di default dell'account.
   c. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
   d. Seleziona Successivo.
4. Per Build event pattern (Crea modello di eventi), procedi come segue:
   a. Per Event source, scegli AWS eventi o eventi EventBridge partner.
   b. Per Event pattern (Modello di eventi), ai fini di questo esempio specificherai il seguente modello di eventi in modo che corrisponda all'evento `EC2 Spot Fleet Instance Change`.

      ```
      {
       "source": ["aws.ec2spotfleet"],
       "detail-type": ["EC2 Spot Fleet Instance Change"]
      }
      ```

      Per aggiungere il modello di eventi, puoi utilizzare un modello scegliendo Event pattern form (Formato del modello di eventi) o specificare il tuo modello scegliendo Custom pattern (JSON editor) (Modello personalizzato (editor JSON)), come segue:

      i. Per utilizzare un modello per creare il modello di eventi, procedi come segue:

         A. Scegli Event pattern form (Formato del modello di eventi).

B. Per Event source (Origine evento), scegli AWS services (Servizi).

C. In AWS Service, scegli Serie di istanze spot EC2.

D. Per Event type (Tipo di evento), scegli EC2 Spot Fleet Instance Change (Modifica dell'istanza della serie di istanze spot EC2).

E. Per personalizzare il modello, scegli Edit pattern (Modifica modello) e apporta le modifiche in modo che corrisponda al modello di eventi di esempio.

ii. (Alternativa) Per specificare un modello di eventi personalizzato, procedi come segue:

A. Scegli Custom pattern (JSON editor) (Modello personalizzato (editor JSON)).

B. Nella casella Event pattern (Modello di eventi), aggiungi il modello di eventi per questo esempio.

c. Seleziona Successivo.

5. Per Select target(s) (Seleziona destinazione/i), esegui queste operazioni:

a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).

b. Per Select a target (Seleziona una destinazione, scegli SNS topic (Argomento SNS) per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando si verifica l'evento.

c. Per Argomento, scegliere un argomento esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) nella Amazon Simple Notification Service Developer Guide.

d. (Facoltativo) In Additional settings (Impostazioni aggiuntive), facoltativamente puoi configurare impostazioni aggiuntive. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi (passaggio 16) nella Amazon EventBridge User Guide.

e. Seleziona Successivo.

6. (Opzionale) Per Tags (Tag), se desideri puoi assegnare uno o più tag alla regola, quindi scegli Next (Successivo).

7. Per Review and create (Verifica e crea), procedi come segue:

a. Verifica i dettagli della regola e modificali se necessario.

b. Scegli Crea regola.

Per ulteriori informazioni, consulta EventBridge le regole di Amazon e i modelli di EventBridge eventi di Amazon nella Amazon EventBridge User Guide

Crea una EventBridge regola per attivare una funzione Lambda

L'esempio seguente crea una EventBridge regola per attivare una funzione Lambda ogni volta che Amazon EC2 emette una notifica di modifica dell'istanza Spot Fleet per l'avvio di un'istanza. Il segnale in questo esempio viene emesso come evento `EC2 Spot Fleet Instance Change`, sottotipo `launched`, che attiva l'azione definita dalla regola.

Prima di creare la EventBridge regola, è necessario creare la funzione Lambda.

Per creare la funzione Lambda da utilizzare nella regola EventBridge

1. Apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Selezionare Create function (Crea funzione).
3. Immettere un nome per la funzione, configurare il codice, quindi scegliere Create function (Crea funzione).

   Per ulteriori informazioni sull'utilizzo di Lambda, consulta Creare una funzione Lambda con la console nella Guida per gli sviluppatori di AWS Lambda .

Per creare una EventBridge regola per attivare una funzione Lambda quando un'istanza in una flotta Spot cambia stato

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.
3. Per Define rule detail (Definisci dettagli della regola), effettua le seguenti operazioni:

   a. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.

      Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso bus di eventi.

   b. Per Event bus (Bus di eventi), scegli default. Quando un servizio AWS nell'account genera un evento, passa sempre al bus di eventi di default dell'account.

   c. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).

   d. Seleziona Successivo.

4. Per Build event pattern (Crea modello di eventi), procedi come segue:

   a. Per Event source, scegli AWS eventi o eventi EventBridge partner.

   b. Per Event pattern (Modello di eventi), ai fini di questo esempio specificherai il seguente modello di eventi in modo che corrisponda all'evento `EC2 Spot Fleet Instance Change` e al sottotipo `launched`.

```
{
 "source": ["aws.ec2spotfleet"],
 "detail-type": ["EC2 Spot Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

   Per aggiungere il modello di eventi, puoi utilizzare un modello scegliendo Event pattern form (Formato del modello di eventi) o specificare il tuo modello scegliendo Custom pattern (JSON editor) (Modello personalizzato (editor JSON)), come segue:

   i. Per utilizzare un modello per creare il modello di eventi, procedi come segue:

      A. Scegli Event pattern form (Formato del modello di eventi).

      B. Per Event source (Origine evento), scegli AWS services (Servizi).

      C. In AWS Service, scegli Serie di istanze spot EC2.

      D. Per Event type (Tipo di evento), scegli EC2 Spot Fleet Instance Change (Modifica dell'istanza della serie di istanze spot EC2).

      E. Scegli Edit pattern (Modifica modello) e aggiungi `"detail": {"sub-type": ["launched"]` per creare una corrispondenza con il modello di evento di esempio. Per il corretto formato JSON, inserisci una virgola (`,`) dopo la parentesi quadrata precedente (`]`).

   ii. (Alternativa) Per specificare un modello di eventi personalizzato, procedi come segue:

      A. Scegli Custom pattern (JSON editor) (Modello personalizzato (editor JSON)).

      B. Nella casella Event pattern (Modello di eventi), aggiungi il modello di eventi per questo esempio.

   c. Seleziona Successivo.

5. Per Select target(s) (Seleziona destinazione/i), esegui queste operazioni:

a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).

b. Per Select a target (Seleziona una destinazione, scegli SNS topic (Argomento SNS) per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando si verifica l'evento.

c. Per Target, scegli Lambda function (Funzione Lambda), e in Function (Funzione), scegli la funzione creata per rispondere quando si verifica l'evento.

d. (Facoltativo) In Additional settings (Impostazioni aggiuntive), facoltativamente puoi configurare impostazioni aggiuntive. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi (passaggio 16) nella Amazon EventBridge User Guide.

e. Seleziona Successivo.

6. (Opzionale) Per Tags (Tag), se desideri puoi assegnare uno o più tag alla regola, quindi scegli Next (Successivo).

7. Per Review and create (Verifica e crea), procedi come segue:

a. Verifica i dettagli della regola e modificali se necessario.

b. Scegli Crea regola.

Per un tutorial su come creare una funzione Lambda e una EventBridge regola che esegua la funzione Lambda, consulta Tutorial: Log the State of an Amazon EC2 Instance Using in the Developer Guide. EventBridge AWS Lambda

Esercitazioni parco istanze e serie di istanze spot EC2

Le esercitazioni seguenti illustrano i processi comuni per la creazione di parchi istanze e serie di istanze spot EC2.

Tutorial

- Tutorial: utilizzo del parco istanze EC2 con la ponderazione dell'istanza
- Tutorial: utilizzo del parco istanze EC2 con capacità primaria on demand
- Tutorial: Avvio di Istanze on demand utilizzando le prenotazioni della capacità obiettivo
- Tutorial: avvio delle istanze in Blocchi di capacità
- Tutorial: utilizzo della serie di istanze spot con la ponderazione dell'istanza

Tutorial: utilizzo del parco istanze EC2 con la ponderazione dell'istanza

In questo tutorial viene utilizzata una società fittizia chiamata Example Corp per illustrare il processo di richiesta di un parco istanze EC2 con l'utilizzo della ponderazione dell'istanza.

Obiettivo

Example Corp, una società farmaceutica, vuole utilizzare la potenza di calcolo di Amazon EC2 per lo screening di composti chimici che potrebbero essere utilizzati per combattere il cancro.

Pianificazione

Prime analisi Example Corp Best Practice Spot. Poi, Example Corp stabilisce i requisiti seguenti per EC2 Fleet.

Tipi di istanza

Example Corp dispone di un'applicazione ad alta intensità di calcolo e di memoria che offre le migliori prestazioni con almeno 60 GB di memoria e otto CPU virtuali (vCPU). Il suo scopo è massimizzare tali risorse per l'applicazione al prezzo più basso possibile. Example Corp stabilisce che uno dei seguenti tipi di istanza EC2 soddisfa le proprie esigenze:

Tipo di istanza	Memoria (GiB)	vCPU
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacità di destinazione in unità

Con la ponderazione delle istanze, la capacità target può essere pari a un numero di istanze (impostazione predefinita) o a una combinazione di fattori come core (vCPU), memoria () e storage (GBGiBs). Considerando la base per la loro applicazione (60 GB di RAM e otto vCPU) come un'unità, Example Corp decide che 20 volte questa quantità soddisferebbe le proprie esigenze. Dunque, la società imposta la capacità target della propria richiesta parco istanze EC2 a 20.

Pesi dell'istanza

Dopo aver stabilito la capacità di destinazione, Example Corp calcola i pesi dell'istanza. Per calcolare il peso dell'istanza per ogni tipo di istanza, la società stabilisce le unità di ogni tipo di istanza necessarie al raggiungimento della capacità di destinazione come segue:

- r3.2xlarge (61,0 GB, 8 vCPU) = 1 unità da 20
- r3.4xlarge (122,0 GB, 16 vCPU) = 2 unità da 20
- r3.8xlarge (244,0 GB, 32 vCPU) = 4 unità da 20

Pertanto, Example Corp assegna pesi di istanza di 1, 2 e 4 alle rispettive configurazioni di avvio nella propria richiesta di EC2 Fleet.

Prezzo all'ora per unità

Example Corp utilizza il prezzo on demand all'ora per istanza come punto di partenza per il proprio prezzo. La società può anche utilizzare i prezzi Spot recenti o una combinazione dei due. Per calcolare il prezzo all'ora per unità, la società divide il prezzo iniziale all'ora per istanza per il peso. Ad esempio:

Tipo di istanza	prezzo on demand	Peso dell'istanza	Prezzo all'ora per unità
r3.2xLarge	0,7 $	1	0,7 $
r3.4xLarge	1,4 $	2	0,7 $
r3.8xLarge	$2,8	4	0,7 $

Example Corp può utilizzare un prezzo globale di 0,7 $ all'ora per unità ed essere competitiva per tutti e tre i tipi di istanza. Potrebbero anche utilizzare un prezzo globale di 0,7 USD per unità ora e un prezzo specifico di 0,9 USD per unità ora nella specifica di avvio `r3.8xlarge`.

Verificare le autorizzazioni

Prima di creare un parco istanze EC2, Example Corp verifica che abbia un ruolo IAM con le autorizzazioni necessarie. Per ulteriori informazioni, consulta Prerequisiti di parco istanze EC2.

Creazione di un modello di avvio

Successivamente, Example Corp crea un modello di avvio. L'ID del modello di avvio viene utilizzato nella fase seguente. Per ulteriori informazioni, consulta Creazione di un modello di avvio.

Creazione del parco istanze EC2

Example Corp crea un file, `config.json`, con la configurazione seguente per il proprio parco istanze EC2. Nell'esempio seguente sostituire gli identificatori di risorsa con i propri identificatori di risorsa.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
```

```
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Example Corp crea EC2 Fleet utilizzando il comando create-fleet seguente.

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

Compimento

La strategia di allocazione stabilisce da quali pool di capacità spot provengono le istanze spot.

Con la strategia `lowest-price` (ovvero la strategia predefinita), le Istanze spot provengono dal pool con il prezzo per unità più basso al momento dell'elaborazione. Per fornire 20 unità di capacità, EC2 Fleet avvia 20 istanze `r3.2xlarge` (20 diviso 1), 10 istanze `r3.4xlarge` (20 diviso 2) o 5 istanze `r3.8xlarge` (20 diviso 4).

Se Example Corp utilizzasse la strategia `diversified`, le Istanze spot proverrebbero da tutti e tre i pool. Il parco istanze EC2 avvierebbe 6 istanze `r3.2xlarge` (per ottenere 6 unità), 3 istanze `r3.4xlarge` (per ottenere 6 unità) e 2 istanze `r3.8xlarge` (per ottenere 8 unità), per un totale di 20 unità.

Tutorial: utilizzo del parco istanze EC2 con capacità primaria on demand

In questo tutorial viene utilizzata una società fittizia chiamata ABC Online per illustrare il processo di richiesta di un parco istanze EC2 con capacità primaria on demand e capacità spot se disponibile.

Obiettivo

ABC Online, un'azienda di consegne a domicilio per ristoranti, vuole essere in grado di assegnare la capacità Amazon EC2 in tutti i tipi di istanza EC2 e opzioni di acquisto per raggiungere le dimensioni, le prestazioni e i costi desiderati.

Pianificazione

ABC Online necessita di una capacità fissa per essere operativa nei periodi di picco, ma vuole trarre vantaggio dall'aumento della capacità a un prezzo inferiore. ABC Online stabilisce i requisiti seguenti per EC2 Fleet:

- Capacità istanza on demand - ABC Online richiede 15 istanze on demand per garantire di poter gestire il flusso nei periodi di picco.
- Capacità istanza spot - ABC Online vorrebbe migliorare le prestazioni eseguendo il provisioning di 5 istanze spot ma a un prezzo inferiore.

Verificare le autorizzazioni

Prima di creare un parco istanze EC2, ABC Online verifica che abbia un ruolo IAM con le autorizzazioni necessarie. Per ulteriori informazioni, consulta Prerequisiti di parco istanze EC2.

Creazione di un modello di avvio

Successivamente, ABC Online crea un modello di avvio. L'ID del modello di avvio viene utilizzato nella fase seguente. Per ulteriori informazioni, consulta Creazione di un modello di avvio.

Creazione del Parco istanze EC2

ABC Online crea un file, `config.json`, con la configurazione seguente per il proprio parco istanze EC2. Nell'esempio seguente sostituire gli identificatori di risorsa con i propri identificatori di risorsa.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
```

```
}
```

ABC Online crea EC2 Fleet utilizzando il comando create-fleet seguente.

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

Compimento

La strategia di allocazione fa in modo che la capacità on demand venga sempre soddisfatta, mentre il saldo della capacità di destinazione viene soddisfatto come Spot se c'è capacità e disponibilità.

Tutorial: Avvio di Istanze on demand utilizzando le prenotazioni della capacità obiettivo

Questo tutorial illustra tutti i passaggi da eseguire in modo che il parco istanze EC2 avvii le istanze on demand sulle prenotazioni della capacità `targeted`.

Verrà illustrato come configurare un parco istanze per utilizzare prima le prenotazioni della capacità on demand `targeted` all'avvio delle istanze on demand. Verrà inoltre illustrato come configurare il parco istanze in modo che, quando la capacità on demand obiettivo totale supera il numero di prenotazioni della capacità inutilizzate disponibili, il parco istanze utilizzi la strategia di allocazione specificata per selezionare i pool di istanze in cui avviare la capacità obiettivo rimanente.

Configurazione del parco istanze EC2

In questo tutorial, la configurazione del parco istanze è la seguente:

- Capacità obiettivo: 10 istanze on demand
- Prenotazioni della capacità `targeted` inutilizzate totali: 6 (meno della capacità obiettivo on demand del parco istanze di 10 istanze on demand)
- Numero di prenotazioni della capacità per pool: 2 (`us-east-1a` e `us-east-1b`)
- Numero di prenotazioni della capacità per pool: 3
- Strategia di allocazione on demand: `lowest-price`. (Quando il numero di prenotazioni della capacità inutilizzate è inferiore alla capacità obiettivo on demand, il parco istanze determina i pool in cui avviare la capacità on demand rimanente in base alla strategia di allocazione on demand.)

Tenere presente che è anche possibile utilizzare la strategia di allocazione `prioritized` invece della strategia di allocazione `lowest-price`.

Per avviare istanze on demand in prenotazioni della capacità targeted è necessario eseguire una serie di passaggi, come indicato di seguito:

- Fase 1: creazione di prenotazioni della capacità
- Fase 2: creazione di un gruppo di risorse di prenotazione della capacità
- Fase 3: aggiunta delle prenotazioni della capacità al gruppo di risorse di prenotazione della capacità
- (Facoltativo) Fase 4: visualizzazione delle prenotazioni delle capacità nel gruppo di risorse
- Fase 5: creazione di un modello di avvio che specifichi che la prenotazione della capacità è destinata a un gruppo di risorse specifico
- (Facoltativo) Fase 6: descrizione del modello di avvio
- Fase 7: creazione di un parco istanze EC2
- (Facoltativo) Fase 8: visualizzazione del numero di prenotazioni delle capacità non utilizzate rimanenti

Fase 1: creazione di prenotazioni della capacità

Utilizzate il create-capacity-reservationcomando per creare le prenotazioni di capacità, tre per e altre tre per. `us-east-1a` `us-east-1b` Ad eccezione della zona di disponibilità, gli altri attributi delle prenotazioni della capacità sono identici.

3 prenotazioni della capacità in **`us-east-1a`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Esempio di ID prenotazione della capacità risultante

```
cr-1234567890abcdef1
```

3 prenotazioni della capacità in **`us-east-1b`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Esempio di ID prenotazione della capacità risultante

```
cr-54321abcdef567890
```

Fase 2: creazione di un gruppo di risorse di prenotazione della capacità

Utilizzare il servizio `resource-groups` e il comando create-group per creare un gruppo di risorse prenotazioni della capacità. In questo esempio, il gruppo di risorse è denominato `my-cr-group`. Per informazioni sul motivo per cui è necessario creare un gruppo di risorse, consulta Utilizzo di Prenotazioni di capacità per Istanze on demand.

```
aws resource-groups create-group \
    --name my-cr-group \
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Fase 3: aggiunta delle prenotazioni della capacità al gruppo di risorse di prenotazione della capacità

Utilizzare il servizio `resource-groups` e il comando group-resources per aggiungere le prenotazioni della capacità create nella fase 1 al gruppo di risorse prenotazioni della capacità. Tenere presente che è necessario fare riferimento alle prenotazioni della capacità on demand in base ai relativi ARN.

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Output di esempio

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

(Facoltativo) Fase 4: visualizzazione delle prenotazioni delle capacità nel gruppo di risorse

Utilizza il `resource-groups` servizio e il list-group-resourcescomando per descrivere facoltativamente il gruppo di risorse per visualizzarne le prenotazioni di capacità.

```
aws resource-groups list-group-resources --group my-cr-group
```

Output di esempio

```
{
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

Fase 5: creazione di un modello di avvio che specifichi che la prenotazione della capacità è destinata a un gruppo di risorse specifico

Utilizzate il create-launch-templatecomando per creare un modello di avvio in cui specificare le prenotazioni di capacità da utilizzare. In questo esempio, il parco istanze utilizza le prenotazioni della

capacità `targeted` che sono state aggiunte a un gruppo di risorse. Pertanto, i dati del modello di avvio specificano che la prenotazione della capacità è destinata a un gruppo di risorse specifico. In questo esempio, il modello di avvio è denominato `my-launch-template`.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
            }
        }'
```

(Facoltativo) Fase 6: descrizione del modello di avvio

Utilizzate il describe-launch-templatecomando per descrivere facoltativamente il modello di lancio per visualizzarne la configurazione.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Output di esempio

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-
groups:us-east-1:123456789012:group/my-cr-group"
                    }
                }
            }
```

```
        }
    ]
}
```

Fase 7: creazione di un parco istanze EC2

Creare un parco istanze EC2 che specifichi le informazioni di configurazione per le istanze che avvierà. La seguente configurazione del parco istanze EC2 mostra solo le configurazioni pertinenti per questo esempio. Il modello di avvio `my-launch-template` è il modello di avvio creato al passaggio 5. Esistono due pool di istanze, entrambi con lo stesso tipo di istanza (`c5.xlarge`) ma con diverse zone di disponibilità (`us-east-1a` e `us-east-1b`). Il prezzo dei pool di istanze è lo stesso perché la determinazione dei prezzi è definita per la Regione, non per la zona di disponibilità. La capacità obiettivo totale è 10 e il tipo di capacità obiettivo predefinito è `on-demand`. La strategia di allocazione on demand è `lowest-price`. La strategia di utilizzo per la prenotazione della capacità è `use-capacity-reservations-first`.

> **Note**
>
> Il tipo di parco istanze deve essere `instant`. Altri tipi di parchi istanze non supportano `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
```

```
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Dopo aver creato il parco istanze `instant` utilizzando la configurazione precedente, vengono avviate le seguenti 10 istanze per soddisfare la capacità obiettivo:

- Le prenotazioni della capacità vengono prima utilizzate per avviare 6 istanze on demand nel modo seguente:
  - 3 istanze on demand vengono avviate in 3 prenotazioni della capacità `c5.xlarge` `targeted` in `us-east-1a`
  - 3 istanze on demand vengono avviate in 3 prenotazioni della capacità `c5.xlarge` `targeted` in `us-east-1b`
- Per soddisfare la capacità obiettivo, vengono avviate 4 istanze on demand aggiuntive nella capacità on demand in base alla strategia di allocazione on demand che in questo esempio è `lowest-price`. Tuttavia, poiché i pool hanno lo stesso prezzo (poiché il prezzo è per Regione e non per zona di disponibilità), il parco istanze avvia le restanti 4 istanze on demand in uno dei pool.

(Facoltativo) Fase 8: visualizzazione del numero di prenotazioni delle capacità non utilizzate rimanenti

Dopo il lancio della flotta, puoi facoltativamente eseguire l'operazione describe-capacity-reservationsper vedere quante prenotazioni di capacità non utilizzate sono rimaste. In questo esempio, dovresti vedere la seguente risposta, che mostra che tutti i Prenotazioni di capacità del pool sono stati utilizzati.

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
```

```
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

Tutorial: avvio delle istanze in Blocchi di capacità

Questo tutorial illustra tutti i passaggi da eseguire in modo che il parco istanze EC2 avvii le istanze in Blocchi di capacità. Per ulteriori informazioni sui Capacity Blocks, consulta. Blocchi di capacità per ML

È possibile utilizzare EC2 Fleet di tipo instantaneo per avviare istanze in Blocchi di capacità. Per ulteriori informazioni, consulta Utilizzo di un EC2 Fleet di tipo "istantaneo".

Nella maggior parte dei casi, la capacità di destinazione della richiesta del parco istanze EC2 deve essere inferiore o uguale alla capacità disponibile della prenotazione del blocco di capacità che hai scelto come destinazione. Le richieste di capacità di destinazione che superano i limiti della prenotazione del blocco di capacità non verranno soddisfatte. Se la richiesta di capacità di destinazione supera i limiti della prenotazione del blocco di capacità, riceverai un'eccezione di capacità insufficiente per la capacità che supera i limiti della prenotazione del blocco di capacità.

> **Note**
>
> Per i blocchi di capacità, il parco istanze EC2 non ricorrerà all'avvio di istanze on demand per la restante capacità di destinazione desiderata.

Se il parco istanze EC2 non è in grado di soddisfare la capacità di destinazione richiesta in una prenotazione del blocco di capacità disponibile, il parco istanze EC2 soddisferà tutta la capacità possibile e restituirà le istanze che è stato in grado di avviare. È possibile ripetere nuovamente la chiamata al parco istanze EC2 fino al provisioning di tutte le istanze.

Dopo aver configurato la richiesta del parco istanze EC2, è necessario attendere la data di inizio della prenotazione del blocco di capacità. Se richiedi al parco istanze EC2 di avviare un blocco di capacità che non è ancora stato avviato, riceverai un errore di capacità insufficiente.

Dopo che la prenotazione del blocco di capacità diventa attiva, puoi effettuare chiamate all'API del parco istanze EC2 ed eseguire il provisioning delle istanze nel tuo blocco di capacità in base ai

parametri selezionati. Le istanze in esecuzione nel blocco di capacità continuano a funzionare finché non le interrompi o le termini tramite una chiamata API Amazon EC2 separata oppure finché Amazon EC2 non termina le istanze al termine della prenotazione del blocco di capacità.

Considerazioni

- Non sono supportati più blocchi di capacità nella stessa richiesta `CreateFleet`.
- L'utilizzo di `OnDemandTargetCapacity` o `SpotTargetCapacity` contemporaneamente all'impostazione di `capacity-block` come `DefaultTargetCapacity` non è supportato.
- Se `DefaultTargetCapacityType` è impostato su `capacity-block`, non puoi specificare `OnDemandOptions::CapacityReservationOptions`. Si verificherà un'eccezione.

Creazione di un modello di avvio

L'ID del modello di avvio viene utilizzato nella fase seguente. Per ulteriori informazioni, consulta Creazione di un modello di avvio.

Per configurare il modello di avvio, per `InstanceMarketOptionsRequest`, imposta `MarketType` su `capacity-block`. Specifica l'ID di prenotazione del blocco di capacità che hai scelto come destinazione impostando il parametro `CapacityReservationID`.

Creazione del parco istanze EC2

Crea un file, `config.json`, con la configurazione seguente per il parco istanze EC2. Nell'esempio seguente sostituire gli identificatori di risorsa con i propri identificatori di risorsa.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "CBR-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
            ]
        }
```

```
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "capacity-block"
    },
    "Type": "instant"
}
```

Utilizza il comando create-fleet.

```
aws ec2 create-fleet \
     --cli-input-json file://config.json
```

Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

Tutorial: utilizzo della serie di istanze spot con la ponderazione dell'istanza

In questo tutorial viene utilizzata una società fittizia chiamata Example Corp per illustrare il processo di richiesta di una serie di istanze spot con l'utilizzo della ponderazione dell'istanza.

Obiettivo

Example Corp, una società farmaceutica, vuole sfruttare la potenza di calcolo di Amazon EC2 per lo screening di composti chimici che potrebbero essere utilizzati per combattere il cancro.

Pianificazione

Prime analisi Example Corp Best Practice Spot. Poi, Example Corp stabilisce i requisiti seguenti per il parco istanze spot.

Tipi di istanza

Example Corp dispone di un'applicazione ad alta intensità di calcolo e di memoria che offre le migliori prestazioni con almeno 60 GB di memoria e otto CPU virtuali (vCPU). Il suo scopo è massimizzare tali risorse per l'applicazione al prezzo più basso possibile. Example Corp stabilisce che uno dei seguenti tipi di istanza EC2 soddisfa le proprie esigenze:

Tipo di istanza	Memoria (GiB)	vCPU
r3.2xlarge	61	8

Tipo di istanza	Memoria (GiB)	vCPU
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacità di destinazione in unità

Con la ponderazione delle istanze, la capacità target può essere pari a un numero di istanze (impostazione predefinita) o a una combinazione di fattori come core (vCPU), memoria () e storage (GBGiBs). Considerando la base per la loro applicazione (60 GB di RAM e otto vCPU) come unità 1, Example Corp decide che 20 volte questa quantità soddisferebbe le proprie esigenze. Dunque, la società imposta la capacità obiettivo della propria richiesta di parco istanze spot a 20.

Pesi dell'istanza

Dopo aver stabilito la capacità di destinazione, Example Corp calcola i pesi dell'istanza. Per calcolare il peso dell'istanza per ogni tipo di istanza, la società stabilisce le unità di ogni tipo di istanza necessarie al raggiungimento della capacità di destinazione come segue:

- r3.2xlarge (61,0 GB, 8 vCPU) = 1 unità da 20
- r3.4xlarge (122,0 GB, 16 vCPU) = 2 unità da 20
- r3.8xlarge (244,0 GB, 32 vCPU) = 4 unità da 20

Pertanto, Example Corp assegna pesi di istanza di 1, 2 e 4 alle rispettive configurazioni di avvio nella propria richiesta del parco istanze spot.

Prezzo all'ora per unità

Example Corp utilizza il prezzo on demand all'ora per istanza come punto di partenza per il proprio prezzo. La società può anche utilizzare i prezzi Spot recenti o una combinazione dei due. Per calcolare il prezzo all'ora per unità, la società divide il prezzo iniziale all'ora per istanza per il peso. Ad esempio:

Tipo di istanza	prezzo on demand	Peso dell'istanza	Prezzo all'ora per unità
r3.2xLarge	0,7 $	1	0,7 $

Tipo di istanza	prezzo on demand	Peso dell'istanza	Prezzo all'ora per unità
r3.4xLarge	1,4 $	2	0,7 $
r3.8xLarge	$2,8	4	0,7 $

Example Corp può utilizzare un prezzo globale di 0,7 $ all'ora per unità ed essere competitiva per tutti e tre i tipi di istanza. Potrebbero anche utilizzare un prezzo globale di 0,7 USD per unità ora e un prezzo specifico di 0,9 USD per unità ora nella specifica di avvio `r3.8xlarge`.

Verificare le autorizzazioni

Prima di creare una richiesta di parco istanze spot, Example Corp verifica che abbia un ruolo IAM con le autorizzazioni necessarie. Per ulteriori informazioni, consulta Autorizzazioni del parco istanze spot.

Creare la richiesta

Example Corp crea un file, `config.json`, con la configurazione seguente per la propria richiesta di serie di istanze spot:

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.2xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 1
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.4xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 2
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.8xlarge",
```

```
      "SubnetId": "subnet-482e4972",
      "SpotPrice": "0.90",
      "WeightedCapacity": 4
    }
  ]
}
```

Example Corp crea la richiesta Spot Fleet utilizzando il comando. request-spot-fleet

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Per ulteriori informazioni, consulta Tipi di richiesta del parco istanze spot.

Compimento

La strategia di allocazione stabilisce da quali pool di capacità spot provengono le istanze spot.

Con la strategia `lowestPrice` (ovvero la strategia predefinita), le Istanze spot provengono dal pool con il prezzo per unità più basso al momento dell'elaborazione. Per fornire 20 unità di capacità, la serie di istanze spot avvia 20 istanze `r3.2xlarge` (20 diviso 1), 10 istanze `r3.4xlarge` (20 diviso 2) o 5 istanze `r3.8xlarge` (20 diviso 4).

Se Example Corp utilizzasse la strategia `diversified`, le Istanze spot proverrebbero da tutti e tre i pool. la serie di istanze spot avvierebbe 6 istanze `r3.2xlarge` (per ottenere 6 unità), 3 istanze `r3.4xlarge` (per ottenere 6 unità) e 2 istanze `r3.8xlarge` (per ottenere 8 unità), per un totale di 20 unità.

Esempi di configurazioni per parco istanze e serie di istanze spot EC2

Gli esempi seguenti illustrano le configurazioni di avvio che è possibile utilizzare per creare parchi istanze e serie di istanze spot EC2.

Argomenti

- Configurazioni parco istanze EC2 di esempio
- Configurazioni del parco istanze spot di esempio

Configurazioni parco istanze EC2 di esempio

Gli esempi seguenti illustrano le configurazioni di avvio che è possibile utilizzare con il comando create-fleet per creare un parco istanze EC2. Per ulteriori informazioni sui parametri, consultare create-fleet nella Guida di riferimento ai comandi della AWS CLI .

Esempi

Esempio 1: Avviare Istanze spot come opzione di acquisto predefinita

L'esempio seguente indica i parametri minimi necessari in un parco istanze EC2: un modello di lancio, una capacità di destinazione e un'opzione d'acquisto predefinita. Il modello di avvio viene identificato dall'ID e dal numero di versione del modello di avvio. La capacità target per il parco istanze è di 2 istanze e l'opzione d'acquisto predefinita è `spot`; ne consegue che il parco istanze avvia 2 Istanze spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
```

```
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Esempio 2: Avviare Istanze on demand come opzione di acquisto predefinita

L'esempio seguente indica i parametri minimi necessari in un Parco istanze EC2: un modello di avvio, una capacità di destinazione e un'opzione d'acquisto predefinita. Il modello di avvio viene identificato dall'ID e dal numero di versione del modello di avvio. La capacità target per il parco istanze è di 2 istanze e l'opzione d'acquisto predefinita è `on-demand`; ne consegue che il parco istanze avvia 2 Istanze on demand.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

Esempio 3: Avviare Istanze on demand come capacità primaria

L'esempio seguente specifica la capacità di destinazione totale di 2 istanze per il parco istanze e una capacità di destinazione di 1 Istanza on demand. L'opzione di acquisto predefinita è `spot`. Il parco istanze avvia 1 Istanza on demand come indicato, ma deve avviare un'altra istanza per soddisfare la capacità target totale. L'opzione di acquisto per la differenza viene calcolata come `TotalTargetCapacity` – `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, ne consegue che il parco istanze avvia 1 istanza spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Esempio 4: Avvio di istanze On-Demand utilizzando prenotazioni di capacità multiple

È possibile configurare un parco istanze affinché utilizzi Prenotazioni di capacità on demand prima all'avvio Istanze on demand impostando la strategia di utilizzo per Prenotazioni di capacità su `use-capacity-reservations-first`. In questo esempio viene illustrato come il parco istanze seleziona la prenotazione della capacità da utilizzare quando sono presenti più prenotazioni della capacità di quelle necessarie per soddisfare la capacità obiettivo.

In questo esempio, la configurazione del parco istanze è la seguente:

- Capacità obiettivo: 12 istanze on demand
- Prenotazioni della capacità inutilizzate totali: 15 (più della capacità obiettivo del parco istanze di 12 istanze on demand)
- Numero di prenotazioni della capacità per pool: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)
- Numero di prenotazioni della capacità per pool: 5
- Strategia di allocazione on demand: `lowest-price` (Quando sono presenti più prenotazioni della capacità inutilizzate in più pool di istanze, il parco istanze determina i pool in cui avviare le istanze on demand in base alla strategia di allocazione on demand).

  Tenere presente che è anche possibile utilizzare la strategia di allocazione `prioritized` invece della strategia di allocazione `lowest-price`.

Prenotazioni di capacità

L'account presenta i seguenti 15 Prenotazioni di capacità inutilizzati in 3 diversi pool. Il numero di Prenotazioni di capacità in ogni pool è indicato da `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configurazione del parco istanze

La seguente configurazione del parco istanze mostra solo le configurazioni pertinenti per questo esempio. La capacità di destinazione totale è 12 e il tipo di capacità di destinazione predefinito è `on-demand`. La strategia di allocazione on demand è `lowest-price`. La strategia di utilizzo per la prenotazione della capacità è `use-capacity-reservations-first`.

In questo esempio, il prezzo istanza on demand è:

- `m5.large` – 0,096 USD all'ora
- `m4.xlarge` – 0,20 USD all'ora
- `m4.2xlarge` – 0,40 USD all'ora

> **Note**
>
> Il tipo di parco istanze deve essere di tipo `instant`. Altri tipi di parchi istanze non supportano `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
```

```
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Dopo aver creato il parco istanze `instant` utilizzando la configurazione precedente, vengono avviate le seguenti 12 istanze per soddisfare la capacità di destinazione:

- 5 istanze on demand `m5.large` in `us-east-1a` – `m5.large` in `us-east-1a` è il prezzo più basso, e ci sono 5 prenotazioni della capacità `m5.large` disponibili inutilizzate
- 5 istanze on demand `m4.xlarge` in us-east-1a – `m4.xlarge` in `us-east-1a` è il prezzo più basso successivo, e ci sono 5 prenotazioni della capacità `m4.xlarge` disponibili inutilizzate
- 2 istanze on demand `m4.2xlarge` in us-east-1a – `m4.2xlarge` in `us-east-1a` è il terzo prezzo più basso, e ci sono 5 prenotazioni della capacità `m4.2xlarge` non utilizzate di cui solo 2 sono necessarie per soddisfare la capacità obiettivo

Dopo il lancio della flotta, puoi correre describe-capacity-reservationsper vedere quante prenotazioni di capacità non utilizzate sono rimaste. In questo esempio, dovresti vedere la seguente risposta, che mostra che sono state utilizzate tutte le prenotazioni della capacità `m5.large` e `m4.xlarge`, con 3 prenotazioni della capacità `m4.2xlarge` rimaste inutilizzate.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
```

```
    "AvailableInstanceCount": 3
}
```

Esempio 5: avvia le istanze On-Demand utilizzando le prenotazioni di capacità quando la capacità target totale supera il numero di prenotazioni di capacità non utilizzate

È possibile configurare un parco istanze affinché utilizzi Prenotazioni di capacità on demand prima all'avvio Istanze on demand impostando la strategia di utilizzo per Prenotazioni di capacità su `use-capacity-reservations-first`. In questo esempio viene illustrato come il parco istanze seleziona i pool di istanze in cui avviare le istanze on demand quando la capacità totale obiettivo supera il numero di prenotazioni della capacità inutilizzate disponibili.

In questo esempio, la configurazione del parco istanze è la seguente:

- Capacità obiettivo: 16 istanze on demand
- Prenotazioni della capacità inutilizzate totali: 15 (meno della capacità obiettivo del parco istanze di 16 istanze on demand)
- Numero di prenotazioni della capacità per pool: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)
- Numero di prenotazioni della capacità per pool: 5
- Strategia di allocazione on demand: `lowest-price`. (Quando il numero di prenotazioni della capacità inutilizzate è inferiore alla capacità obiettivo on demand, il parco istanze determina i pool in cui avviare la capacità on demand rimanente in base alla strategia di allocazione on demand.)

  Tenere presente che è anche possibile utilizzare la strategia di allocazione `prioritized` invece della strategia di allocazione `lowest-price`.

Prenotazioni di capacità

L'account presenta i seguenti 15 Prenotazioni di capacità inutilizzati in 3 diversi pool. Il numero di Prenotazioni di capacità in ogni pool è indicato da `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
```

```
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configurazione del parco istanze

La seguente configurazione del parco istanze mostra solo le configurazioni pertinenti per questo esempio. La capacità di destinazione totale è 16 e il tipo di capacità di destinazione predefinito è `on-demand`. La strategia di allocazione on demand è `lowest-price`. La strategia di utilizzo per la prenotazione della capacità è `use-capacity-reservations-first`.

In questo esempio, il prezzo istanza on demand è:

- m5.large – $0,096 all'ora
- m4.xlarge – $0,20 all'ora
- m4.2xlarge – 0,40 USD all'ora

> **Note**
>
> Il tipo di parco istanze deve essere `instant`. Altri tipi di parchi istanze non supportano `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Dopo aver creato il parco istanze `instant` utilizzando la configurazione precedente, vengono avviate le seguenti 16 istanze per soddisfare la capacità di destinazione:

- 6 istanze on demand `m5.large` in `us-east-1a` – `m5.large` in `us-east-1a` è il prezzo più basso, e ci sono 5 prenotazioni della capacità `m5.large` disponibili inutilizzate. Le prenotazioni della capacità vengono prima utilizzate per avviare 5 istanze on demand. Dopo che vengono utilizzate le rimanenti prenotazioni della capacità `m4.xlarge` e `m4.2xlarge`, per soddisfare la capacità obiettivo viene avviata un'ulteriore istanza on demand in base alla strategia di allocazione on demand, che in questo esempio è `lowest-price`.
- 5 istanze on demand `m4.xlarge` in `us-east-1a` – `m4.xlarge` in `us-east-1a` è il prezzo più basso successivo, e ci sono 5 prenotazioni della capacità `m4.xlarge` disponibili inutilizzate
- 5 istanze on demand `m4.2xlarge` in `us-east-1a` – `m4.2xlarge` in `us-east-1a` è il terzo prezzo più basso, e ci sono 5 prenotazioni della capacità `m4.2xlarge` disponibili inutilizzate

Dopo il lancio della flotta, puoi correre describe-capacity-reservationsper vedere quante prenotazioni di capacità non utilizzate sono rimaste. In questo esempio, dovresti vedere la seguente risposta, che mostra che tutti i Prenotazioni di capacità del pool sono stati utilizzati.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

Esempio 6: avvio di istanze On-Demand utilizzando prenotazioni di capacità mirate

È possibile configurare un parco istanze affinché utilizzi prima le prenotazioni della capacità on demand `targeted` prima all'avvio di istanze on demand impostando la strategia di utilizzo per le prenotazioni della capacità su `use-capacity-reservations-first`. In questo esempio viene illustrato come avviare istanze on demand in prenotazione della capacità `targeted`, in cui gli attributi

della prenotazione della capacità sono gli stessi ad eccezione delle relative zone di disponibilità (`us-east-1a` e `us-east-1b`). Viene inoltre illustrato come il parco istanze seleziona i pool di istanze in cui avviare le istanze on demand quando la capacità totale obiettivo supera il numero di prenotazioni della capacità inutilizzate disponibili.

In questo esempio, la configurazione del parco istanze è la seguente:

- Capacità obiettivo: 10 istanze on demand
- Prenotazioni della capacità `targeted` inutilizzate totali: 6 (meno della capacità obiettivo on demand del parco istanze di 10 istanze on demand)
- Numero di prenotazioni della capacità per pool: 2 (`us-east-1a` e `us-east-1b`)
- Numero di prenotazioni della capacità per pool: 3
- Strategia di allocazione on demand: `lowest-price`. (Quando il numero di prenotazioni della capacità inutilizzate è inferiore alla capacità obiettivo on demand, il parco istanze determina i pool in cui avviare la capacità on demand rimanente in base alla strategia di allocazione on demand.)

  Tenere presente che è anche possibile utilizzare la strategia di allocazione `prioritized` invece della strategia di allocazione `lowest-price`.

Per una spiegazione passo per passo delle procedure che è necessario eseguire per riprodurre questo esempio, consultare Tutorial: Avvio di Istanze on demand utilizzando le prenotazioni della capacità obiettivo.

Prenotazioni di capacità

L'account presenta le seguenti 6 prenotazioni della capacità inutilizzati in 2 diversi pool. In questo esempio, i pool differiscono per la zona di disponibilità. Il numero di Prenotazioni di capacità in ogni pool è indicato da `AvailableInstanceCount`.


```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

```
{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configurazione del parco istanze

La seguente configurazione del parco istanze mostra solo le configurazioni pertinenti per questo esempio. La capacità obiettivo totale è 10 e il tipo di capacità obiettivo predefinito è `on-demand`. La strategia di allocazione on demand è `lowest-price`. La strategia di utilizzo per la prenotazione della capacità è `use-capacity-reservations-first`.

In questo esempio, il prezzo dell'istanza on demand per `c5.xlarge` in `us-east-1` è 0,17 $ all'ora.

> **Note**
>
> Il tipo di parco istanze deve essere `instant`. Altri tipi di parchi istanze non supportano `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
```

```
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Dopo aver creato il parco istanze `instant` utilizzando la configurazione precedente, vengono avviate le seguenti 10 istanze per soddisfare la capacità obiettivo:

- Le prenotazioni della capacità vengono prima utilizzate per avviare 6 istanze on demand nel modo seguente:
  - 3 istanze on demand vengono avviate in 3 prenotazioni della capacità `c5.xlarge` `targeted` in `us-east-1a`
  - 3 istanze on demand vengono avviate in 3 prenotazioni della capacità `c5.xlarge` `targeted` in `us-east-1b`
- Per soddisfare la capacità obiettivo, vengono avviate 4 istanze on demand aggiuntive nella capacità on demand in base alla strategia di allocazione on demand che in questo esempio è `lowest-price`. Tuttavia, poiché i pool hanno lo stesso prezzo (poiché il prezzo è per Regione e non per zona di disponibilità), il parco istanze avvia le restanti 4 istanze on demand in uno dei pool.

Dopo il lancio della flotta, puoi correre describe-capacity-reservationsper vedere quante prenotazioni di capacità non utilizzate sono rimaste. In questo esempio, dovresti vedere la seguente risposta, che mostra che tutti i Prenotazioni di capacità del pool sono stati utilizzati.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

```
{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

Esempio 7: configura il ribilanciamento della capacità per avviare istanze Spot sostitutive

Nell'esempio seguente viene configurato EC2 Fleet affinché avvii un'istanza spot sostitutiva quando Amazon EC2 emette un suggerimento di ribilanciamento per un'istanza spot del parco istanze. Per configurare la sostituzione automatica delle istanze spot, per `ReplacementStrategy`, specificare `launch-before-terminate`. Per configurare il ritardo temporale dal momento in cui vengono avviate le nuove istanze spot sostitutive a quando le vecchie istanze spot vengono eliminate automaticamente, per `termination-delay`, specificare un valore in secondi. Per ulteriori informazioni, consulta Opzioni di configurazione.

> **Note**
>
> Si consiglia di utilizzare `launch-before-terminate` solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza in modo che le vecchie istanze vengano terminate solo dopo il completamento di queste procedure. Saranno addebitati i costi per entrambe le istanze durante la loro esecuzione.

L'efficacia della strategia di ribilanciamento della capacità dipende dal numero di pool di capacità spot specificati nella richiesta parco istanze EC2. Si consiglia di configurare il parco istanze con un insieme diversificato di tipi di istanza e zone di disponibilità e per `AllocationStrategy`, specificare `capacity-optimized`. Per ulteriori informazioni sugli aspetti da considerare durante la configurazione di un parco istanze EC2 per il ribilanciamento della capacità, consulta Ribilanciamento della capacità.

```
{
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
```

```
            },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                   ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Esempio 8: avvio di istanze Spot in un parco istanze ottimizzato in termini di capacità

Nell'esempio seguente viene illustrato come configurare un parco istanze EC2 con una strategia di allocazione spot che ottimizza la capacità. Per ottimizzare la capacità, è necessario impostare `AllocationStrategy` su `capacity-optimized`.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. La capacità obiettivo è di 50 Istanze spot. Il parco istanze EC2 tenta di avviare 50 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                  ]
           }
    ],
    "TargetCapacitySpecification": {
```

```
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

Esempio 9: avvia le istanze Spot in un parco istanze con priorità ottimizzate in termini di capacità

Nell'esempio seguente viene illustrato come configurare un parco istanze EC2 con una strategia di allocazione spot che ottimizza la capacità che applica la priorità in base al miglior tentativo.

Quando si utilizza la strategia di allocazione `capacity-optimized-prioritized`, è possibile utilizzare il parametro `Priority` per specificare le priorità dei pool di capacità spot, dove a un numero inferiore corrisponde la priorità più alta. È inoltre possibile impostare la stessa priorità per diversi pool di capacità spot, se si preferisce non applicare priorità differenti. Se non si imposta una priorità per un pool, il pool verrà considerato ultimo in termini di priorità.

Per assegnare priorità ai pool di capacità spot, è necessario impostare `AllocationStrategy` su `capacity-optimized-prioritized`. Il parco istanze EC2 ottimizzerà innanzitutto la capacità, ma rispetterà le priorità sulla base del miglior tentativo (ad esempio, se il rispetto delle priorità non influirà in modo significativo sulla capacità del parco istanze EC2 di fornire capacità ottimale). Questa è una buona opzione per i carichi di lavoro in cui è necessario ridurre al minimo la possibilità di interruzioni e la preferenza per determinati tipi di istanza è importante.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. Ogni pool ha una priorità, dove a un numero inferiore corrisponde la priorità più alta. La capacità obiettivo è di 50 Istanze spot. Il parco istanze EC2 tenta di avviare 50 istanze spot nel pool di capacità spot con la priorità più alta sulla base del miglior tentativo, ma prima ottimizza la capacità.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
```

```
                        {
                            "InstanceType": "r4.2xlarge",
                            "Priority": 1,
                            "Placement": {
                                "AvailabilityZone": "us-west-2a"
                            },
                        },
                        {
                            "InstanceType": "m4.2xlarge",
                            "Priority": 2,
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            },
                        },
                        {
                            "InstanceType": "c5.2xlarge",
                            "Priority": 3,
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            }
                        }
                    ]
                }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

Esempio 10: avvio di istanze Spot in un parco istanze price-capacity-optimized

Nell'esempio seguente viene illustrato come configurare un parco istanze EC2 con una strategia di allocazione spot che ottimizza sia la capacità sia il prezzo più basso. Per ottimizzare la capacità tenendo conto del prezzo, è necessario impostare la `AllocationStrategy` spot su `price-capacity-optimized`.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. La capacità obiettivo è di 50 Istanze spot. Il parco istanze EC2 tenta di avviare 50 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando, scegliendo al contempo il pool con il prezzo più basso.

```
{
```

```
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                 ]
           }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
```

```
}
```

Esempio 11: configura la selezione del tipo di istanza basata sugli attributi

Nell'esempio seguente viene illustrato come configurare un parco istanze EC2 in modo da utilizzare la selezione del tipo di istanza basata su attributi per identificare i tipi di istanza. Per specificare gli attributi di istanza richiesti, specifica gli attributi nella struttura `InstanceRequirements`.

Nell'esempio precedente, vengono specificati due attributi di istanza:

- `VCpuCount`: viene specificato un minimo di 2 vCPU. Poiché non è specificato alcun massimo, non esiste un limite massimo.
- `MemoryMiB`: viene specificato un minimo di 4 MiB di memoria. Poiché non è specificato alcun massimo, non esiste un limite massimo.

Verranno identificati tutti i tipi di istanza con 2 o più vCPU e 4 MiB o più di memoria. Tuttavia, la protezione dei prezzi e la strategia di allocazione potrebbero escludere alcuni tipi di istanze quando il parco istanze EC2 alloca le istanze.

Per un elenco e le descrizioni di tutti i possibili attributi che puoi specificare, consulta InstanceRequirementsAmazon EC2 API Reference.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
```

```
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Configurazioni del parco istanze spot di esempio

Gli esempi seguenti mostrano le configurazioni di avvio che è possibile utilizzare con il request-spot-fleetcomando per creare una richiesta Spot Fleet. Per ulteriori informazioni, consulta Creare una richiesta di parco istanze spot.

> **Note**
>
> Per parco istanze spot, non è possibile specificare un ID di interfaccia di rete in un modello di avvio o in una specifica di avvio. Assicurati di omettere il parametro `NetworkInterfaceID` ne modello di avvio o nella specifica di avvio.

Esempi

- Esempio 1: Avviare le Istanze spot utilizzando la zona di disponibilità o la sottorete con il prezzo più basso nella regione
- Esempio 2: Avviare le Istanze spot utilizzando la zona di disponibilità o la sottorete con il prezzo più basso in un elenco specificato
- Esempio 3: Avviare le Istanze spot utilizzando il tipo di istanza con il prezzo più basso in un elenco specificato
- Esempio 4. Sostituire il prezzo per la richiesta.
- Esempio 5: Avviare un parco istanze spot utilizzando la strategia di allocazione diversificata
- Esempio 6: Avviare un parco istanze spot utilizzando la ponderazione di istanza
- Esempio 7: Avviare un parco istanze spot con capacità on demand
- Esempio 8: configurare il ribilanciamento della capacità per avviare la sostituzione delle Istanze spot
- Esempio 9: Avviare le istanze spot in un parco istanze ottimizzato per la capacità
- Esempio 10: Avviare le istanze spot in un parco istanze ottimizzato per la capacità con priorità

- Esempio 11: Avvio di istanze Spot in un parco istanze priceCapacityOptimized
- Esempio 12: configurazione della selezione del tipo di istanza basata su attributi

Esempio 1: Avviare le Istanze spot utilizzando la zona di disponibilità o la sottorete con il prezzo più basso nella regione

L'esempio seguente indica una specifica di avvio singola senza una zona di disponibilità o una sottorete. Il parco istanze spot avvia le istanze nella zona di disponibilità con il prezzo più basso che ha una sottorete predefinita. Il prezzo che si paga non supera quello on-demand.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Esempio 2: Avviare le Istanze spot utilizzando la zona di disponibilità o la sottorete con il prezzo più basso in un elenco specificato

Gli esempi seguenti indicano due specifiche di avvio con zone di disponibilità o sottoreti diverse, ma con tipo di istanza e AMI uguali.

Zone di disponibilità

Il parco istanze spot avvia le istanze nella sottorete predefinita della zona di disponibilità specificata.

```
{
```

```
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "Placement": {
              "AvailabilityZone": "us-west-2a, us-west-2b"
          },
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Sottoreti

È possibile specificare sottoreti predefinite o sottoreti non predefinite. Queste ultime possono essere da un VPC predefinito o da un VPC non predefinito. Il servizio Spot avvia le istanze in qualsiasi sottorete si trovi nella zona di disponibilità con il prezzo più basso.

Non è possibile specificare sottoreti diverse dalla stessa zona di disponibilità in una richiesta di parco istanze spot.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
```

```
            "InstanceType": "m3.medium",
            "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
            "IamInstanceProfile": {
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
            }
        }
    ]
}
```

Se le istanze vengono lanciate in un VPC predefinito, esse ricevono un indirizzo IPv4 pubblico per impostazione predefinita. Se le istanze vengono lanciate in un VPC non predefinito, esse non ricevono un indirizzo IPv4 pubblico per impostazione predefinita. Utilizzare un'interfaccia di rete nella specifica di avvio per assegnare un indirizzo IPv4 pubblico alle istanze avviate in un VPC non predefinito. Quando si specifica un'interfaccia di rete, bisogna includere l'ID della sottorete e l'ID del gruppo di sicurezza utilizzando l'interfaccia di rete.

```
...
    {
        "ImageId": "ami-1a2b3c4d",
        "KeyName": "my-key-pair",
        "InstanceType": "m3.medium",
        "NetworkInterfaces": [
            {
                "DeviceIndex": 0,
                "SubnetId": "subnet-1a2b3c4d",
                "Groups": [ "sg-1a2b3c4d" ],
                "AssociatePublicIpAddress": true
            }
        ],
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"
        }
    }
...
```

Esempio 3: Avviare le Istanze spot utilizzando il tipo di istanza con il prezzo più basso in un elenco specificato

Gli esempi seguenti indicano due configurazioni di avvio con tipi di istanza diversi, ma con AMI e zona di disponibilità o sottorete uguali. Il parco istanze spot avvia le istanze utilizzando il tipo di istanza specificato con il prezzo più basso.

Zona di disponibilità

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "Placement": {
            "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

Sottorete

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
```

```
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "c5.4xlarge",
        "SubnetId": "subnet-1a2b3c4d"
    },
    {
        "ImageId": "ami-1a2b3c4d",
        "SecurityGroups": [
            {
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "r3.8xlarge",
        "SubnetId": "subnet-1a2b3c4d"
    }
  ]
}
```

Esempio 4. Sostituire il prezzo per la richiesta.

Consigliamo di utilizzare il prezzo massimo predefinito, ossia il prezzo on-demand. Se si preferisce, è possibile specificare un prezzo massimo per la richiesta del parco istanze e dei prezzi massimi per le specifiche di avvio singole.

Gli esempi seguenti specificano un prezzo massimo per la richiesta del parco istanze e dei prezzi massimi per due delle tre specifiche di avvio. Il prezzo massimo per la richiesta del parco istanze viene utilizzata per ogni specifica di avvio che non indica un prezzo massimo. Il parco istanze spot avvia le istanze utilizzando il tipo di istanza con il prezzo più basso.

Zona di disponibilità

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
```

```
            },
            "SpotPrice": "0.10"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.4xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            },
            "SpotPrice": "0.20"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

Sottorete

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
```

```
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Esempio 5: Avviare un parco istanze spot utilizzando la strategia di allocazione diversificata

L'esempio seguente utilizza la strategia di allocazione `diversified`. Le specifiche di avvio hanno tipi di istanza diversi ma AMI e zona di disponibilità o sottorete uguali. Il parco istanze spot distribuisce le 30 istanze tra le tre specifiche di avvio, in modo che ci siano 10 istanze di ogni tipo. Per ulteriori informazioni, consulta Strategie di allocazione per istanze spot.

Zona di disponibilità

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
```

```
  ]
}
```

Sottorete

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Una best practice per aumentare la possibilità che una richiesta spot venga soddisfatta dalla capacità EC2 nel caso si verifichi un'interruzione in una delle zone di disponibilità è diversificare e varie zone. Per questo scenario, includi ogni zona di disponibilità che hai a disposizione nella specifica di avvio. E, invece di utilizzare la stessa sottorete ogni volta, utilizza tre sottoreti univoche (ognuna che mappa a una zona diversa).

Zona di disponibilità

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
```

```
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2a"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2c"
          }
      }
  ]
}
```

Sottorete

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
```

```
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
    ]
}
```

Esempio 6: Avviare un parco istanze spot utilizzando la ponderazione di istanza

Gli esempi seguenti utilizzano la ponderazione d'istanza, il che significa che il prezzo è all'ora per unità anziché all'ora per istanza. Ogni configurazione di avvio elenca un tipo di istanza diverso e un peso diverso. Il parco istanze spot seleziona il tipo di istanza con il prezzo più basso all'ora per unità. Il parco istanze spot calcola il numero di istanze spot da avviare dividendo la capacità obiettivo per il peso dell'istanza. Se il risultato non è un numero intero, il Parco istanze spot lo arrotonda al numero intero successivo, in modo che la dimensione del parco istanze non sia inferiore alla sua capacità obiettivo.

Se la richiesta `r3.2xlarge` va a buon fine, lo Spot assegna 4 di queste istanze. Dividere 20 per 6 per un totale di 3,33 istanze, quindi arrotondare fino a 4 istanze.

Se la richiesta `c3.xlarge` va a buon fine, lo Spot assegna 7 di queste istanze. Dividere 20 per 3 per un totale di 6,66 istanze, quindi arrotondare fino a 7 istanze.

Per ulteriori informazioni, consulta Ponderazione delle istanze del parco istanze spot.

Zona di disponibilità

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 6
      },
```

```
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 3
      }
    ]
}
```

Sottorete

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 3
      }
  ]
}
```

Esempio 7: Avviare un parco istanze spot con capacità on demand

Per assicurarsi di avere sempre capacità di istanza, è possibile includere una richiesta di capacità on demand nella richiesta del Parco istanze spot. La richiesta on-demand viene sempre soddisfatta se c'è capacità, mentre il saldo della capacità target viene soddisfatto come Spot se ci sono capacità e disponibilità.

L'esempio seguente specifica la capacità di destinazione desiderata come 10, di cui 5 deve essere capacità on-demand. La capacità spot non è specificata; è implicita nel rapporto tra la capacità

obiettivo meno la capacità on demand. Amazon EC2 avvia 5 unità di capacità come on demand e 5 unità di capacità (10-5=5) come Spot se ci sono capacità e disponibilità Amazon EC2.

Per ulteriori informazioni, consulta Richieste on demand nel parco istanze spot.

```
{
  "IamFleetRole": "arn:aws:iam::781603563322:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
        "Version": "2"
      },
      "Overrides": [
        {
          "InstanceType": "t2.medium",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-d0dc51fb"
        }
      ]
    }
  ]
}
```

Esempio 8: configurare il ribilanciamento della capacità per avviare la sostituzione delle Istanze spot

Nell'esempio seguente viene configurato il parco istanze spot affinché avvii un'istanza spot sostitutiva quando Amazon EC2 emette un suggerimento di ribilanciamento per un'istanza spot del parco istanze. Per configurare la sostituzione automatica delle istanze spot, per `ReplacementStrategy`, specificare `launch-before-terminate`. Per configurare il ritardo temporale dal momento in cui vengono avviate le nuove istanze spot sostitutive a quando le vecchie istanze spot vengono

eliminate automaticamente, per `termination-delay`, specificare un valore in secondi. Per ulteriori informazioni, consulta Opzioni di configurazione.

> **Note**
>
> Consigliamo di utilizzare `launch-before-terminate` solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza. Ciò garantirà che le vecchie istanze vengano terminate solo dopo il completamento delle procedure di arresto. Saranno addebitati i costi per entrambe le istanze durante la loro esecuzione.

L'efficacia della strategia di ribilanciamento della capacità dipende dal numero di pool di istanze spot specificati nella richiesta del parco istanze spot. Si consiglia di configurare il parco istanze con un insieme diversificato di tipi di istanza e zone di disponibilità e per `AllocationStrategy`, specificare `capacityOptimized`. Per ulteriori informazioni sugli aspetti da considerare durante la configurazione di una serie di istanze spot per il ribilanciamento della capacità, consulta Ribilanciamento della capacità.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
                },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                           "Placement": {
```

```
                            "AvailabilityZone": "us-east-1a"
                        }
                    },
                    {
                        "InstanceType": "c5.large",
                        "WeightedCapacity": 1,
                        "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    }
                ]
          }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Esempio 9: Avviare le istanze spot in un parco istanze ottimizzato per la capacità

Nell'esempio seguente viene illustrato come configurare un parco istanze spot con una strategia di allocazione spot che ottimizza la capacità. Per ottimizzare la capacità, è necessario impostare `AllocationStrategy` su `capacityOptimized`.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. La capacità obiettivo è di 50 Istanze spot. Il parco istanze spot tenta di avviare 50 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
```

```
            },
                "Overrides": [
                      {
                          "InstanceType": "r4.2xlarge",
                          "AvailabilityZone": "us-west-2a"
                      },
                      {
                          "InstanceType": "m4.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                      },
                      {
                          "InstanceType": "c5.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                      }
                ]
            }
      ]
}
```

Esempio 10: Avviare le istanze spot in un parco istanze ottimizzato per la capacità con priorità

Nell'esempio seguente viene illustrato come configurare un parco istanze spot con una strategia di allocazione spot che ottimizza la capacità che applica la priorità in base al miglior tentativo.

Quando si utilizza la strategia di allocazione `capacityOptimizedPrioritized`, è possibile utilizzare il parametro `Priority` per specificare le priorità dei pool di capacità spot, dove a un numero inferiore corrisponde la priorità più alta. È inoltre possibile impostare la stessa priorità per diversi pool di capacità spot, se si preferisce non applicare priorità differenti. Se non si imposta una priorità per un pool, il pool verrà considerato ultimo in termini di priorità.

Per assegnare priorità ai pool di capacità spot, è necessario impostare `AllocationStrategy` su `capacityOptimizedPrioritized`. Il parco istanze spot ottimizzerà innanzitutto la capacità, ma rispetterà le priorità sulla base del miglior tentativo (ad esempio, se il rispetto delle priorità non influirà in modo significativo sulla capacità del parco istanze spot di fornire capacità ottimale). Questa è una buona opzione per i carichi di lavoro in cui è necessario ridurre al minimo la possibilità di interruzioni e la preferenza per determinati tipi di istanza è importante.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. Ogni pool ha una priorità, dove a un numero inferiore corrisponde la priorità più alta. La capacità obiettivo è di 50

Istanze spot. Il parco istanze EC2 tenta di avviare 50 istanze spot nel pool di capacità spot con la priorità più alta sulla base del miglior tentativo, ma prima ottimizza la capacità.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Priority": 1,
                            "AvailabilityZone": "us-west-2a"
                       },
                        {
                            "InstanceType": "m4.2xlarge",
                            "Priority": 2,
                            "AvailabilityZone": "us-west-2b"
                        },
                        {
                            "InstanceType": "c5.2xlarge",
                            "Priority": 3,
                            "AvailabilityZone": "us-west-2b"
                        }
                    ]
             }
       ]
}
```

Esempio 11: Avvio di istanze Spot in un parco istanze priceCapacityOptimized

Nell'esempio seguente viene illustrato come configurare un parco istanze spot con una strategia di allocazione spot che ottimizza sia la capacità sia il prezzo più basso. Per ottimizzare la capacità tenendo conto del prezzo, è necessario impostare la `AllocationStrategy` spot su `priceCapacityOptimized`.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. La capacità obiettivo è di 50 Istanze spot. Il parco istanze spot tenta di avviare 50 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando, scegliendo al contempo il pool con il prezzo più basso.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
                     {
                          "InstanceType": "r4.2xlarge",
                          "AvailabilityZone": "us-west-2a"
                     },
                     {
                          "InstanceType": "m4.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                     },
                     {
                          "InstanceType": "c5.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                     }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

Esempio 12: configurazione della selezione del tipo di istanza basata su attributi

Nell'esempio seguente viene illustrato come configurare un parco istanze spot in modo da utilizzare la selezione del tipo di istanza basata su attributi per identificare i tipi di istanza. Per specificare gli attributi di istanza richiesti, specifica gli attributi nella struttura `InstanceRequirements`.

Nell'esempio precedente, vengono specificati due attributi di istanza:

- `VCpuCount`: viene specificato un minimo di 2 vCPU. Poiché non è specificato alcun massimo, non esiste un limite massimo.
- `MemoryMiB`: viene specificato un minimo di 4 MiB di memoria. Poiché non è specificato alcun massimo, non esiste un limite massimo.

Verranno identificati tutti i tipi di istanza con 2 o più vCPU e 4 MiB o più di memoria. Tuttavia, la protezione dei prezzi e la strategia di allocazione potrebbero escludere alcuni tipi di istanze quando il parco istanze spot alloca le istanze.

Per un elenco e le descrizioni di tutti i possibili attributi che puoi specificare, consulta InstanceRequirementsAmazon EC2 API Reference.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

Quote del parco istanze

Alle istanze avviate da un parco istanze EC2 o da una serie di istanze Spot si applicano le consuete quote di Amazon EC2 (in precedenza chiamate limiti), ad esempio limiti di istanze spot e limiti di volume.

Inoltre, si applicano le quote seguenti:

Descrizione della quota	Quota
Il numero di flotte EC2 e flotte Spot per regione di tipo `maintain` e `request` negli stati `active` `deleted_running` `cancelled_running`	1.000 [1] [2] [3]
Il numero di flotte EC2 di tipo `instant`	Illimitato
Il numero di pool di capacità Spot (combinazione unica di tipo di istanza e sottorete) per flotte EC2 e flotte Spot di tipo e `maintain` `request`	300 [1]
Il numero di pool di capacità Spot (combinazione unica di tipo di istanza e sottorete) per flotte EC2 di tipo `instant`	Illimitato
La dimensione dei dati utente in una specifica di avvio	16 KB [2]
La capacità obiettivo per il parco istanze EC2 o la serie di istanze Spot	10.000
La capacità obiettivo per tutti i parchi istanze EC2 e le serie di istanze Spot in una regione	100.000 [1]
Una richiesta di parco istanze EC2 o una richiesta di parco istanze spot non può comprendere Regioni diverse.	

Descrizione della quota	Quota
Una richiesta di parco istanze EC2 o una richiesta di parco istanze spot non può comprendere sottoreti diverse della stessa zona di disponibilità.	

[1] Queste quote si applicano ai parchi istanze EC2 e alle serie di istanze Spot.

[2] Tali quote sono rigide. Non puoi richiedere l'aumento di queste quote.

[3] Dopo aver eliminato un parco istanze EC2 o annullato una richiesta di serie di istanze Spot, e se hai specificato che il parco istanze non deve terminare le istanze spot quando hai eliminato o annullato la richiesta, la richiesta del parco istanze entra nello stato `deleted_running` (parco istanze EC2) o `cancelled_running` (serie di istanze Spot) e l'esecuzione delle istanze continua finché non viene interrotta o terminata manualmente. Se termini le istanze, la richiesta del parco istanze assume lo stato `deleted_terminating` (parco istanze EC2) o `cancelled_terminating` (serie di istanze Spot) e non conta ai fini di questa quota. Per ulteriori informazioni, consulta Eliminazione di un parco istanze EC2 e Annullare una richiesta di parco istanze spot.

Richiesta di un aumento della quota per la capacità obiettivo

Se hai bisogno di estendere la quota di default per la capacità obiettivo, puoi richiedere un aumento della quota.

Come richiedere un aumento della quota per la capacità obiettivo

1. Apri il modulo AWS Support Center Create case.
2. Selezionare Service limit increase (Aumento limiti del servizio).
3. In Limit type (Tipo di limite), scegli EC2 Fleet (parco istanze EC2).
4. Per Regione, scegli la AWS regione in cui richiedere l'aumento della quota.
5. In Limit (Limite), scegli Target Fleet Capacity per Fleet (in units) (Capacità del parco istanze di destinazione per parco istanze [in unità]) oppure Target Fleet Capacity per Region (in units) (Capacità del parco istanze di destinazione per regione [in unità]), a seconda della quota che desideri aumentare.
6. In New limit value (Nuovo valore limite), inserisci il valore della nuova quota.

7. Per richiedere un aumento per un'altra quota, scegli Add another request (Aggiungi un'altra richiesta) e ripeti i passaggi da 4 a 6.
8. In Use case description (Descrizione del caso d'uso), inserisci il motivo della richiesta di aumento della quota.
9. In Contact options (Opzioni di contatto), specifica la lingua e il metodo di contatto preferiti.
10. Scegli Invia.

Monitoraggio di Amazon EC2

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle istanze Amazon Elastic Compute Cloud (Amazon EC2) e delle soluzioni. AWS È necessario raccogliere i dati di monitoraggio da tutte le parti delle AWS soluzioni in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. Prima di iniziare il monitoraggio di Amazon EC2, è opportuno creare un piano di monitoraggio che includa:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse intendi eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

Dopo aver definito gli obiettivi del monitoraggio e aver creato il tuo piano di monitoraggio, la fase successiva consiste in stabilire una baseline per le normali prestazioni Amazon EC2 nel tuo ambiente. È necessario misurare le prestazioni Amazon EC2 in diversi orari e in diverse condizioni di carico. Durante il monitoraggio di Amazon EC2, è necessario archiviare una cronologia dei dati di monitoraggio raccolti. Puoi comparare prestazioni Amazon EC2 correnti con questi dati storici per aiutarti a identificare i modelli di prestazioni normali e le anomalie di prestazioni, oltre a ideare metodi per gestirli. Ad esempio, puoi monitorare l'utilizzo della CPU, I/O su disco e l'utilizzo della rete per le istanze EC2. Quando le prestazioni non rientrano nella baseline stabilita, può essere necessario riconfigurare o ottimizzare l'istanza per ridurre l'utilizzo della CPU, migliorare l'I/O su disco o ridurre il traffico di rete.

Per stabilire una baseline, devi monitorare almeno gli elementi seguenti:

Voce da monitorare	Parametro Amazon EC2	Agente/registri di monitoraggio CloudWatch
Utilizzo CPU	CPUUtilization	
Utilizzo rete	NetworkIn NetworkOut	

Voce da monitorare	Parametro Amazon EC2	Agente/registri di monitoraggio CloudWatch
Prestazioni disco	DiskReadOps DiskWriteOps	
Letture/scritture su disco	DiskReadBytes DiskWriteBytes	
Utilizzo memoria, utilizzo scambio disco, utilizzo spazio disco, utilizzo file di pagina, raccolta log		[Istanze Linux e Windows Server] Raccogli parametri e log dalle istanze Amazon EC2 e dai server locali con l'agente CloudWatch [Migrazione dal precedente agente CloudWatch Logs su istanze di Windows Server] Migrazione della raccolta di registri delle istanze di Windows Server all'agente CloudWatch

Monitoraggio automatico e manuale

AWS fornisce diversi strumenti che puoi utilizzare per monitorare Amazon EC2. Alcuni di questi strumenti possono essere configurati in modo che eseguano automaticamente il monitoraggio, mentre altri richiedono l'intervento manuale.

Strumenti di monitoraggio

- Strumenti di monitoraggio automatici
- Strumenti di monitoraggio manuali

Strumenti di monitoraggio automatici

Per controllare Amazon EC2 e segnalare l'eventuale presenza di problemi, puoi usare gli strumenti di monitoraggio automatici seguenti:

- Controlli dello stato del sistema: monitora i AWS sistemi necessari per utilizzare l'istanza per assicurarti che funzionino correttamente. Questi controlli rilevano problemi con l'istanza che richiedono l' AWS intervento per la riparazione. Quando una verifica di stato del sistema ha esito negativo, puoi scegliere se attendere la risoluzione del problema da parte di AWS oppure puoi risolverlo direttamente (ad esempio, arrestando e riavviando o terminando e sostituendo un'istanza). Esempi di problemi che causano il mancato superamento dei controlli dello stato del sistema:
  - Perdita di connettività di rete
  - Perdita di alimentazione elettrica del sistema
  - Problemi di software sull'host fisico
  - Problemi hardware sull'host fisico che incidono sulla raggiungibilità della rete

  Per ulteriori informazioni, consulta Verifiche dello stato delle istanze.
- Verifiche dello stato delle istanze – Monitorano la configurazione del software e della rete della singola istanza. Tali verifiche rilevano i problemi per la cui risoluzione è richiesto il tuo intervento. Se l'esito della verifica dello stato di un'istanza è negativo, solitamente è necessario risolvere direttamente il problema (ad esempio, riavviando l'istanza o apportando modifiche al sistema operativo). Esempi di problemi che potrebbero causare il mancato superamento delle verifiche dello stato dell'istanza:
  - Verifiche dello stato del sistema non riuscite
  - Configurazione non corretta di rete o startup
  - Memoria esaurita
  - File system danneggiato
  - Kernel non compatibile

  Per ulteriori informazioni, consulta Verifiche dello stato delle istanze.
- CloudWatch Allarmi Amazon: monitora una singola metrica in un periodo di tempo specificato ed esegui una o più azioni in base al valore della metrica rispetto a una determinata soglia in diversi periodi di tempo. L'operazione è una notifica inviata a un topic Amazon Simple Notification Service (Amazon SNS) o alla policy di Dimensionamento automatico Amazon EC2. Gli allarmi

richiamano azioni solo per modifiche di stato sostenute. CloudWatch gli allarmi non richiameranno azioni semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.

- Amazon EventBridge: automatizza i tuoi AWS servizi e rispondi automaticamente agli eventi di sistema. Gli eventi AWS dei servizi vengono forniti quasi EventBridge in tempo reale e puoi specificare azioni automatiche da intraprendere quando un evento corrisponde a una regola che scrivi. Per ulteriori informazioni, consulta What is Amazon EventBridge? .
- Amazon CloudWatch Logs: monitora, archivia e accedi ai tuoi file di registro da istanze Amazon EC2 o altre AWS CloudTrail fonti. Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.
- CloudWatch agente: raccogli log e metriche a livello di sistema sia dagli host che dai guest sulle istanze EC2 e sui server locali. Per ulteriori informazioni, consulta la sezione Raccolta di metriche e log da istanze Amazon EC2 e server locali con l' CloudWatch agente nella Amazon User Guide. CloudWatch

Strumenti di monitoraggio manuali

Un'altra parte importante del monitoraggio di Amazon EC2 consiste nel monitorare manualmente gli elementi che gli script di monitoraggio, i controlli di stato e gli CloudWatch allarmi non coprono. Le dashboard di Amazon EC2 e CloudWatch della console forniscono una at-a-glance panoramica dello stato del tuo ambiente Amazon EC2.

- Nel pannello di controllo di Amazon EC2 sono visualizzati:
  - Stato dei servizi ed eventi pianificati per regione
  - Stato istanza
  - Verifiche di stato
  - Stato allarme
  - Dettagli parametri istanza (nel riquadro di navigazione, fare clic su Instances (Istanze), selezionare un'istanza, quindi fare clic sulla scheda Monitoring (Monitoraggio))
  - Dettagli parametri volume (nel riquadro di navigazione, fare clic su Volumes (Volumi), selezionare un volume, quindi fare clic sulla scheda Monitoring (Monitoraggio))
- Amazon CloudWatch Dashboard mostra:
  - Stato e allarmi attuali

- Grafici degli allarmi e delle risorse
- Stato di integrità dei servizi

Inoltre, puoi utilizzare CloudWatch per effettuare le seguenti operazioni:

- Creare grafici dei dati di monitoraggio di Amazon EC2 per la risoluzione di problemi e rilevare tendenze
- Cerca e sfoglia tutte le metriche AWS delle tue risorse
- Crea e modifica gli allarmi per ricevere le notifiche dei problemi.
- Visualizza le at-a-glance panoramiche dei tuoi allarmi e delle tue risorse AWS

Best practice per il monitoraggio

Utilizza le seguenti best practice per il monitoraggio come aiuto per le attività di monitoraggio di Amazon EC2.

- Rendere il monitoraggio una priorità per risolvere i piccoli problemi prima che diventino grandi problemi.
- Crea e implementa un piano di monitoraggio che raccolga i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica uno. Il tuo piano di monitoraggio deve riguardare, almeno, le domande seguenti:
  - Quali sono gli obiettivi del monitoraggio?
  - Di quali risorse intendi eseguire il monitoraggio?
  - Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
  - Quali strumenti di monitoraggio verranno utilizzati?
  - Chi eseguirà i processi di monitoraggio?
  - Chi deve ricevere una notifica quando si verifica un problema?
- Automatizzare le attività di monitoraggio il più possibile.
- Controllare i file di log delle istanze EC2.

Monitoraggio dello stato delle istanze

Puoi monitorare lo stato delle tue istanze visualizzando le relative verifiche dello stato e i relativi eventi pianificati.

Una verifica dello stato fornisce le informazioni risultanti dai controlli automatici eseguiti da Amazon EC2, che rilevano gli eventuali problemi specifici con le istanze. Le informazioni sul controllo dello stato, insieme ai dati forniti da Amazon CloudWatch, ti offrono una visibilità operativa dettagliata su ciascuna delle tue istanze.

Puoi anche visualizzare lo stato di specifici eventi pianificati per le istanze. Lo stato degli eventi fornisce informazioni sulle prossime attività pianificate per le istanze, come il riavvio o il ritiro. Fornisce anche l'ora di inizio e di fine pianificata per ciascun evento.

Indice

Verifiche dello stato delle istanze

Grazie al monitoraggio dello stato delle istanze, puoi determinare rapidamente se Amazon EC2 ha rilevato problemi che potrebbero impedire alle istanze di eseguire le applicazioni. Amazon EC2 esegue i controlli automatici su ogni istanza EC2 in esecuzione per individuare i problemi di hardware e software. Puoi visualizzare i risultati delle verifiche dello stato per individuare problemi specifici e rilevabili. I dati sullo stato degli eventi aumentano le informazioni già fornite da Amazon EC2 sullo stato di ciascuna istanza (ad esempio`running`,`stopping`,) e i parametri di utilizzo monitorati da CloudWatch Amazon (utilizzo della CPU, traffico di rete e attività del disco). `pending`

Le verifiche dello stato vengono eseguite ogni minuto e restituiscono un risultato positivo o negativo. Se vengono superate tutte le verifiche, lo stato complessivo dell'istanza sarà OK. Se invece una o più verifiche non vengono superate, lo stato complessivo sarà impaired (danneggiata). Le verifiche dello stato sono integrate in Amazon EC2 in modo tale da non poter essere disattivate o eliminate.

Quando un controllo dello stato fallisce, la CloudWatch metrica corrispondente per i controlli dello stato viene incrementata. Per ulteriori informazioni, consulta Parametri di controllo dello stato. È possibile utilizzare queste metriche per creare CloudWatch allarmi che vengono attivati in base al risultato dei controlli di stato. Ad esempio, puoi creare un allarme che ti avvisi se il risultato delle verifiche dello stato di una specifica istanza è negativo. Per ulteriori informazioni, consulta Creazione e modifica degli allarmi di controllo dello stato.

Puoi anche creare un CloudWatch allarme Amazon che monitora un'istanza Amazon EC2 e ripristina automaticamente l'istanza se viene danneggiata a causa di un problema sottostante. Per ulteriori informazioni, consulta Resilienza delle istanze.

Indice

Tipi di verifica dello stato

Esistono tre tipi di controlli dello stato.

Verifiche dello stato del sistema

I controlli dello stato del sistema monitorano i AWS sistemi su cui viene eseguita l'istanza. Tali verifiche rilevano i problemi sottostanti della tua istanza per la cui risoluzione è richiesto l'intervento di AWS . Quando un controllo dello stato del sistema fallisce, puoi scegliere di AWS attendere che il problema venga risolto oppure puoi risolverlo da solo. Puoi arrestare e avviare manualmente le istanze supportate da Amazon EBS, operazione che nella maggior parte dei casi comporta la migrazione dell'istanza a un nuovo host. Per le istanze Linux supportate dall'instance store, puoi terminare e sostituire l'istanza. Per le istanze di Windows, il volume root deve essere un volume Amazon EBS; l'archivio istanze non è supportato per il volume root. Si noti che i volumi dell'instance store sono effimeri e tutti i dati vengono persi quando l'istanza viene arrestata.

Di seguito sono riportati esempi di problemi che possono causare il mancato superamento delle verifiche dello stato del sistema:

- Perdita di connettività di rete
- Perdita di alimentazione elettrica del sistema
- Problemi di software sull'host fisico
- Problemi hardware sull'host fisico che incidono sulla raggiungibilità della rete

Se un controllo dello stato del sistema fallisce, incrementiamo la metrica StatusCheckFailed_System.

Istanze Bare Metal

Se esegui un riavvio dal sistema operativo su un'istanza bare metal, il controllo dello stato del sistema potrebbe restituire temporaneamente uno stato di errore. Quando l'istanza diventa disponibile, il controllo dello stato del sistema deve restituire uno stato di riuscita.

Verifiche dello stato delle istanze

Verifiche dello stato delle istanze Monitorano la configurazione del software e della rete della singola istanza. Amazon EC2 verifica lo stato di integrità dell'istanza inviando una richiesta ARP (Address Resolution Protocol) all'interfaccia di rete (NIC). Tali verifiche rilevano i problemi per la cui risoluzione è richiesto il tuo intervento. Se l'esito della verifica dello stato di un'istanza è negativo, solitamente devi risolvere direttamente il problema (ad esempio riavviando l'istanza o modificandone la configurazione).

> **Note**
>
> Le distribuzioni Linux recenti che utilizzano `systemd-networkd` per la configurazione di rete potrebbero riportare i controlli di integrità in modo diverso rispetto alle distribuzioni precedenti. Durante il processo di avvio, questo tipo di rete può iniziare prima e potenzialmente terminare prima di altre attività di avvio, che possono influire anche sullo stato dell'istanza. I controlli dello stato che dipendono dalla disponibilità della rete possono segnalare lo stato di integrità prima del completamento di altre attività.

Di seguito sono riportati esempi di problemi che possono causare il mancato superamento delle verifiche dello stato delle istanze:

- Verifiche dello stato del sistema non riuscite
- Configurazione errata di rete o startup
- Memoria esaurita
- File system danneggiato
- Kernel non compatibile
- [Istanze Windows] Durante il riavvio dell'istanza o durante il raggruppamento di un'istanza Windows archiviata in un pacchetto, un controllo dello stato dell'istanza segnala un errore fino a quando l'istanza non diventa nuovamente disponibile.

Se il controllo dello stato dell'istanza fallisce, incrementiamo la metrica _Instance. StatusCheckFailed

Istanze Bare Metal

Se esegui un riavvio dal sistema operativo su un'istanza bare metal, il controllo dello stato dell'istanza potrebbe restituire temporaneamente uno stato di errore. Quando l'istanza diventa disponibile, il controllo dello stato dell'istanza deve restituire uno stato di riuscita.

Controlli dello stato dei volumi EBS collegati

I controlli dello stato dei volumi EBS collegati verificano se i volumi Amazon EBS collegati a un'istanza sono raggiungibili e in grado di completare operazioni di I/O. Il parametro `StatusCheckFailed_AttachedEBS` è un valore binario che segnala un deterioramento nel caso in cui uno o più volumi EBS collegati all'istanza non siano in grado di completare le operazioni di I/O. Questi controlli dello stato rilevano problemi di fondo con l'infrastruttura di calcolo o Amazon EBS. Quando la metrica di controllo dello stato EBS allegata fallisce, puoi AWS attendere la risoluzione del problema oppure puoi intraprendere azioni, come sostituire i volumi interessati o arrestare e riavviare l'istanza.

Di seguito sono riportati esempi di problemi che possono causare il mancato superamento dei controlli dello stato dei volumi EBS collegati:

- Problemi hardware o software sui sottosistemi di archiviazione alla base dei volumi EBS
- Problemi hardware sull'host fisico che incidono sulla raggiungibilità dei volumi EBS
- Problemi di connettività tra l'istanza e i volumi EBS

È possibile utilizzare il parametro `StatusCheckFailed_AttachedEBS` per migliorare la resilienza di un carico di lavoro. Puoi utilizzare questa metrica per creare CloudWatch allarmi Amazon che vengono attivati in base al risultato del controllo dello stato. Ad esempio, è possibile eseguire il failover su una zona di disponibilità o su un'istanza secondaria quando si rileva un impatto prolungato. In alternativa, puoi monitorare le prestazioni di I/O di ciascun volume collegato utilizzando i CloudWatch parametri EBS per rilevare e sostituire il volume danneggiato. Se il carico di lavoro non determina I/O su nessuno dei volumi EBS collegati all'istanza e il controllo dello stato del volume EBS collegato segnala un problema, è possibile arrestare e avviare l'istanza per risolvere i problemi con l'host fisico che influiscono sulla raggiungibilità dei volumi EBS. Per ulteriori informazioni, consulta i CloudWatch parametri di Amazon per Amazon EBS

> **Note**
>
> - Il parametro di controllo dello stato dei volumi EBS collegati è disponibile solo per le istanze Nitro.
> - Puoi monitorare la metrica di controllo dello stato EBS allegata creando un CloudWatch allarme basato sulla metrica. `StatusCheckFailed_AttachedEBS` Non è possibile visualizzare questo controllo dello stato utilizzando il comando. describe-instance-status AWS CLI

Utilizzo dei controlli dello stato

È possibile utilizzare i controlli dello stato tramite la console e gli strumenti della riga di comando, come AWS CLI.

Argomenti

- Visualizzazione dei controlli di stato
- Creazione e modifica degli allarmi di controllo dello stato

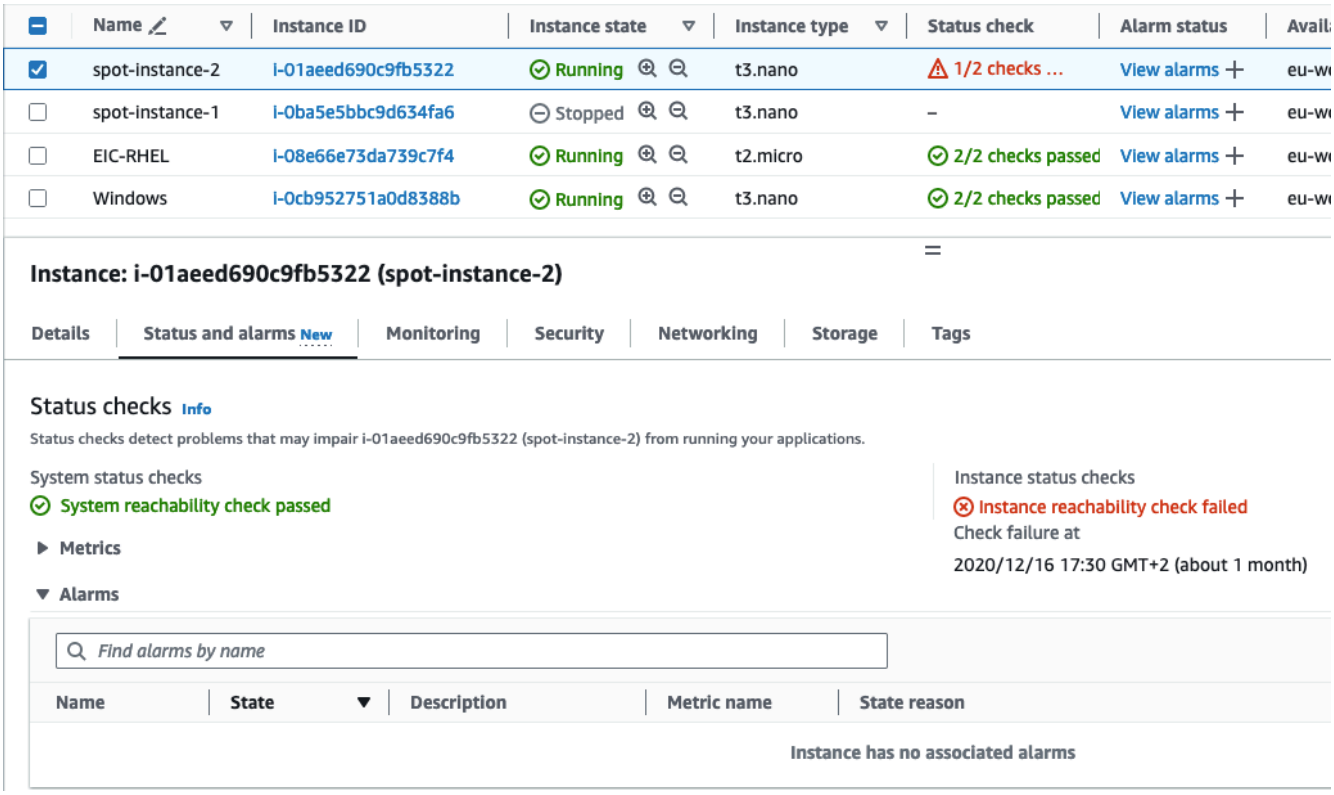
Visualizzazione dei controlli di stato

Per visualizzare i controlli dello stato, utilizza uno dei metodi seguenti.

Console

Per visualizzare i controlli di stato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Nella pagina Instances (Istanze), la colonna Status check (Verifiche dello stato) elenca lo stato operativo di ogni istanza.
4. Per visualizzare lo stato di una specifica istanza, seleziona l'istanza, quindi la scheda Stato e allarmi.



Se l'esito della verifica dello stato di un'istanza è negativo, solitamente devi risolvere direttamente il problema (ad esempio riavviando l'istanza o modificandone la configurazione). Per risolvere gli errori di controllo dello stato del sistema o dell'istanza sulle istanze Linux, consulta. Risolvi i problemi relativi alle istanze Linux con controlli di stato non riusciti

5. Per esaminare le CloudWatch metriche relative ai controlli dello stato, nella scheda Stato e allarmi, espandi Metriche per visualizzare i grafici relativi alle seguenti metriche:

   - Verifica stato non riuscita per il sistema
   - Verifica stato non riuscita per l'istanza

   Per ulteriori informazioni, consulta the section called “Parametri di controllo dello stato”.

Command line

È possibile visualizzare i controlli di stato per le istanze in esecuzione utilizzando il comando (). describe-instance-statusAWS CLI

Per visualizzare lo stato di tutte le istanze, utilizzare il comando seguente:

```
aws ec2 describe-instance-status
```

Per ottenere lo stato di tutte le istanze con lo stato di un'istanza di `impaired`, utilizzare il comando seguente:

```
aws ec2 describe-instance-status \
    --filters Name=instance-status.status,Values=impaired
```

Per ottenere lo stato di una singola istanza, utilizzare il comando seguente:

```
aws ec2 describe-instance-status \
    --instance-ids i-1234567890abcdef0
```

In alternativa, utilizzare i comandi seguenti:

- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)
- DescribeInstanceStatus(API di interrogazione Amazon EC2)

Se hai un'istanza Linux con un controllo dello stato non riuscito, consultaRisolvi i problemi relativi alle istanze Linux con controlli di stato non riusciti.

Creazione e modifica degli allarmi di controllo dello stato

Puoi utilizzare le metriche di controllo dello stato per creare CloudWatch allarmi che ti avvisino quando un controllo dello stato di un'istanza non è riuscito.

> **Important**
>
> Gli allarmi per il controllo dello stato e il controllo dello stato possono temporaneamente entrare in uno stato dei dati insufficiente se mancano dei punti dati metrici. Sebbene raro, ciò può accadere in caso di interruzione dei sistemi di reporting delle metriche, anche quando un'istanza è integra. Ti consigliamo di considerare questo stato come dati mancanti anziché come un errore nel controllo dello stato o una violazione dell'allarme, specialmente quando intraprendi azioni di arresto, interruzione, riavvio o ripristino sull'istanza in risposta.

Per creare un avviso di controllo dello stato, utilizza uno dei metodi seguenti:

Console

Utilizzare la procedura seguente per configurare un allarme che invii una notifica tramite e-mail o che arresti, termini o recuperi un'istanza se la verifica dello stato ha esito negativo.

Per creare un allarme di verifica dello stato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza, scegliere la scheda Status Checks (Verifiche dello stato), quindi Actions (Operazioni), Create status check alarm (Crea un allarme di verifica stato).
4. Nella pagina Gestisci gli CloudWatch allarmi, in Aggiungi o modifica allarme, scegli Crea un avviso.
5. Per la Alarm notification (Notifica allarme), attivare l'opzione per configurare le notifiche Amazon Simple Notification Service (Amazon SNS). Selezionare un argomento Amazon SNS esistente o immettere un nome per creare un nuovo argomento.

   Se aggiungi un indirizzo e-mail all'elenco dei destinatari o hai creato un nuovo argomento, Amazon SNS invia un'e-mail di conferma di abbonamento a ogni nuovo indirizzo. Ogni destinatario deve confermare l'abbonamento scegliendo il collegamento contenuto nel messaggio. Le notifiche di avviso vengono inviate solo agli indirizzi confermati.
6. Per Alarm action (Operazione allarme), attivare l'interruttore per specificare un'azione da eseguire quando viene attivato l'allarme. Selezionare l'azione.
7. Per Alarm thresholds (Soglie di allarme), selezionare il parametro e i criteri per l'allarme.

   È possibile lasciare le impostazioni di default per Group samples by (Raggruppa campioni per), ossia Average (Media), e per Type of data to sample (Tipo di dati da campionare), ossia Status check failed:either (Controllo stato non riuscito: una delle due voci), oppure modificarle in base alle proprie esigenze.

   In Consecutive period (Periodo consecutivo), impostare il numero di periodi che si desidera valutare e, in Period (Periodo), immettere la durata del periodo di valutazione prima di attivare l'allarme e inviare un'e-mail.
8. (Facoltativo) Per Sample metric data (Dati dei parametri di esempio), scegliere Add to dashboard (Aggiungi al pannello di controllo).
9. Scegliere Create (Crea).

Se necessario, puoi apportare delle modifiche a un allarme di stato delle istanze.

Per modificare un allarme di verifica dello stato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Azioni, Monitoraggio, Gestisci CloudWatch allarmi.
4. Nella pagina Gestisci gli CloudWatch allarmi, in Aggiungi o modifica allarme, scegli Modifica un avviso.
5. Per Search for alarm (Cerca allarme), scegli l'allarme da modificare.
6. Una volta completate le modifiche, scegliere Update (Aggiorna).

Command line

Nell'esempio seguente, l'allarme pubblica una notifica in un argomento SNS, `arn:aws:sns:us-west-2:111122223333:my-sns-topic`, quando l'istanza non supera la verifica di stato dell'istanza o del sistema per almeno due periodi consecutivi. La CloudWatch metrica utilizzata è. `StatusCheckFailed`

Per creare un allarme di controllo dello stato utilizzando il AWS CLI

1. Selezionare un argomento SNS esistente o crearne uno nuovo. Per ulteriori informazioni, consulta Using the AWS CLI with Amazon SNS nella Guida per l'AWS Command Line Interface utente.
2. Utilizza il seguente comando list-metrics per visualizzare i parametri Amazon disponibili per Amazon CloudWatch EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Usa il seguente put-metric-alarmcomando per creare l'allarme.

```
aws cloudwatch put-metric-alarm \
    --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \
    --metric-name StatusCheckFailed \
    --namespace AWS/EC2 \
    --statistic Maximum \
    --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
    --unit Count \
```

```
    --period 300 \
    --evaluation-periods 2 \
    --threshold 1 \
    --comparison-operator GreaterThanOrEqualToThreshold \
    --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

Il periodo è l'intervallo di tempo, in secondi, in cui vengono raccolte le CloudWatch metriche di Amazon. Questo esempio utilizza 300, ossia 60 secondi moltiplicati per 5 minuti. Il periodo di valutazione è il numero di periodi consecutivi in cui il valore del parametro deve essere paragonato alla soglia. Questo esempio usa 2. Le operazioni di allarme sono le operazioni da eseguire quando l'allarme viene attivato. Questo esempio configura l'allarme in modo che invii un'e-mail utilizzando Amazon SNS.

Eventi di modifica dello stato per le tue istanze

Amazon EC2 invia un `EC2 Instance State-change Notification` evento ad Amazon EventBridge quando lo stato di un'istanza cambia.

Di seguito vengono riportati dati di esempio per questo evento. In questo esempio, l'istanza è entrata nello stato `pending`.

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"
   ],
   "detail":{
      "instance-id":"i-abcd1111",
      "state":"pending"
   }
}
```

I valori possibili per `state` sono:

- `pending`

- `running`
- `stopping`
- `stopped`
- `shutting-down`
- `terminated`

Quando avvii un'istanza, il relativo stato diventa `pending` e quindi `running`. Quando arresti un'istanza, il relativo stato diventa `stopping` e quindi `stopped`. Quando termini un'istanza, il relativo stato diventa `shutting-down` e quindi `terminated`.

Ricezione di una notifica via e-mail quando un'istanza cambia stato

Per ricevere notifiche e-mail quando l'istanza cambia stato, crea un argomento Amazon SNS e quindi crea una EventBridge regola per l'`EC2 Instance State-change Notification`evento.

Creazione di un argomento SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel pannello di navigazione, scegli Topics (Argomenti).
3. Scegli Create topic (Crea argomento).
4. Per Tipo, scegliere Standard.
5. In Name (Nome) inserisci un nome per l'argomento.
6. Scegli Create topic (Crea argomento).
7. Scegli Crea sottoscrizione.
8. Per Protocollo, scegli E-mail.
9. In Endpoint inserisci l'indirizzo e-mail utilizzabile che riceve le notifiche.
10. Scegli Crea sottoscrizione.
11. Riceverai un messaggio e-mail con l'oggetto seguente: AWS Notification - Subscription Confirmation. Segui le istruzioni per confermare la tu sottoscrizione.

Per creare una regola EventBridge

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.

3. In Name (Nome) inserisci un nome per la regola.
4. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
5. Seleziona Successivo.
6. Per Event pattern (Modello eventi), procedi come segue:
   a. In Event source (Origine eventi), selezionare Servizi AWS.
   b. Per Servizio AWS, scegli EC2.
   c. Per Event Type (Tipo di evento), scegliere EC2 Instance State-change Notification (Notifica variazione di stato istanze EC2).
   d. Per impostazione predefinita, riceverai una notifica per qualsiasi modifica dello stato di qualsiasi istanza. Se preferisci, puoi selezionare stati o istanze specifiche.
7. Seleziona Successivo.
8. Specifica un obiettivo come segue:
   a. Per Target types (Tipi di target), scegli Servizio AWS.
   b. Per Select a target (Seleziona un target), scegli SNS topic (Argomento SNS).
   c. In Topic (Argomento), scegli l'argomento SNS creato nella procedura precedente.
9. Seleziona Successivo.
10. (Facoltativo) Aggiungi tag alla regola.
11. Seleziona Successivo.
12. Scegli Crea regola.
13. Per testare la regola, avvia un cambio di stato. Ad esempio, avvia un'istanza arrestata, arresta un'istanza in esecuzione o avvia una nuova istanza. Riceverai messaggi e-mail con l'oggetto seguente: AWS Notification Message. Il corpo dell'e-mail contiene i dati relativi all'evento.

Eventi pianificati per le istanze

AWS puoi pianificare eventi per le tue istanze, come il riavvio, l'arresto/avvio o il ritiro. Questi eventi non si verificano di frequente. Se una delle tue istanze sarà interessata da un evento programmato, AWS invia un'email all'indirizzo email associato al tuo AWS account prima dell'evento programmato. L'e-mail fornisce dettagli sull'evento, inclusa la data di inizio e di fine. A seconda dell'evento, potresti essere in grado di intervenire per controllarne la tempistica. AWS invia anche un AWS Health evento, che puoi monitorare e gestire utilizzando Amazon CloudWatch Events. Per ulteriori informazioni sul

monitoraggio AWS Health degli eventi con CloudWatch, consulta Monitoraggio AWS Health degli CloudWatch eventi con Events.

Gli eventi pianificati sono gestiti da AWS; non puoi pianificare eventi per le tue istanze. È possibile visualizzare gli eventi pianificati da AWS, personalizzare le notifiche degli eventi pianificati per includere o rimuovere tag dalla notifica e-mail ed eseguire azioni quando è pianificato il riavvio, il ritiro o l'arresto di un'istanza.

Per aggiornare le informazioni di contatto del proprio account in modo da essere certi di ricevere le notifiche sugli eventi pianificati, accedere alla pagina Account Settings (Impostazioni account).

> **Note**
>
> Quando un'istanza è interessata da un evento pianificato e fa parte di un gruppo con scalabilità automatica, il Dimensionamento automatico Amazon EC2 alla fine la sostituisce come parte dei controlli dell'integrità, senza ulteriori operazioni necessarie da parte tua. Per ulteriori informazioni sui controlli dell'integrità eseguiti dal Dimensionamento automatico Amazon EC2, consulta la sezione Controlli dell'integrità per le istanze a scalabilità automatica nella Guida per l'utente del Dimensionamento automatico Amazon EC2.

Indice

Tipi di eventi pianificati

Amazon EC2 supporta i seguenti tipi di eventi per le istanze, dove l'evento si verifica in un orario pianificato:

- Instance stop (Arresto dell'istanza): l'istanza viene arrestata all'orario pianificato. Quando la avvii nuovamente, l'istanza viene migrata a un nuovo host. Si applica solo alle istanze supportate da Amazon EBS.
- Instance retirement (Ritiro dell'istanza): l'istanza viene terminata all'orario pianificato se supportata da Amazon EBS o terminata se supportata da un instance store.
- Instance reboot (Riavvio dell'istanza): l'istanza viene riavviata all'orario pianificato.
- System reboot (Riavvio del sistema): l'host dell'istanze viene riavviato all'orario pianificato.
- System maintenance (Manutenzione del sistema): all'orario pianificato, l'istanza potrebbe essere temporaneamente interessata dalle operazioni di manutenzione della rete o dell'alimentazione elettrica.

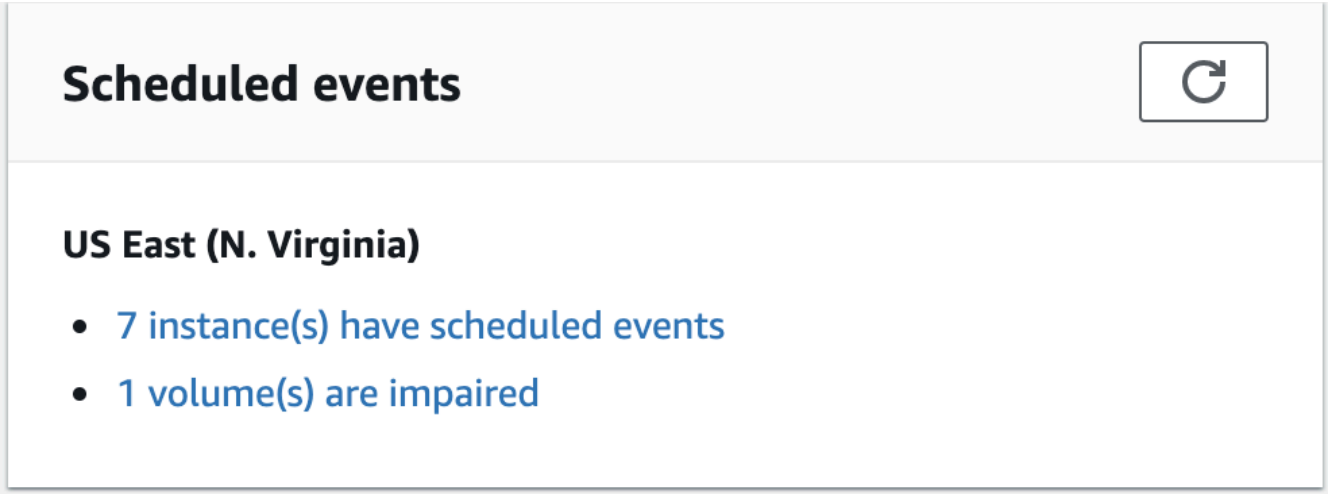
Visualizzazione degli eventi pianificati

Oltre a ricevere una notifica e-mail relativa agli eventi pianificati, puoi controllare tali eventi utilizzando uno dei seguenti metodi.

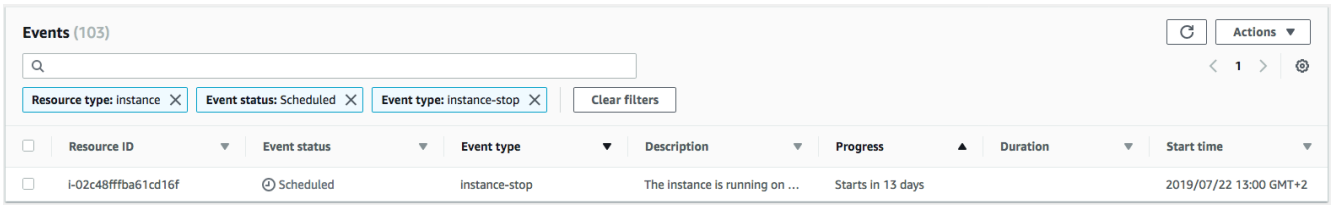
Console

Per visualizzare gli eventi pianificati per le istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. La dashboard visualizza in Eventi pianificati qualsiasi risorsa a cui è associato un evento.



3. Per maggiori dettagli, scegli Eventi nel pannello di navigazione. Vengono visualizzate le risorse a cui è associato un evento. Puoi filtrare per caratteristiche come il tipo di evento, il tipo di risorsa e la zona di disponibilità.



AWS CLI

Per visualizzare gli eventi pianificati per le istanze

Utilizza il comando describe-instance-status.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query "InstanceStatuses[].Events"
```

Il seguente esempio di output mostra un evento di riavvio.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

Di seguito è riportato un output di esempio che mostra un evento di ritiro di un'istanza.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
            "NotBefore": "2015-05-23T00:00:00.000Z"
```

```
        }
    ]
]
```

PowerShell

Come visualizzare gli eventi pianificati per le istanze utilizzando AWS Tools for Windows PowerShell

Utilizza il seguente comando Get-EC2InstanceStatus.

```
PS C:\> (Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

Di seguito è riportato un output di esempio che mostra un evento di ritiro di un'istanza.

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

Per visualizzare gli eventi pianificati per le istanze utilizzando i metadati dell'istanza

È possibile recuperare informazioni sugli eventi di manutenzione attivi per le istanze, dai metadati dell'istanza utilizzando Servizio di metadati dell'istanza Versione 2 o Servizio di metadati dell'istanza Versione 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

Segue un esempio di output con informazioni su un evento di riavvio del sistema pianificato, in formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

Per visualizzare la cronologia degli eventi completati o annullati per le istanze che utilizzano i metadati dell'istanza

È possibile recuperare informazioni sugli eventi completati o cancellati per le istanze dai metadati dell'istanza utilizzando Servizio di metadati dell'istanza Versione 2 o Servizio di metadati dell'istanza Versione 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

Segue un output di esempio con informazioni su un evento di riavvio del sistema che è stato cancellato e un evento di riavvio del sistema che è stato completato, in formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
```

```
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

Puoi utilizzarli AWS Health Dashboard per conoscere gli eventi che possono influire sulla tua istanza. AWS Health Dashboard Organizza i problemi in tre gruppi: problemi aperti, modifiche pianificate e altre notifiche. Il gruppo delle modifiche programmate contiene elementi in corso o prossimi.

Per ulteriori informazioni, consulta Nozioni di base su AWS Health Dashboard nella Guida per l'utente di AWS Health .

Personalizzazione delle notifiche di eventi pianificati

Puoi personalizzare le notifiche di eventi pianificati per includere tag nella notifica e-mail. Questo semplifica l'identificazione della risorsa interessata (istanze o Host dedicati) e l'assegnazione delle priorità alle operazioni per il prossimo evento.

Quando personalizzi le notifiche di eventi per includere i tag, puoi scegliere di includere:

- Tutti i tag associati alla risorsa interessata
- Solo tag specifici associati alla risorsa interessata

Ad esempio, supponi di assegnare i tag `application`, `costcenter`, `project` e `owner` a tutte le istanze. Puoi scegliere di includere tutti i tag nelle notifiche di eventi. In alternativa, se desideri visualizzare solo i tag `owner` e `project` nelle notifiche di eventi, puoi scegliere di includere solo tali tag.

Dopo aver selezionato i tag da includere, le notifiche di eventi includeranno l'ID risorsa (ID istanza o ID Host dedicato) e le coppie valore e chiave tag associate alla risorsa interessata.

Attività

- Inclusione dei tag nelle notifiche di eventi
- Rimozione di tag da notifiche di eventi
- Visualizzazione dei tag da includere nelle notifiche di eventi

Inclusione dei tag nelle notifiche di eventi

I tag che scegli di includere si applicano a tutte le risorse (istanze e Host dedicati) nell'area selezionata. Per personalizzare le notifiche di eventi in altre regioni, seleziona innanzitutto la regione richiesta e quindi esegui le fasi seguenti.

Puoi includere tag nelle notifiche di eventi utilizzando uno dei metodi seguenti.

Console

Per includere tag nelle notifiche di eventi

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Scegliere Actions (Operazioni), Manage event notifications (Gestisci notifiche eventi).
4. Attiva Inclusione dei tag nelle notifiche di eventi.
5. Eseguire una delle seguenti operazioni, a seconda dei tag che si desidera includere nelle notifiche di eventi:
   - Per includere tutti i tag associati all'istanza interessata o Host dedicato, selezionare Includi tutti i tag delle risorse.
   - Per selezionare i tag da includere, seleziona Scegli i tag da includere, quindi seleziona o inserisci le chiavi di tag.
6. Seleziona Salva.

AWS CLI

Per includere tutti i tag nelle notifiche di eventi

Utilizzate il AWS CLI comando register-instance-event-notification-attributes e impostate il `IncludeAllTagsOfInstance` parametro su. `true`

```
aws ec2 register-instance-event-notification-attributes \
```

```
    --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

Per includere tag specifici nelle notifiche di eventi

Utilizzate il AWS CLI comando register-instance-event-notification-attributes e specificate i tag da includere utilizzando il `InstanceTagKeys` parametro.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Rimozione di tag da notifiche di eventi

Puoi rimuovere i tag dalle notifiche di eventi utilizzando uno dei metodi descritti di seguito.

Console

Per rimuovere tag dalle notifiche di eventi

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Scegliere Actions (Operazioni), Manage event notifications (Gestisci notifiche eventi).
4. Per rimuovere tutti i tag dalle notifiche di eventi, disattiva Includi tag delle risorse nelle notifiche di eventi.
5. Per rimuovere tag specifici dalle notifiche degli eventi, scegli la X) per le chiavi di tag corrispondenti.
6. Seleziona Salva.

AWS CLI

Per rimuovere tutti i tag dalle notifiche di eventi

Utilizzate il AWS CLI comando deregister-instance-event-notification-attributes e impostate il `IncludeAllTagsOfInstance` parametro su. `false`

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

Per rimuovere tag specifici dalle notifiche di eventi

Utilizzate il AWS CLI comando deregister-instance-event-notification-attributes e specificate i tag da rimuovere utilizzando il `InstanceTagKeys` parametro.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Visualizzazione dei tag da includere nelle notifiche di eventi

Puoi visualizzare i tag da includere nelle notifiche di eventi utilizzando uno dei metodi descritti di seguito.

Console

Per visualizzare i tag da includere nelle notifiche di eventi

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Scegliere Actions (Operazioni), Manage event notifications (Gestisci notifiche eventi).

AWS CLI

Per visualizzare i tag da includere nelle notifiche di eventi

Utilizzate il comando describe-instance-event-notification-attributes AWS CLI .

```
aws ec2 describe-instance-event-notification-attributes
```

Utilizzo delle istanze per le quali è pianificato l'arresto o il ritiro

Quando AWS rileva un guasto irreparabile dell'host sottostante dell'istanza, pianifica l'arresto o la chiusura dell'istanza, a seconda del tipo di dispositivo root dell'istanza. Se il dispositivo root è un volume EBS, viene pianificato l'arresto dell'istanza. Se il dispositivo root è un volume instance store, viene pianificato la terminazione dell'istanza. Per ulteriori informazioni, consulta Ritiro dell'istanza.

> **Important**
>
> Tutti i dati archiviati nei volumi instance store vengono persi quando un'istanza viene arrestata, ibernata o terminata. Sono inclusi i volumi instance store collegati a un'istanza che ha un volume EBS come dispositivo root. Accertati di salvare i dati contenuti nei volumi instance store di cui potresti aver bisogno successivamente prima che l'istanza venga arrestata o terminata.

Operazioni per le istanze supportate da Amazon EBS

Puoi attendere che l'istanza venga arrestata come pianificato oppure puoi arrestare e avviare manualmente l'istanza, comportandone la migrazione in un nuovo host. Per ulteriori informazioni sull'arresto dell'istanza nonché sulle modifiche alla configurazione dell'istanza quando viene arrestata, consultare Arresta e avvia le istanze Amazon EC2.

È possibile automatizzare un arresto e un avvio immediato in risposta a un evento di arresto dell'istanza pianificato. Per ulteriori informazioni, consulta Automazione delle azioni per le istanze Amazon EC2 nella Guida per l'utente di AWS Health .

Operazioni per le istanze supportate da instance store

Ti consigliamo di avviare un'istanza sostitutiva dall'AMI più recente verso la quale migrare tutti i dati necessari prima della terminazione pianificata dell'istanza. Quindi puoi terminare l'istanza originale o attendere che venga terminata come pianificato.

Utilizzo delle istanze per le quali è pianificato il riavvio

Quando AWS deve eseguire attività come l'installazione di aggiornamenti o la manutenzione dell'host sottostante, può pianificare il riavvio dell'istanza o dell'host sottostante. Puoi ripianificare la maggior parte degli eventi di riavvio in modo che l'istanza venga riavviata in una data e ora specifica adatta alle tue esigenze.

Visualizzazione del tipo di evento di riavvio

È possibile visualizzare se un evento di riavvio è un riavvio di istanza o un riavvio del sistema utilizzando uno dei metodi descritti di seguito.

Console

Per visualizzare il tipo di evento di riavvio pianificato

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Scegliere Resource type: instance (Tipo di risorsa: istanza) dall'elenco dei filtri.
4. Per ogni istanza, vedere il valore nella colonna Event Type (Tipo di evento). Il valore è system-reboot o instance-reboot.

AWS CLI

Per visualizzare il tipo di evento di riavvio pianificato

Utilizza il comando describe-instance-status.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0
```

Per gli eventi di riavvio pianificato, il valore per `Code` sarà `system-reboot` o `instance-reboot`. Il seguente esempio di output mostra un evento `system-reboot`.

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

Operazioni per il riavvio delle istanze

Puoi attendere che il riavvio dell'istanza si verifichi entro la finestra pianificata, puoi ripianificare l'istanza per il riavvio a una data e ora adatta alle tue esigenze, oppure puoi riavviare l'istanza immediatamente nel momento in cui lo desideri.

Dopo il riavvio dell'istanza, l'evento pianificato viene annullato e la descrizione dell'evento aggiornata. La manutenzione in attesa dell'host sottostante è completata e puoi iniziare a utilizzare di nuovo la tua istanza una volta che è stata avviata completamente.

Operazioni per il riavvio del sistema

Non è possibile riavviare manualmente il sistema. Puoi attendere che il riavvio del sistema si verifichi entro la finestra pianificata oppure puoi ripianificare il riavvio a una data e ora adatta alle tue esigenze. Un riavvio di sistema viene normalmente completato in pochi minuti. Dopo il riavvio di sistema, l'istanza mantiene il suo indirizzo IP e nome DNS e gli eventuali dati sui volumi instance store locali vengono conservati. Una volta completato il riavvio di sistema, l'evento pianificato per l'istanza viene annullato e puoi verificare che il software sulla tua istanza funzioni come previsto.

In alternativa, se devi eseguire la manutenzione dell'istanza in un momento diverso, e non è possibile ripianificare il riavvio di sistema, puoi arrestare e avviare un'istanza supportata da Amazon EBS da migrare al nuovo host. Tuttavia, i dati sui volumi instance store locali non verranno conservati. È possibile inoltre automatizzare un arresto e un avvio immediato dell'istanza in risposta a un evento di riavvio del sistema pianificato. Per ulteriori informazioni, consulta Automazione delle operazioni per le istanze EC2 nella Guida per l'utente di AWS Health . In caso di un'istanza supportata da instance store, se non puoi ripianificare il riavvio di sistema, puoi avviare un'istanza sostitutiva dall'AMI più recente verso cui migrare tutti i dati necessari prima che la manutenzione venga avviata, quindi terminare l'istanza originale.

Utilizzo delle istanze per le quali è pianificata la manutenzione

Quando AWS deve gestire l'host sottostante per un'istanza, pianifica la manutenzione dell'istanza. Esistono due tipi di eventi di manutenzione: della rete e dell'alimentazione elettrica.

Durante la manutenzione della rete, le istanze per le quali è pianificato l'evento perdono la connettività di rete per un breve periodo di tempo. La normale connettività di rete dell'istanza viene ripristinata al completamento della manutenzione.

Durante la manutenzione dell'alimentazione elettrica, le istanze per le quali è pianificato l'evento vengono impostate sulla modalità offline per un breve periodo di tempo, quindi vengono riavviate. Tutte le impostazioni di configurazione dell'istanza vengono mantenute anche dopo il riavvio.

Una volta riavviata l'istanza (solitamente l'operazione richiede alcuni minuti), verifica che la tua applicazione funzioni come previsto. A questo punto, all'istanza non dovrebbero più essere associati eventi pianificati oppure, se ciò avvenisse, la descrizione dell'evento pianificato inizia con [Completed] ([Completato]). Talvolta può essere necessaria anche un'ora perché la descrizione dello stato dell'istanza venga aggiornata. Gli eventi di manutenzione completati vengono visualizzati nel pannello di controllo della console di Amazon EC2 per un massimo di una settimana.

Operazioni per le istanze supportate da Amazon EBS

Puoi attendere che la manutenzione venga eseguita come pianificato oppure puoi arrestare e avviare manualmente l'istanza, comportandone la migrazione in un nuovo host. Per ulteriori informazioni sull'arresto dell'istanza nonché sulle modifiche alla configurazione dell'istanza quando viene arrestata, consultare Arresta e avvia le istanze Amazon EC2.

È possibile automatizzare un arresto e un avvio immediato in risposta a un evento di manutenzione dell'istanza pianificato. Per ulteriori informazioni, consulta Automazione delle operazioni per le istanze EC2 nella Guida per l'utente di AWS Health .

Operazioni per le istanze supportate da instance store

Puoi attendere che la manutenzione venga eseguita come pianificato In alternativa, se desideri mantenere il normale funzionamento durante una finestra di manutenzione pianificata, puoi avviare un'istanza sostitutiva dall'AMI più recente verso cui migrare tutti i dati necessari prima che la manutenzione venga avviata, quindi terminare l'istanza originale.

Riprogrammazione di un evento pianificato

È possibile riprogrammare un evento in modo che si verifichi in una data e un'ora specifiche. Solo gli eventi con data di scadenza possono essere ripianificati. Esistono altre limitazioni per la ripianificazione di un evento.

È possibile ripianificare un evento utilizzando uno dei metodi descritti di seguito.

Console

Per riprogrammare un evento

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Scegliere Resource type: instance (Tipo di risorsa: istanza) dall'elenco dei filtri.

4. Selezionare una o più istanze, quindi selezionare Actions (Operazioni), Schedule Event (Pianificazione evento).

   Solo gli eventi che possiedono una data di scadenza dell'evento, indicata da un valore per Deadline (Scadenza), possono essere ripianificati. Se uno degli eventi selezionati non ha una data di scadenza, Actions (Operazioni), Schedule event (Pianificazione evento) è disabilitato.

5. In New start time (Nuova ora di inizio), inserire una nuova data e ora per il riavvio. La nuova data e ora deve essere precedente alla Event Deadline (Scadenza evento).

6. Seleziona Salva.

   Potrebbero essere necessari 1-2 minuti affinché l'ora di inizio dell'evento aggiornata sia visibile nella console.

AWS CLI

Per riprogrammare un evento

1. Solo gli eventi che possiedono una data di scadenza dell'evento, indicata da un valore per `NotBeforeDeadline`, possono essere ripianificati. Utilizzate il describe-instance-statuscomando per visualizzare il valore del `NotBeforeDeadline` parametro.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0
```

   Nell'esempio seguente viene illustrato un evento `system-reboot` che non può essere ripianificato in quanto `NotBeforeDeadline` contiene un valore.

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

2. Per riprogrammare l'evento, utilizzate il modify-instance-event-start comando -time. Specifica la nuova ora di inizio dell'evento usando il parametro `not-before`. La nuova data di inizio dell'evento deve precedere `NotBeforeDeadline`.

```
aws ec2 modify-instance-event-start-time \
    --instance-id i-1234567890abcdef0 \
    --instance-event-id instance-event-0d59937288b749b32 \
    --not-before 2019-03-25T10:00:00.000
```

   Potrebbero essere necessari uno o due minuti prima che il describe-instance-statuscomando restituisca il valore del parametro aggiornato`not-before`.

Limitazioni

- Solo gli eventi che possiedono una data di scadenza dell'evento possono essere ripianificati. L'evento può essere ripianificato fino alla data di scadenza dell'evento medesimo. La colonna Scadenza nella console e il `NotBeforeDeadline` campo nella AWS CLI indicano se l'evento ha una data di scadenza.
- Solo gli eventi non ancora iniziati possono essere ripianificati. La colonna Ora di inizio nella console e il `NotBefore` campo nella AWS CLI indicano l'ora di inizio dell'evento. Gli eventi pianificati per l'avvio nei prossimi 5 minuti non possono essere ripianificati.
- La nuova ora di inizio dell'evento deve essere almeno 60 minuti dopo l'ora corrente.
- In caso di ripianificazione di più eventi mediante la console, la data di scadenza dell'evento è determinata dalla data di scadenza dell'evento più vicina.

Definizione delle finestre degli eventi per gli eventi pianificati

Puoi definire finestre di eventi personalizzate con ricorrenza settimanale per eventi pianificati che riavviano, arrestano o terminano le istanze Amazon EC2. Puoi associare una o più istanze a una finestra di eventi. Se per tali istanze è programmato un evento pianificato, AWS programmerà gli eventi all'interno della finestra di eventi associata.

Puoi utilizzare le finestre di eventi per aumentare al massimo la disponibilità del carico di lavoro specificando le finestre di eventi che si verificano durante i periodi non di picco per il carico di lavoro. È inoltre possibile allineare le finestre di eventi alle pianificazioni di manutenzione interne.

Puoi definire una finestra di eventi specificando un insieme di intervalli di tempo. La durata minima per un intervallo di tempo è di 2 ore. Gli intervalli di tempo combinati devono essere pari ad almeno 4 ore.

È possibile associare una o più istanze a una finestra di eventi utilizzando ID istanza o tag istanza. Puoi inoltre associare host dedicati a una finestra di evento utilizzando l'ID host.

> **Warning**
>
> Le finestre di eventi sono applicabili solo agli eventi pianificati che arrestano, riavviano o terminano le istanze.
> Le finestre di eventi non sono applicabili a:
>
> - Eventi pianificati accelerati ed eventi di manutenzione della rete.
> - Manutenzione non programmata, ad esempio AutoRecovery riavvii non pianificati.

Utilizzo delle finestre di eventi

- Considerazioni
- Visualizzazione di finestre di eventi
- Creazione di finestre di eventi
- Modifica delle finestre di eventi
- Eliminazione di finestre di eventi
- Aggiunta di tag alle finestre di eventi

Considerazioni

- Tutti gli orari delle finestre di eventi sono in UTC.
- La durata minima settimanale della finestra di eventi è di 4 ore.
- Gli intervalli di tempo all'interno di una finestra di eventi devono essere di almeno 2 ore.
- A una finestra di eventi è possibile associare un solo tipo di destinazione (ID istanza, ID host dedicato o tag istanza).
- A una finestra di eventi è possibile associare un solo tipo di destinazione (ID istanza, ID host dedicato o tag istanza).

- A una finestra di eventi è possibile associare un massimo di 100 ID istanza o 50 ID host dedicati o 50 tag istanza. I tag istanza possono essere associati a qualsiasi numero di istanze.
- È possibile creare un massimo di 200 finestre di eventi per regione. AWS
- Più istanze associate alle finestre di eventi possono potenzialmente avere eventi pianificati nello stesso momento.
- Se AWS ha già programmato un evento, la modifica della finestra di un evento non cambierà l'ora dell'evento programmato. Se l'evento ha una data di scadenza, puoi riprogrammare l'evento.
- Puoi arrestare e avviare un'istanza prima dell'evento pianificato, il che migra l'istanza a un nuovo host e l'evento pianificato non avrà più luogo.

Visualizzazione di finestre di eventi

È possibile visualizzare le finestre di eventi utilizzando uno dei metodi descritti di seguito.

Console

Per visualizzare finestre di eventi

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Seleziona Operazioni, Gestisci finestre di eventi.
4. Seleziona una finestra di eventi per visualizzarne i dettagli.

AWS CLI

Per descrivere tutte le finestre di eventi

Utilizza il comando describe-instance-event-windows.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1
```

Output previsto

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0abcdef1234567890",
```

```
            "Name": "myEventWindowName",
            "CronExpression": "* 21-23 * * 2,3",
            "AssociationTarget": {
                "InstanceIds": [
                    "i-1234567890abcdef0",
                    "i-0598c7d356eba48d7"
                ],
                "Tags": [],
                "DedicatedHostIds": []
            },
            "State": "active",
            "Tags": []
        }

        ...

    ],
    "NextToken": "9d624e0c-388b-4862-a31e-a85c64fc1d4a"
}
```

Per descrivere una finestra di eventi specifica

Utilizzate il describe-instance-event-windowscomando con il `--instance-event-window-id` parametro per descrivere una finestra di evento specifica.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

Per descrivere le finestre di eventi che corrispondono a uno o più filtri

Utilizzate il describe-instance-event-windowscomando con il `--filters` parametro. Nell'esempio seguente, il filtro `instance-id` viene utilizzato per descrivere tutte le finestre di eventi associate all'istanza specificata.

Quando viene utilizzato un filtro, si stabilisce una corrispondenza diretta. Tuttavia, il filtro `instance-id` è diverso. Se non esiste una corrispondenza diretta con l'ID istanza, viene restituito alle associazioni indirette con la finestra di eventi, ad esempio i tag dell'istanza o l'ID host dedicato (se l'istanza si trova su un host dedicato).

Per l'elenco dei filtri supportati, vedere describe-instance-event-windowsnella Guida di AWS CLI riferimento.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --max-results 100 \
    --next-token <next-token-value>
```

Output previsto

Nell'esempio seguente, l'istanza si trova su un host dedicato, associato alla finestra di eventi.

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0dbc0adb66f235982",
            "TimeRanges": [
                {
                    "StartWeekDay": "sunday",
                    "StartHour": 2,
                    "EndWeekDay": "sunday",
                    "EndHour": 8
                }
            ],
            "Name": "myEventWindowName",
            "AssociationTarget": {
                "InstanceIds": [],
                "Tags": [],
                "DedicatedHostIds": [
                    "h-0140d9a7ecbd102dd"
                ]
            },
            "State": "active",
            "Tags": []
        }
    ]
}
```

Creazione di finestre di eventi

È possibile creare una o più finestre di eventi. Per ogni finestra di eventi, è necessario specificare uno o più blocchi temporali. Ad esempio, puoi creare una finestra di eventi con blocchi temporali che

si verificano ogni giorno alle 4 del mattino per 2 ore. Oppure puoi creare una finestra di eventi con blocchi temporali che si verificano la domenica dalle 2 alle 4 e il mercoledì dalle 3 alle 5.

Per i vincoli della finestra di eventi, consulta Considerazioni discusso precedenza in questo argomento.

Le finestre di eventi vengono ripetute settimanalmente finché non vengono eliminate.

Per creare una finestra di eventi, utilizza uno dei seguenti metodi:

Console

Per creare una finestra di eventi

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Seleziona Operazioni, Gestisci finestre di eventi.
4. Seleziona Crea finestra di eventi dell'istanza.
5. Per Nome finestra di eventi inserisci un nome descrittivo per la finestra.
6. Per Pianificazione della finestra di eventi, scegli di specificare i blocchi temporali nella finestra di eventi utilizzando il generatore di pianificazione cron o specificando gli intervalli di tempo.
   - Se si sceglie Generatore di pianificazione cron, specifica quanto segue:
     1. Per Giorni (UTC) specifica i giorni della settimana in cui viene visualizzata la finestra di eventi.
     2. Per Ora di inizio (UTC), specifica l'ora in cui inizia la finestra di evento.
     3. Per Durata, specifica la durata dei blocchi temporali nella finestra di eventi. La durata minima per un blocco temporale è di 2 ore. La durata minima della finestra di eventi deve essere pari o superiore a 4 ore in totale. Tutti gli orari sono in UTC.
   - Se scegli Intervalli di tempo, seleziona Aggiungi un nuovo intervallo di tempo e specifica il giorno e l'ora di inizio e il giorno e l'ora di fine. Ripeti l'operazione per ogni intervallo di tempo. La durata minima per un intervallo di tempo è di 2 ore. La durata minima per tutti gli intervalli di tempo combinati deve essere pari o superiore a 4 ore in totale.
7. (Facoltativo) Per Dettagli destinazione, associa una o più istanze alla finestra di evento in modo che, se le istanze sono pianificate per la manutenzione, l'evento pianificato si verifichi durante la finestra di eventi associata. È possibile associare una o più istanze a una finestra

di eventi utilizzando gli ID istanza o i tag di istanza. Puoi inoltre associare gli host dedicati a una finestra di eventi utilizzando l'ID host.

Tieni presente che è possibile creare la finestra di eventi senza associare una destinazione alla finestra. Successivamente, potrai modificare la finestra per associare una o più destinazioni.

8. (Facoltativo) Per Tag della finestra di eventi, seleziona Aggiungi tag e inserisci la chiave e il valore per il tag. Ripetere per ogni tag.
9. Seleziona Crea finestra di eventi.

AWS CLI

Per creare una finestra evento utilizzando la AWS CLI, è necessario innanzitutto creare la finestra degli eventi, quindi associare una o più destinazioni alla finestra dell'evento.

Creazione di una finestra di eventi

Durante la creazione della finestra di eventi, è possibile definire un insieme di intervalli temporali o un'espressione cron, ma non entrambi.

Per creare una finestra di eventi con un intervallo temporale

Utilizzate il create-instance-event-windowcomando e specificate il `--time-range` parametro. Non è possibile specificare anche il parametro `--cron-expression`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
```

```
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Per creare una finestra di eventi con un'espressione cron

Utilizzate il create-instance-event-windowcomando e specificate il `--cron-expression` parametro. Non è possibile specificare anche il parametro `--time-range`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
```

```
    }
}
```

Associazione di una destinazione a una finestra di eventi

Tuttavia, un solo tipo di destinazione (ID istanza, ID host dedicati o tag istanza) può essere associato a una finestra di eventi.

Per associare i tag di istanza a una finestra di eventi

Utilizzate il associate-instance-event-windowcomando e specificate il `instance-event-window-id` parametro per specificare la finestra dell'evento. Per associare i tag di istanza, specificare il parametro `--association-target` e per i valori dei parametri specifica uno o più tag.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
```

```
    }
}
```

Per associare una o più istanze a una finestra di eventi

Utilizzate il associate-instance-event-windowcomando e specificate il `instance-event-window-id` parametro per specificare la finestra dell'evento. Per associare le istanze, specifica il parametro `--association-target` e per i valori dei parametri specifica uno o più ID istanza.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Per associare un host dedicato a una finestra di eventi

Utilizzate il associate-instance-event-windowcomando e specificate il `instance-event-window-id` parametro per specificare la finestra dell'evento. Per associare le istanze, specifica il parametro `--association-target` e per i valori dei parametri specifica uno o più ID host dedicati.

```
aws ec2 associate-instance-event-window \
```

```
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

Modifica delle finestre di eventi

È possibile modificare tutti i campi di una finestra di eventi tranne il relativo ID. Ad esempio, quando inizia l'ora legale, è possibile modificare la pianificazione della finestra di eventi. Per le finestre di eventi esistenti, potrebbe essere necessario aggiungere o rimuovere destinazioni.

Per modificare una finestra di eventi, utilizza uno dei seguenti metodi.

Console

Per modificare una finestra di eventi

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Seleziona Operazioni, Gestisci finestre di eventi.
4. Selezionare la finestra degli eventi da modificare, quindi seleziona Operazioni, Modifica finestra di eventi per l'istanza.
5. Modifica i campi nella finestra di eventi e seleziona Modifica finestra di eventi.

AWS CLI

Per modificare una finestra di eventi utilizzando AWS CLI, è possibile modificare l'intervallo di tempo o l'espressione cron e associare o dissociare uno o più obiettivi alla finestra dell'evento.

Modifica dell'ora della finestra di eventi

Durante la modifica della finestra di eventi, è possibile modificare un intervallo temporale o un'espressione cron, ma non entrambi.

Per modificare l'intervallo temporale di una finestra di eventi

Utilizzate il modify-instance-event-windowcomando e specificate la finestra dell'evento da modificare. Specifica il parametro `--time-range` per modificare l'intervallo di tempo. Non è possibile specificare anche il parametro `--cron-expression`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
```

```
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Per modificare un insieme di intervalli temporali di una finestra di eventi

Utilizzate il modify-instance-event-windowcomando e specificate la finestra dell'evento da modificare. Specifica il parametro `--time-range` per modificare l'intervallo di tempo. Non è possibile specificare il parametro `--cron-expression` nella stessa chiamata.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
```

```
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Per modificare l'espressione cron di una finestra di eventi

Utilizzate il modify-instance-event-windowcomando e specificate la finestra dell'evento da modificare. Specifica il parametro `--cron-expression` per modificare l'espressione cron. Non è possibile specificare anche il parametro `--time-range`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
```

```
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Modifica delle destinazioni associate a una finestra di eventi

È possibile associare ulteriori destinazioni a una finestra di eventi. Da una finestra di eventi è inoltre possibile dissociare le destinazioni esistenti. Tuttavia, un solo tipo di destinazione (ID istanza, ID host dedicati o tag istanza) può essere associato a una finestra di eventi.

Come associare ulteriori destinazioni a una finestra di eventi

Per le istruzioni su come associare le destinazioni a una finestra di eventi, consulta Associate a target with an event window.

Per dissociare i tag di istanza da una finestra di eventi

Utilizzate il disassociate-instance-event-windowcomando e specificate il `instance-event-window-id` parametro per specificare la finestra dell'evento. Per dissociare i tag di istanza, specifica il parametro `--association-target` e per i valori dei parametri specifica uno o più tag.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
```

```
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Per dissociare una o più istanze da una finestra di eventi

Utilizzate il disassociate-instance-event-windowcomando e specificate il `instance-event-window-id` parametro per specificare la finestra dell'evento. Per dissociare le istanze, specifica il parametro `--association-target` e per i valori dei parametri specifica uno o più ID istanza.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Per dissociare un host dedicato da una finestra di eventi

Utilizzate il disassociate-instance-event-windowcomando e specificate il `instance-event-window-id` parametro per specificare la finestra dell'evento. Per dissociare un host dedicato, specifica il parametro `--association-target` e per i valori dei parametri specifica uno o più ID host dedicati.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Output previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Eliminazione di finestre di eventi

È possibile eliminare una finestra di eventi alla volta utilizzando uno dei metodi descritti di seguito.

Console

Per eliminare una finestra di eventi

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Seleziona Operazioni, Gestisci finestre di eventi.
4. Seleziona la finestra di eventi da eliminare, quindi seleziona Operazioni, Elimina finestra di eventi per l'istanza.
5. Quando richiesto, digitare **`delete`**, quindi scegliere Delete (Elimina).

AWS CLI

Per eliminare una finestra di eventi

Utilizzate il delete-instance-event-windowcomando e specificate la finestra dell'evento da eliminare.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

Per forzare l'eliminazione di una finestra di eventi

Utilizza il parametro `--force-delete` se la finestra di eventi è attualmente associata a destinazioni.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

Output previsto

```
{
    "InstanceEventWindowState": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "State": "deleting"
    }
}
```

Aggiunta di tag alle finestre di eventi

È possibile taggare una finestra di eventi nel momento in cui viene creata o successivamente.

Per taggare una finestra di eventi al momento della creazione, consulta Creazione di finestre di eventi.

Per taggare una finestra di eventi, utilizza uno dei seguenti metodi:

Console

Per applicare i tag a una finestra di eventi esistente

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Seleziona Operazioni, Gestisci finestre di eventi.
4. Seleziona la finestra di eventi da taggare, quindi seleziona Operazioni, Gestisci tag della finestra di eventi per l'istanza.
5. Per aggiungere un tag, scegli Aggiungi tag. Ripetere per ogni tag.
6. Seleziona Salva.

AWS CLI

Per applicare i tag a una finestra di eventi esistente

Utilizzare il comando create-tags per aggiungere un tag alle risorse esistenti. Nell'esempio seguente, la finestra di eventi esistente è taggata con Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources iew-0abcdef1234567890 \
    --tags Key=purpose,Value=test
```

Monitora le tue istanze utilizzando CloudWatch

Puoi monitorare le tue istanze utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi di Amazon EC2 in metriche leggibili quasi in tempo reale. Queste statistiche vengono registrate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione Web.

Per impostazione predefinita, Amazon EC2 invia dati metrici CloudWatch in periodi di 5 minuti. Per inviare i dati metrici relativi alla tua istanza CloudWatch in periodi di 1 minuto, puoi abilitare il monitoraggio dettagliato sull'istanza. Per ulteriori informazioni, consulta Abilitazione o disabilitazione del monitoraggio dettagliato per le istanze.

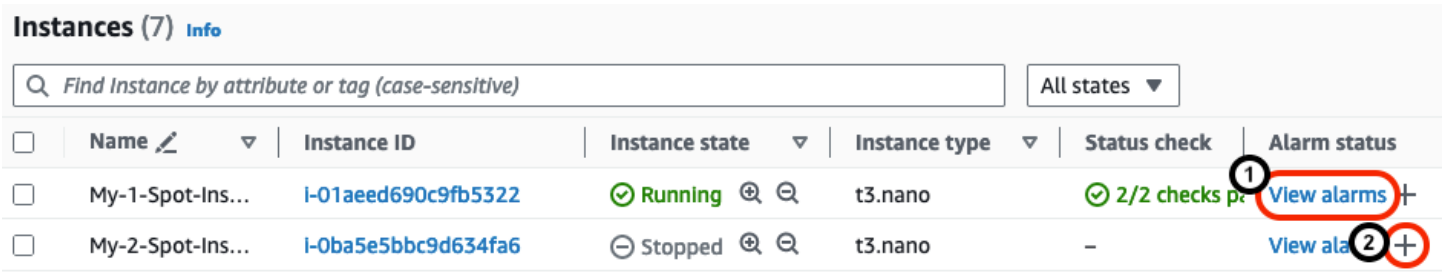
La console Amazon EC2 mostra una serie di grafici basati sui dati grezzi di Amazon. CloudWatch A seconda delle tue esigenze, potresti preferire ottenere i dati per le tue istanze da Amazon CloudWatch anziché dai grafici nella console.

Per informazioni sulla CloudWatch fatturazione e sui costi di Amazon, consulta CloudWatch fatturazione e costi nella Amazon CloudWatch User Guide.

Indice

Gestisci gli CloudWatch allarmi per le tue istanze EC2 nella console EC2

Dalla schermata Istanze nella console Amazon EC2, puoi gestire gli allarmi CloudWatch Amazon per le tue istanze. Nella tabella Istanze, la colonna di stato degli allarmi fornisce due controlli della console: un controllo per la visualizzazione degli allarmi e un altro per crearli o modificarli. La schermata seguente indica questi controlli della console, numerati 1 (Visualizza allarmi) e 2 (un segno + per creare o modificare un avviso).



Visualizza gli allarmi dalla schermata Istanze

Puoi visualizzare gli allarmi di ogni istanza dalla schermata Istanze.

Per visualizzare l'allarme di un'istanza dalla schermata Istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Nella tabella Istanze, per l'istanza scelta, scegli Visualizza avvisi (numerati 1 nella schermata precedente).

4. Nella finestra Dettagli dell'allarme per ***i-0123456789example***, scegli il nome dell'allarme per visualizzarlo nella console. CloudWatch

Crea allarmi dalla schermata Istanze

È possibile creare un allarme per ogni istanza dalla schermata Istanze.

Per creare un allarme per un'istanza dalla schermata Istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Nella tabella Istanze, per l'istanza scelta, scegliete il segno più (numerato 2 nella schermata precedente).
4. Nella schermata Gestisci gli CloudWatch allarmi, crea il tuo allarme. Per ulteriori informazioni, consulta Crea un CloudWatch allarme per un'istanza.

Modifica gli allarmi dalla schermata Istanze

È possibile modificare l'allarme per un'istanza dalla schermata Istanze.

Per modificare un avviso per un'istanza dalla schermata Istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Nella tabella Istanze, per l'istanza scelta, scegli il segno più (numerato 2 nella schermata precedente).
4. Nella schermata Gestisci gli CloudWatch allarmi, modifica la sveglia. Per ulteriori informazioni, consulta Modificare o eliminare un CloudWatch allarme nella Amazon CloudWatch User Guide.

Abilitazione o disabilitazione del monitoraggio dettagliato per le istanze

Per impostazione predefinita, per l'istanza è abilitato il monitoraggio base. È possibile scegliere di abilitare il monitoraggio dettagliato.

La tabella seguente evidenzia le differenze tra il monitoraggio base e il monitoraggio dettagliato delle istanze.

Tipo di monitoraggio	Descrizione	Costi
Monitoraggio base	Solo i parametri di controllo dello stato sono disponibili in periodi di 1 minuto. Tutti gli altri parametri sono disponibili in periodi di 5 minuti.	Nessun costo.
Monitoraggio dettagliato	Tutti i parametri, inclusi i parametri di controllo dello stato, sono disponibili in periodi di 1 minuto. Per ottenere questo tipo di dati, devi abilitarne esplicitamente la ricezione per l'istanza. Per le istanze per le quali hai abilitato il monitoraggio dettagliato, puoi ricevere inoltre i dati aggregati sui gruppi di istanze simili.	Ti viene addebitato il costo in base alla metrica inviata a CloudWatch. Non verrà addebitato alcun costo per l'archiviazione dei dati. Per ulteriori informazioni, consulta la pagina dei prezzi del piano a pagamento e dell'Esempio 1 - EC2 Detailed Monitoring sulla pagina CloudWatch dei prezzi di Amazon.

Argomenti

- Autorizzazioni IAM richieste
- Abilitazione del monitoraggio dettagliato
- Disattivazione del monitoraggio dettagliato

Autorizzazioni IAM richieste

Per abilitare il monitoraggio dettagliato per un'istanza, l'utente deve disporre dell'autorizzazione per utilizzare l'operazione API MonitorInstances. Per disabilitare il monitoraggio dettagliato per un'istanza, l'utente deve disporre dell'autorizzazione per utilizzare l'operazione API UnmonitorInstances.

Abilitazione del monitoraggio dettagliato

Puoi abilitare il monitoraggio dettagliato su un'istanza al momento dell'avvio o dopo averla eseguita o arrestata. L'abilitazione del monitoraggio dettagliato su un'istanza non riguarda il monitoraggio

dei volumi EBS collegati all'istanza. Per ulteriori informazioni, consulta i CloudWatch parametri di Amazon per Amazon EBS.

Console

Per abilitare il monitoraggio dettagliato per un'istanza esistente

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Azioni, Monitoraggio e risoluzione dei problemi, Gestione del monitoraggio dettagliato.
4. Nella pagina dei dettagli di Detailed monitoring (Monitoraggio dettagliato), per Detailed monitoring (Monitoraggio dettagliato) selezionare la casella di controllo Enable (Abilita).
5. Seleziona Salva.

Per abilitare il monitoraggio dettagliato durante l'avvio di un'istanza

Quando avvii un'istanza utilizzando la console Amazon EC2, in Dettagli avanzati, seleziona la casella di controllo Monitoraggio CloudWatch dettagliato.

AWS CLI

Per abilitare il monitoraggio dettagliato per un'istanza esistente

Utilizza il comando monitor-instances seguente per abilitare il monitoraggio dettagliato per le istanze specificate.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Per abilitare il monitoraggio dettagliato durante l'avvio di un'istanza

Utilizza il comando run-instances con il contrassegno `--monitoring` per abilitare il monitoraggio dettagliato.

```
aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

Disattivazione del monitoraggio dettagliato

Puoi disattivare il monitoraggio dettagliato su un'istanza al momento dell'avvio o dopo averla eseguita o arrestata.

Console

Per disattivare il monitoraggio dettagliato

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Azioni, Monitoraggio e risoluzione dei problemi, Gestisci il monitoraggio dettagliato.
4. Nella pagina dei dettagli di Detailed monitoring (Monitoraggio dettagliato), per Detailed monitoring (Monitoraggio dettagliato) deselezionare la casella di controllo Enable (Abilita).
5. Seleziona Salva.

AWS CLI

Per disattivare il monitoraggio dettagliato

Utilizza il comando unmonitor-instances seguente per disattivare il monitoraggio dettagliato per le istanze specificate.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

Elenca le CloudWatch metriche disponibili per le tue istanze

Amazon EC2 invia i parametri ad Amazon. CloudWatch Puoi utilizzare il AWS Management Console AWS CLI, the o un'API per elencare i parametri a cui invia Amazon EC2. CloudWatch Per impostazione predefinita, ciascun punto dati copre i 5 minuti seguenti all'orario di avvio delle attività dell'istanza. Se hai abilitato il monitoraggio dettagliato, ciascun punto dati copre il primo minuto di attività successivo all'orario di avvio. Per le statistiche Minimum (Minimo), Maximum (Massimo) e Average (Media), la granularità minima per i parametri forniti da EC2 è di 1 minuto.

Per informazioni su come ottenere le statistiche relative a questi parametri, consulta Ottenere le statistiche sui parametri delle istanze.

Indice

Parametri dell'istanza

Il namespace `AWS/EC2` include i seguenti parametri di istanza.

Parametro	Descrizione	Unità	Statistiche significative
`CPUUtilization`	La percentuale di tempo della CPU fisica che Amazon EC2 utilizza per eseguire l'istanza EC2, che include il tempo impiegato per eseguire sia il codice utente che il codice Amazon EC2. A un livello molto alto, `CPUUtilization` è la somma di `CPUUtilization` guest e `CPUUtilization` hypervisor. Gli strumenti del sistema operativo possono mostrare una percentuale diversa rispetto a quella CloudWatch dovuta a fattori quali la simulazione di dispositivi legacy, la configura zione di dispositivi non legacy, i carichi di lavoro	Percentuale	• Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
	che richiedono interruzioni, la migrazione in tempo reale e l'aggiornamento in tempo reale.		
`DiskReadOps`	Operazioni di lettura completate da tutti i volumi di instance store disponibili per l'istanza in un determinato periodo di tempo. Per calcolare le operazioni I/O medie al secondo (IOPS) per il periodo, dividi il numero di operazioni totali nel periodo per il numero di secondi in quel periodo. Se non vi sono volumi instance store, il valore è 0 oppure il parametro non è riportato.	Conteggio	• Somma • Media • Minimo • Massimo
`DiskWriteOps`	Operazioni di scrittura completate in tutti i volumi di instance store disponibili per l'istanza in un determinato periodo di tempo. Per calcolare le operazioni I/O medie al secondo (IOPS) per il periodo, dividi il numero di operazioni totali nel periodo per il numero di secondi in quel periodo. Se non vi sono volumi instance store, il valore è 0 oppure il parametro non è riportato.	Conteggio	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`DiskReadBytes`	Byte letti da tutti i volumi di instance store disponibili per l'istanza. Questo parametro viene utilizzato per determinare il volume dei dati che l'applicazione legge dal disco rigido dell'istanza. Può essere utilizzato per determinare la velocità dell'applicazione. Il numero segnalato è il numero di byte ricevuti durante il periodo. Se utilizzi il monitoraggio di base (5 minuti), puoi dividere questo numero per 300 per trovare i byte/secondo. Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione `DIFF_TIME` matematica CloudWatch metrica per trovare i byte al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch as`m1`, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `DiskReadBytes` in byte/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch Se non vi sono volumi instance store, il valore è 0 oppure il parametro non è riportato.	Byte	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`DiskWriteBytes`	Byte scritti in tutti i volumi di instance store disponibili per l'istanza. Questo parametro viene utilizzato per determinare il volume dei dati che l'applicazione scrive sul disco rigido dell'istanza. Può essere utilizzato per determinare la velocità dell'appl icazione. Il numero segnalato è il numero di byte ricevuti durante il periodo. Se utilizzi il monitorag gio di base (5 minuti), puoi dividere questo numero per 300 per trovare i byte/secondo. Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica per trovare i byte `DIFF_TIME` al secondo. Ad esempio, se hai rappresentato graficamente CloudWatc h `asm1`, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `DiskWriteBytes` in byte/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch Se non vi sono volumi instance store, il valore è 0 oppure il parametro non è riportato.	Byte	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`MetadataNoToken`	Il numero di volte in cui l'Instance Metadata Service (IMDS) è stato effettuato con successo utilizzando un metodo che non utilizza un token. Questa metrica viene utilizzata per determinare se esistono processi che accedono ai metadati dell'istanza che utilizzano Instance Metadata Service versione 1 (IMDSv1), che non utilizza un token. Se tutte le richieste utilizzano sessioni supportate da token, ad esempio Instance Metadata Service Version 2 (IMDSv2), il valore è 0. Per ulteriori informazioni, consulta Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2.	Conteggio	• Somma • Percentili
`MetadataNoTokenRejected`	Il numero di volte in cui è stata tentata una chiamata IMDSv1 dopo la disattivazione di IMDSv1. Se viene visualizzata questa metrica, indica che una chiamata IMDSv1 è stata tentata e rifiutata. Puoi riattivare IMDSv1 o assicurarti che tutte le chiamate utilizzino IMDSv2. Per ulteriori informazioni, consulta Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2.	Conteggio	• Somma • Percentili

Parametro	Descrizione	Unità	Statistiche significative
`NetworkIn`	Il numero di byte ricevuti dall'istanza su tutte le interfacce di rete. Questo parametro identifica il volume del traffico di rete in entrata in una singola istanza. Il numero segnalato è il numero di byte ricevuti durante il periodo. Se utilizzi il monitoraggio di base (5 minuti) e la statistica è Sum (Somma), puoi dividere questo numero per 300 per trovare i byte/secondo. Se hai il monitoraggio dettagliato (1 minuto) e la statistica è Sum (Somma), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica per trovare i byte al secondo. `DIFF_TIME` Ad esempio, se hai rappresentato graficamente CloudWatch as`m1`, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `NetworkIn` in byte/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch	Byte	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`NetworkOut`	Il numero di byte inviati dall'istanza su tutte le interfacce di rete. Questo parametro identifica il volume del traffico di rete in uscita da una singola istanza. Il numero segnalato è il numero di byte inviati durante il periodo. Se utilizzi il monitoraggio di base (5 minuti) e la statistica è Sum (Somma), puoi dividere questo numero per 300 per trovare i byte/secondo. Se hai il monitoraggio dettagliato (1 minuto) e la statistica è Sum (Somma), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica per trovare i byte `DIFF_TIME` al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch as`m1`, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `NetworkOut` in byte/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch	Byte	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`NetworkPackets In`	Il numero di pacchetti ricevuti dall'istanza su tutte le interfacce di rete. Questo parametro identifica il volume del traffico in entrata in termini di numero di pacchetti su una singola istanza. Questo parametro è disponibile solo per il monitoraggio di base (periodi di 5 minuti). Per calcolare il numero di pacchetti al secondo (PPS) ricevuti dall'istanza per 5 minuti, dividi il valore della statistica Sum (Somma) per 300. Puoi anche usare la funzione matematica CloudWatch metrica per trovare i pacchetti `DIFF_TIME` al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch asm1, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `NetworkPacketsIn` in pacchetti/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch	Conteggio	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`NetworkPackets0ut`	Il numero di pacchetti inviati dall'istanza su tutte le interfacce di rete. Questo parametro identifica il volume del traffico in uscita in termini di numero di pacchetti su una singola istanza. Questo parametro è disponibile solo per il monitoraggio di base (periodi di 5 minuti). Per calcolare il numero di pacchetti al secondo (PPS) inviati dall'istanza nell'arco dei 5 minuti, dividi il valore della statistica Sum (Somma) per 300. Puoi anche usare la funzione matematica CloudWatch metrica per trovare i pacchetti `DIFF_TIME` al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch asm1, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `NetworkPackets0ut` in pacchetti/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch	Conteggio	• Somma • Media • Minimo • Massimo

Parametri dei crediti CPU

Il namespace `AWS/EC2` include i seguenti parametri di credito CPU per le istanze dalle prestazioni ottimizzabili.

Parametro	Descrizione	Unità	Statistiche significative
`CPUCredit Usage`	Il numero di crediti CPU spesi dall'istanza per l'utilizzo della CPU. Un credito CPU equivale a un vCPU che viene eseguito al 100% dell'util	Crediti (vCPU/minuti)	• Somma • Media • Minimo

Parametro	Descrizione	Unità	Statistiche significative
	izzo per un minuto o una combinazione equivalente di vCPU, utilizzo e tempo (per esempio, un vCPU che viene eseguito al 50% dell'utilizzo per due minuti o due vCPU che vengono eseguiti al 25% dell'utilizzo per due minuti). I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti. Se specifichi un periodo superiore a 5 minuti, usa la statistica `Sum` al posto di quella `Average`.		• Massimo

Parametro	Descrizione	Unità	Statistiche significative
`CPUCreditBalance`	Il numero di crediti CPU ottenuti, che un'istanza ha accumulato da quando è stata lanciata o avviata. Per le T2 Standard `CPUCreditBalance` include anche il numero di crediti di lancio che sono stati accumulati. I crediti vengono accumulati nel saldo del credito dopo che sono stati ottenuti e rimossi dal saldo del credito una volta spesi. Il saldo del credito ha un limite massimo, determinato dalla dimensione dell'istanza. Una volta che il limite viene raggiunto, tutti i nuovi crediti guadagnati vengono scartati. Per le T2 Standard, i crediti di lancio non contano per il limite. I crediti in `CPUCreditBalance` sono disponibili affinché l'istanza li spenda per andare oltre l'utilizzo di base della CPU. Quando l'istanza è in fase di esecuzione, i crediti in `CPUCreditBalance` non scadono. Quando un'istanza T3 o T3a si arresta, il valore `CPUCreditBalance` persiste per sette giorni. Successivamente, tutti i crediti accumulati vengono persi. Quando un'istanza T2 si arresta, il valore `CPUCreditBalance` non persiste e tutti i crediti accumulati vengono persi. I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti.	Crediti (vCPU/minuti)	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`CPUSurplusCreditBalance`	Il numero di crediti extra spesi da un'istanza a `unlimited` quando il rispettivo valore `CPUCreditBalance` è pari a zero. Il valore `CPUSurplusCreditBalance` viene saldato con i crediti CPU ottenuti. Se il numero dei crediti extra va oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore, i crediti extra spesi, eccedenti il limite, incorreranno in costi aggiuntivi. I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti.	Crediti (vCPU/minuti)	• Somma • Media • Minimo • Massimo
`CPUSurplusCreditsCharged`	Il numero di crediti extra spesi da un'istanza, che non sono saldati con i crediti CPU ottenuti e che pertanto incorrono in costi aggiuntivi. I crediti extra spesi subiscono costi aggiuntivi quando si verifica uno dei seguenti casi: • I crediti extra spesi vanno oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore. I crediti extra spesi, che eccedono il limite, subiscono costi aggiuntivi alla fine dell'ora; • l'istanza viene arrestata o terminata; • l'istanza passa da `unlimited` a `standard`. I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti.	Crediti (vCPU/minuti)	• Somma • Media • Minimo • Massimo

Parametri degli host dedicati

Lo spazio dei nomi `AWS/EC2` include i seguenti parametri per gli host dedicati T3.

Parametro	Descrizione	Unità	Statistiche significative
`DedicatedHostCPUUtilization`	La percentuale di capacità di calcolo allocata attualmente in uso dalle istanze in esecuzione sull'host dedicato.	Percentuale	• Somma • Media • Minimo • Massimo

Parametri Amazon EBS delle istanze basate su Nitro

Lo spazio dei nomi `AWS/EC2` include i seguenti parametri Amazon EBS aggiuntivi per le istanze basate su Nitro che non sono istanze bare metal.

Parametro	Descrizione	Unità	Statistiche significative
`EBSReadOps`	Operazioni di lettura completate da tutti i volumi Amazon EBS collegati all'istanza in un determinato periodo di tempo. Per calcolare le operazioni di I/O di lettura medie al secondo (IOPS di lettura) per il periodo, dividi le operazioni totali nel periodo per il numero di secondi in quel periodo. Se utilizzi il monitoraggio base (5 minuti), puoi dividere questo numero per 300 per calcolare le operazioni IOPS di lettura. Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica per trovare le operazioni `DIFF_TIME` al secondo. Ad esempio, se hai rappresentato graficamente CloudWatc	Conteggio	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
	h asm1, la formula matematica metrica `m1/(DIFF_TIME(m1))` restituisce la metrica `EBSReadOps` in operazioni/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch		
`EBSWriteOps`	Le operazioni di scrittura completate su tutti i volumi EBS collegati all'istanza in un determinato periodo di tempo. Per calcolare le operazioni di I/O di scrittura medie al secondo (IOPS di scrittura) per il periodo, dividi le operazioni totali nel periodo per il numero di secondi in quel periodo. Se utilizzi il monitoraggio base (5 minuti), puoi dividere questo numero per 300 per calcolare le operazioni IOPS di scrittura. Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica per trovare le operazioni `DIFF_TIME` al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch asm1, la formula matematica metrica `m1/(DIFF_TIME(m1))` restituisce la metrica `EBSWriteOps` in operazioni/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch	Conteggio	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`EBSReadBytes`	I byte letti da tutti i volumi EBS collegati all'istanza in un determinato periodo di tempo. Il numero segnalato è il numero di byte letti durante il periodo. Se utilizzi il monitoraggio base (5 minuti), puoi dividere questo numero per 300 per trovare i byte letti al secondo. Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica per trovare i byte `DIFF_TIME` al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch asm1, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `EBSReadBytes` in byte/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch	Byte	• Somma • Media • Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`EBSWriteBytes`	I byte scritti su tutti i volumi EBS collegati all'istanza in un determinato periodo di tempo. Il numero segnalato è il numero di byte scritti durante il periodo. Se utilizzi il monitoraggio base (5 minuti), puoi dividere questo numero per 300 per trovare i byte scritti al secondo. Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica per trovare i byte `DIFF_TIME` al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch as `m1`, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `EBSWriteBytes` in byte/secondo. Per ulteriori informazioni *`DIFF_TIME`* e altre funzioni matematiche metriche, consulta Use metric Math nella Amazon User Guide. CloudWatch	Byte	• Somma • Media • Minimo • Massimo
`EBSIOBalance%`	Fornisce informazioni sulla percentuale di crediti di I/O rimanenti nel burst bucket. Questo parametro è disponibile solo per il monitoraggio base. Questo parametro è disponibile solo per alcune istanze di dimensioni `*.4xlarge` e inferiori che supportano le prestazioni massime per soli 30 minuti almeno una volta ogni 24 ore. La statistica `Sum` non è applicabile a questo parametro.	Percentuale	• Minimo • Massimo

Parametro	Descrizione	Unità	Statistiche significative
`EBSByteBalance%`	Fornisce informazioni sulla percentuale di crediti del throughput rimanenti nel burst bucket. Questo parametro è disponibile solo per il monitoraggio base. Questo parametro è disponibile solo per alcune istanze di dimensioni `*.4xlarge` e inferiori che supportano le prestazioni massime per soli 30 minuti almeno una volta ogni 24 ore. La statistica `Sum` non è applicabile a questo parametro.	Percentuale	• Minimo • Massimo

Per informazioni sui parametri forniti per i tuoi volumi EBS, consulta Metrics for Amazon EBS Volumes nella Amazon EBS User Guide. Per informazioni sui parametri forniti per i parchi istanze Spot, consulta CloudWatch metriche per Spot Fleet.

Parametri di controllo dello stato

Per impostazione predefinita, i parametri di controllo dello stato sono disponibili a una frequenza di 1 minuto senza costi aggiuntivi. Per un'istanza appena avviata, i dati del parametro di controllo dello stato sono disponibili solo dopo che l'istanza ha completato lo stato di inizializzazione (entro pochi minuti da quando l'istanza assume lo stato `running`). Per ulteriori informazioni sui controlli di stato EC2, vedere Verifiche dello stato delle istanze.

Il namespace `AWS/EC2` include i parametri di controllo dello stato descritti di seguito.

Parametro	Descrizione	Unità	Statistiche significative
`StatusCheckFailed`	Indica se l'istanza ha superato sia il controllo dello stato dell'istanza che il controllo dello stato del sistema nell'ultimo minuto.	Conteggio	• Somma • Media

Parametro	Descrizione	Unità	Statistiche significative
	Questo parametro può essere `0` (superato) o 1 (non riuscito). Per impostazione predefinita, questo parametro è disponibile a una frequenza di 1 minuto senza costi aggiuntivi.		
`StatusCheckFailed_Instance`	Indica se l'istanza ha superato il controllo dello stato dell'istanza nell'ultimo minuto. Questo parametro può essere `0` (superato) o 1 (non riuscito). Per impostazione predefinita, questo parametro è disponibile a una frequenza di 1 minuto senza costi aggiuntivi.	Conteggio	• Somma • Media
`StatusCheckFailed_System`	Indica se l'istanza ha superato il controllo dello stato del sistema nell'ultimo minuto. Questo parametro può essere `0` (superato) o 1 (non riuscito). Per impostazione predefinita, questo parametro è disponibile a una frequenza di 1 minuto senza costi aggiuntivi.	Conteggio	• Somma • Media
`StatusCheckFailed_AttachedEBS`	Indica se l'istanza ha superato il controllo dello stato del volume EBS collegato nell'ultimo minuto. Questo parametro può essere `0` (superato) o 1 (non riuscito). Per impostazione predefinita, questo parametro è disponibile a una frequenza di 1 minuto senza costi aggiuntivi.	Conteggio	• Somma • Media

Il AWS/EBS namespace include la seguente metrica di controllo dello stato.

Parametro	Descrizione	Unità	Statistiche significative
VolumeStalledIOCheck	Nota: solo per istanze Nitro. Non pubblicato per i volumi e le AWS Fargate attività allegati ad Amazon ECS. Riporta se un volume ha superato o meno un controllo I/O bloccato nell'ultimo minuto. Questo parametro può essere 0 (superato) o 1 (non riuscito).	Nessuno	• Somma • Media • Minimo • Massimo

Parametri di mirroring del traffico

Lo spazio dei nomi AWS/EC2 include i parametri per il traffico con mirroring. Per ulteriori informazioni, consulta Monitora il traffico in mirroring utilizzando Amazon CloudWatch nella Amazon VPC Traffic Mirroring Guide.

Parametri del gruppo con scalabilità automatica

Lo spazio dei nomi AWS/AutoScaling include i parametri per i gruppi Auto Scaling. Per ulteriori informazioni, consulta Monitora i CloudWatch parametri per i gruppi e le istanze di Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.

Dimensioni dei parametri Amazon EC2

È possibile utilizzare le seguenti dimensioni per perfezionare i parametri elencati nelle tabelle precedenti.

Dimensione	Descrizione
AutoScalingGroupName	Questa dimensione filtra i dati richiesti per tutte le istanze in un gruppo di capacità specificato. Un gruppo Auto Scaling è una raccolta di istanze che definisci se utilizzi Auto Scaling. La dimensione è disponibile solo per i parametri di Amazon

Dimensione	Descrizione
	EC2 quando le istanze si trovano in un gruppo Auto Scaling. Disponibile per le istanze con monitoraggio dettagliato o di base abilitato.
`ImageId`	Questa dimensione filtra i dati richiesti per tutte le istanze che eseguono questa Amazon Machine Image (AMI) di Amazon EC2. Disponibile per le istanze con monitoraggio dettagliato abilitato.
`InstanceId`	Questa dimensione filtra i dati richiesti solo per l'istanza identific ata. Ciò aiuta a definire un'istanza esatta dalla quale monitorare i dati.
`InstanceType`	Questa dimensione filtra i dati richiesti per tutte le istanze in esecuzione con questo tipo di istanza specificato. Ciò aiuta a categorizzare i dati in base al tipo di istanza in esecuzion e. Ad esempio, puoi confrontare i dati da un'istanza m1.small e un'istanza m1.large per determinare quale ha il valore commerciale migliore per la tua applicazione. Disponibile per le istanze con monitoraggio dettagliato abilitato.

Parametri di utilizzo Amazon EC2

Puoi utilizzare i parametri di CloudWatch utilizzo per fornire visibilità sull'utilizzo delle risorse da parte del tuo account. Utilizza queste metriche per visualizzare l'utilizzo corrente del servizio su CloudWatch grafici e dashboard.

I parametri di utilizzo di Amazon EC2 corrispondono alle AWS quote di servizio. È possibile configurare gli allarmi che avvisano quando l'uso si avvicina a una quota di servizio. Per ulteriori informazioni sull' CloudWatchintegrazione con le quote di servizio, consulta i parametri di AWS utilizzo nella Amazon CloudWatch User Guide.

Amazon EC2 pubblica i seguenti parametri nello spazio dei nomi `AWS/Usage`.

Parametro	Descrizione
`ResourceCount`	Il numero delle risorse specificate in esecuzione nell'account. Le risorse sono definite dalle dimensioni associate al parametro. La statistica più utile per questo parametro è `MAXIMUM`, che rappresenta il numero massimo di risorse utilizzate durante il periodo di 1 minuto.

Le seguenti dimensioni vengono utilizzate per perfezionare i parametri di utilizzo pubblicati da Amazon EC2.

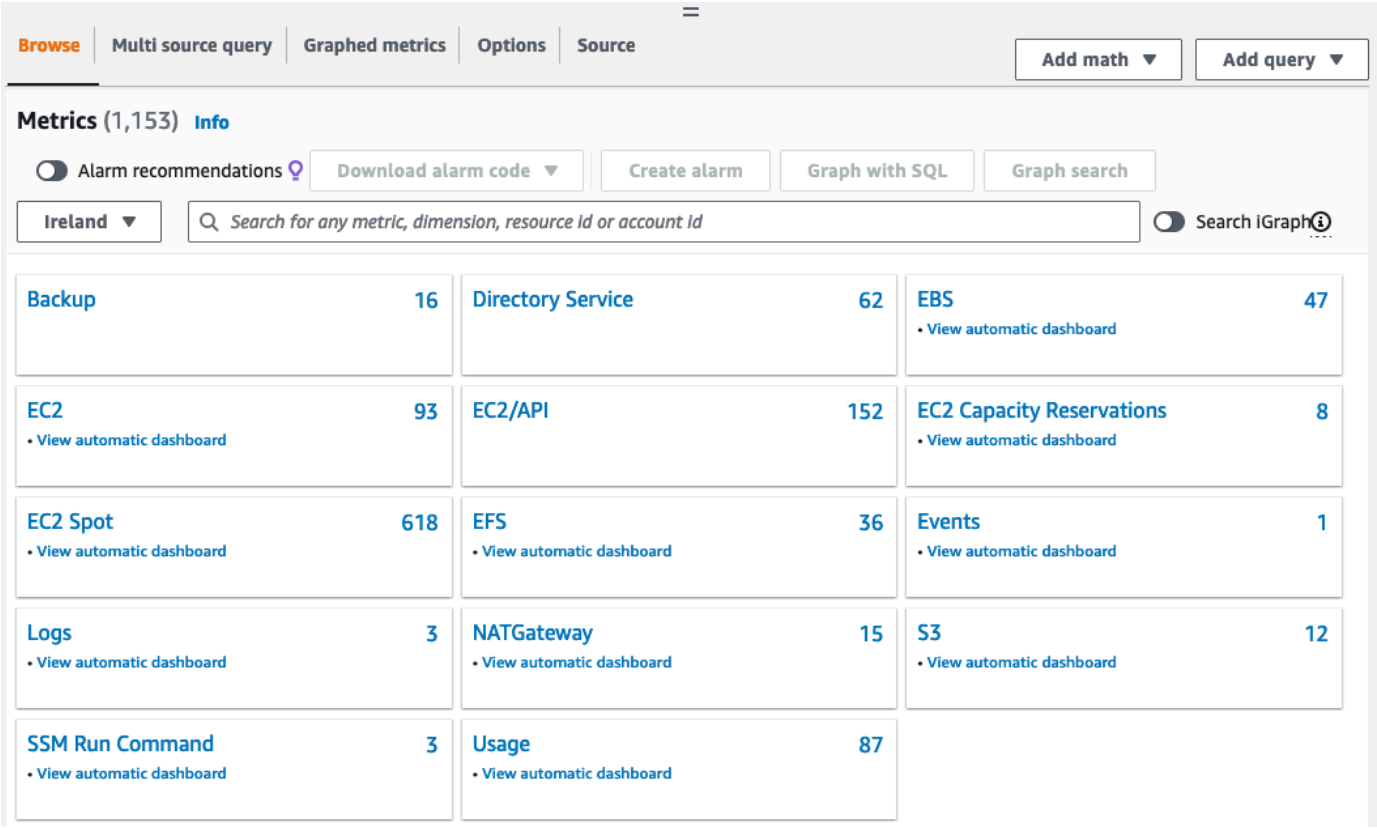
Dimensione	Descrizione
`Service`	Il nome del AWS servizio che contiene la risorsa. Per i parametri di utilizzo di Amazon EC2, il valore per questa dimensione è `EC2`.
`Type`	Il tipo di entità che viene segnalato. Attualmente, l'unico valore valido per i parametri di utilizzo Amazon EC2 è `Resource`.
`Resource`	Il tipo di risorsa in esecuzione. Attualmente, l'unico valore valido per i parametri di utilizzo di Amazon EC2 è `vCPU`, che restituisce informazioni sulle istanze in esecuzione.
`Class`	La classe della risorsa monitorata. Per i parametri di utilizzo di Amazon EC2 con `vCPU` come valore della dimensione `Resource`, i valori validi sono `Standard/OnDemand` , `F/OnDemand` , `G/OnDemand` , `Inf/OnDemand` , `P/OnDemand` e `X/OnDemand` . I valori per questa dimensione definiscono la prima lettera dei tipi di istanza segnalati dal parametro. Ad esempio, `Standard/OnDemand` restituisce informazioni su tutte le istanze in esecuzione con tipi che iniziano con A, C, D, H, I, M, R, T e Z e `G/OnDemand` restituisce informazioni su tutte le istanze in esecuzione con tipi che iniziano con G.

Elencare i parametri tramite la console

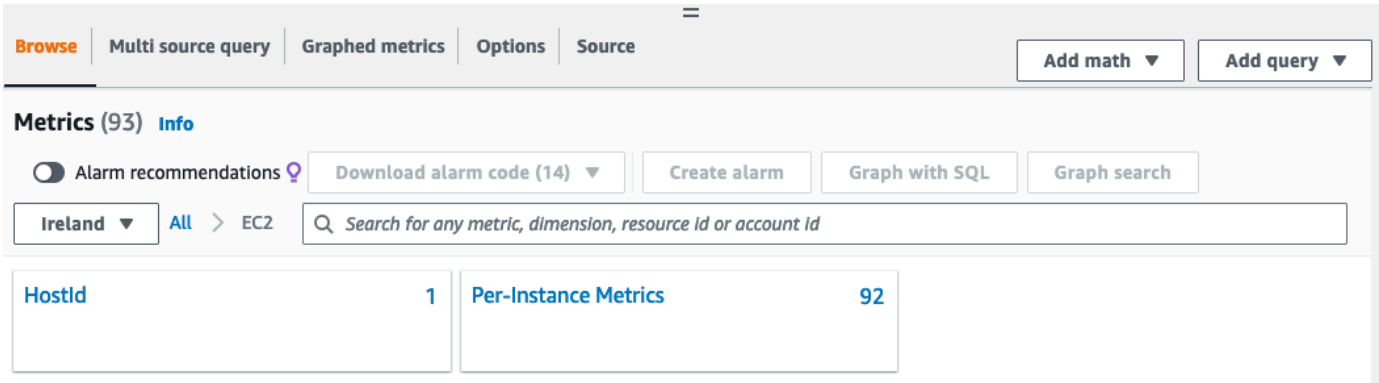
I parametri sono raggruppati in primo luogo in base allo spazio dei nomi e in secondo luogo in base alle diverse combinazioni di dimensioni all'interno di ciascuno spazio dei nomi. Ad esempio, puoi visualizzare tutti i parametri forniti da Amazon EC2 oppure i parametri raggruppati per ID istanza, tipo di istanza, ID immagine (AMI) o gruppo Auto Scaling.

Per visualizzare i parametri disponibili per categoria (console)

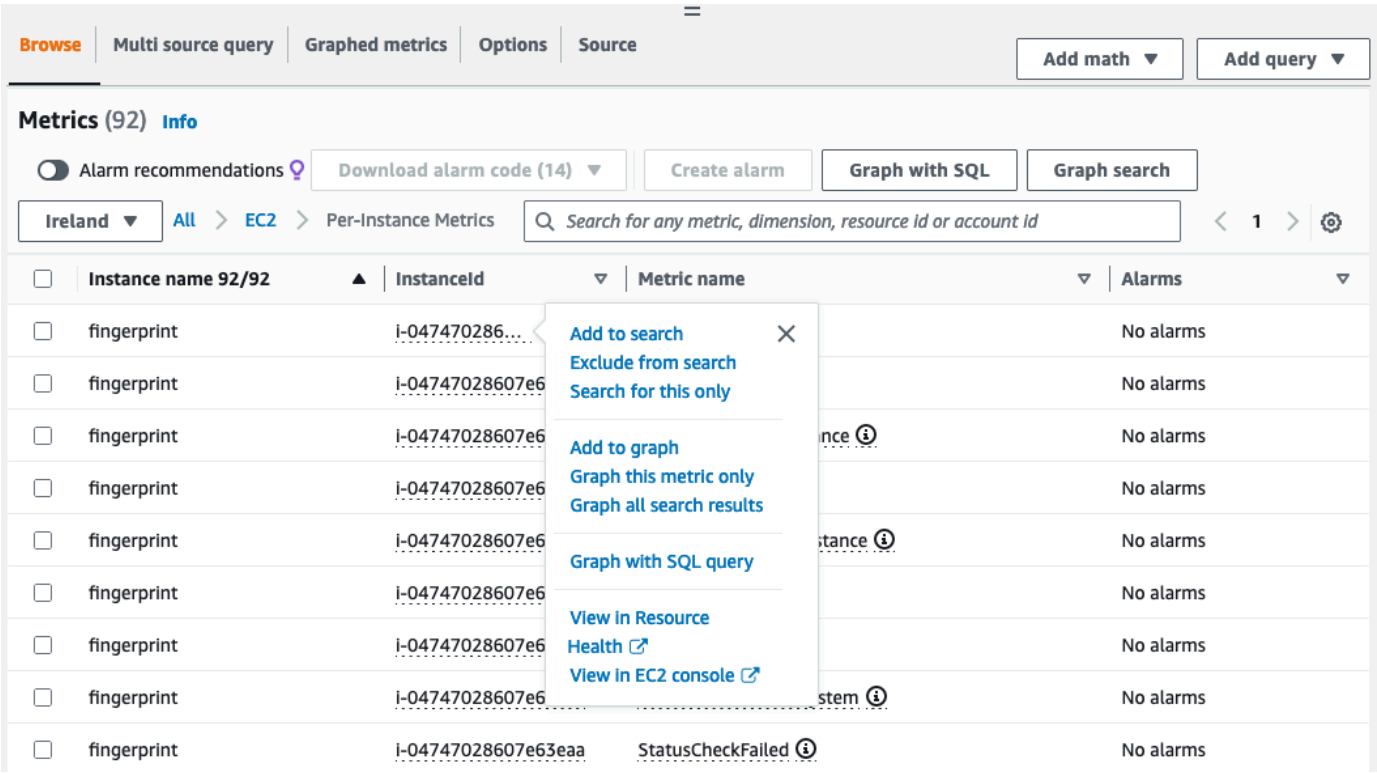
1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, espandi Metriche, quindi scegli Tutte le metriche.
3. Selezionare il parametro namespace EC2.



4. Selezionare una dimensione di parametro (ad esempio, Per-Instance Metrics (Parametri per istanza)).



5. Per ordinare i parametri, utilizza l'intestazione della colonna. Per creare il grafico di un parametro, seleziona la casella di controllo accanto al parametro. Per filtrare per risorsa, scegli l'ID della risorsa e quindi Add to search (Aggiungi alla ricerca). Per filtrare in base a un parametro, scegli il nome del parametro e quindi Add to search (Aggiungi alla ricerca).



Elenca le metriche utilizzando il AWS CLI

Usa il comando list-metrics per elencare le CloudWatch metriche per le tue istanze.

Come elencare tutti i parametri disponibili per Amazon EC2 (AWS CLI)

L'esempio seguente specifica lo spazio dei nomi `AWS/EC2` per visualizzare tutti i parametri per Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

Di seguito è riportato un output di esempio:

```
{
  "Metrics": [
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "NetworkOut"
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "CPUUtilization"
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "NetworkIn"
    },
    ...
  ]
}
```

Per elencare tutti i parametri disponibili per un'istanza (AWS CLI)

L'esempio seguente specifica lo spazio dei nomi `AWS/EC2` e la dimensione `InstanceId` per visualizzare i risultati solo per l'istanza specificata.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --dimensions
 Name=InstanceId,Value=i-1234567890abcdef0
```

Per elencare un parametro su tutte le istanze (AWS CLI)

L'esempio seguente specifica lo spazio dei nomi `AWS/EC2` e un nome parametro per visualizzare i risultati solo per il parametro specificato.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --metric-name CPUUtilization
```

Installa e configura l' CloudWatchagente utilizzando la console Amazon EC2 per aggiungere parametri aggiuntivi

> L'installazione e la configurazione dell' CloudWatch agente tramite la console Amazon EC2 sono in versione beta per Amazon EC2 e sono soggette a modifiche.

Per impostazione predefinita, Amazon CloudWatch fornisce parametri di base, come `CPUUtilization` e`NetworkIn`, per il monitoraggio delle istanze Amazon EC2. Per raccogliere parametri aggiuntivi, puoi installare l' CloudWatch agente sulle tue istanze EC2 e quindi configurare l'agente in modo che emetta parametri selezionati. Invece di installare e configurare manualmente l' CloudWatch agente su ogni istanza EC2, puoi utilizzare la console Amazon EC2 per farlo al posto tuo.

Questo argomento spiega come utilizzare la console Amazon EC2 per installare l' CloudWatch agente sulle istanze e configurare l'agente per l'emissione di parametri selezionati.

Per i passaggi manuali di questo processo, consulta Installazione dell' CloudWatch agente utilizzando AWS Systems Manager nella Amazon CloudWatch User Guide. Per ulteriori informazioni sull' CloudWatch agente, consulta Raccogli metriche, log e tracce con l' CloudWatch agente.

Argomenti

- Prerequisiti

- Come funziona
- Costi
- Installa e configura l'agente CloudWatch

Prerequisiti

Per utilizzare Amazon EC2 per installare e configurare l' CloudWatch agente, devi soddisfare i prerequisiti utente e istanza descritti in questa sezione.

Prerequisiti per gli utenti

Per utilizzare questa funzionalità, l'utente o il ruolo della console IAM deve disporre delle autorizzazioni necessarie per l'utilizzo di Amazon EC2 e delle seguenti autorizzazioni IAM:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:ListCommandInvocations",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetInstanceProfile",
                "iam:SimulatePrincipalPolicy"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Prerequisiti dell'istanza

- Stato dell'istanza: `running`
- Sistema operativo supportato: Linux
- AWS Systems Manager Agente (agente SSM): installato. Due note sull'agente SSM:
  - SSM Agent è preinstallato su alcune Amazon Machine Images (AMI) fornite da terze parti AWS affidabili. Per informazioni sulle AMI supportate e le istruzioni per l'installazione dell'agente SSM, consulta Amazon Machine Images (AMI) con agente SSM preinstallato nella Guida per l'utente.AWS Systems Manager
  - Se riscontri problemi con l'agente SSM, consulta la sezione Risoluzione dei problemi dell'agente SSM nella Guida per l'utente.AWS Systems Manager
- Autorizzazioni IAM per l'istanza: le seguenti politiche AWS gestite devono essere aggiunte a un ruolo IAM collegato all'istanza:
  - AmazonSSM ManagedInstanceCore: consente a un'istanza di utilizzare Systems Manager per installare e configurare l'agente. CloudWatch
  - CloudWatchAgentServerPolicy— Consente a un'istanza di utilizzare l' CloudWatchagente su cui scrivere dati. CloudWatch

  Per informazioni su come aggiungere le autorizzazioni IAM alla tua istanza, consulta Using instance profiles nella IAM User Guide.

Come funziona

Prima di poter utilizzare la console Amazon EC2 per installare e configurare l' CloudWatch agente, devi assicurarti che il tuo utente o ruolo IAM e le istanze su cui desideri aggiungere parametri soddisfino determinati prerequisiti. Quindi, puoi utilizzare la console Amazon EC2 per installare e configurare l' CloudWatch agente sulle istanze selezionate.

Per prima cosa, soddisfa i prerequisiti

- Sono necessarie le autorizzazioni IAM richieste: prima di iniziare, assicurati che l'utente o il ruolo della console disponga delle autorizzazioni IAM necessarie per utilizzare questa funzionalità.

- Istanze: per utilizzare la funzionalità, le istanze EC2 devono essere istanze Linux, avere l'agente SSM installato, disporre delle autorizzazioni IAM richieste ed essere in esecuzione.

Quindi puoi utilizzare la funzionalità

1. Seleziona le tue istanze: nella console Amazon EC2, selezioni le istanze su cui installare e configurare l'agente. CloudWatch Quindi avvia il processo scegliendo Configura agente. CloudWatch
2. Convalida dell'agente SSM: Amazon EC2 verifica che l'agente SSM sia installato e avviato su ogni istanza. Tutte le istanze che non superano questo controllo vengono escluse dal processo. L'agente SSM viene utilizzato per eseguire azioni sull'istanza durante questo processo.
3. Convalida delle autorizzazioni IAM: Amazon EC2 verifica che ogni istanza disponga delle autorizzazioni IAM necessarie per questo processo. Tutte le istanze che non superano questo controllo vengono escluse dal processo. Le autorizzazioni IAM consentono all' CloudWatch agente di raccogliere metriche dall'istanza e di AWS Systems Manager integrarsi con l'agente SSM.
4. CloudWatch Agente di convalida: Amazon EC2 verifica che CloudWatch l'agente sia installato e in esecuzione su ogni istanza. Se qualche istanza non supera questo controllo, Amazon EC2 si offre di installare e avviare CloudWatch l'agente per te. L' CloudWatch agente raccoglierà i parametri selezionati su ogni istanza una volta completato questo processo.
5. Seleziona la configurazione delle metriche: selezioni le metriche che l' CloudWatch agente deve emettere dalle tue istanze. Una volta selezionato, Amazon EC2 archivia un file di configurazione in Parameter Store, dove rimane fino al completamento del processo. Amazon EC2 eliminerà il file di configurazione da Parameter Store a meno che il processo non venga interrotto. Tieni presente che se non selezioni una metrica, ma l'hai aggiunta in precedenza all'istanza, questa verrà rimossa dall'istanza al termine del processo.
6. Aggiorna la configurazione CloudWatch dell'agente: Amazon EC2 invia la configurazione dei parametri all'agente. CloudWatch Questa è l'ultima fase del processo. In caso di successo, le istanze possono emettere dati per i parametri selezionati e Amazon EC2 elimina il file di configurazione da Parameter Store.

Costi

Le metriche aggiuntive che aggiungi durante questo processo vengono fatturate come metriche personalizzate. Per ulteriori informazioni sui prezzi delle CloudWatch metriche, consulta la pagina dei CloudWatch prezzi di Amazon.

Installa e configura l'agente CloudWatch

Puoi utilizzare la console Amazon EC2 per installare e configurare l' CloudWatch agente per aggiungere parametri aggiuntivi.

> **Note**
>
> Ogni volta che esegui questa procedura, sovrascrivi la configurazione dell'agente esistente CloudWatch . Se non si seleziona una metrica selezionata in precedenza, questa verrà rimossa dall'istanza.

Per installare e configurare l' CloudWatch agente utilizzando la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona le istanze su cui installare e configurare l' CloudWatch agente.
4. Scegli Azioni, Monitoraggio e risoluzione dei problemi, Configura agente. CloudWatch

   > **Tip**
   >
   > Questa funzionalità non è disponibile in tutte. Regioni AWS Se CloudWatchl'agente Configure non è disponibile, prova un'altra regione.

5. Per ogni fase del processo, leggi il testo della console, quindi scegli Avanti.
6. Per completare il processo, nella fase finale, scegli Completa.

Ottenere le statistiche sui parametri delle istanze

Puoi ottenere statistiche per le CloudWatch metriche relative alle tue istanze.

Indice

- Aggregazione di statistiche per AMI

Panoramica sulle statistiche

Le statistiche sono aggregazioni di dati metrici su periodi di tempo specifici. CloudWatch fornisce statistiche basate sui punti dati metrici forniti dai dati personalizzati o forniti da altri servizi di. AWS CloudWatch Le aggregazioni vengono effettuate usando lo spazio dei nomi, il nome parametro, le dimensioni e l'unità di misura del punto dati, entro un periodo di tempo specificato. Nella seguente tabella vengono descritte le statistiche disponibili.

Statistica	Descrizione
`Minimum`	Il valore più basso osservato durante il periodo specificato. Puoi utilizzare questo valore per determinare volumi di attività bassi per l'applicazione.
`Maximum`	Il valore più alto osservato durante il periodo specificato. Puoi utilizzare questo valore per determinare volumi di attività alti per l'applicazione.
`Sum`	Tutti i valori inviati per i parametri abbinati uniti insieme. Questa statistica può essere utile per determinare il volume totale di un parametro.
`Average`	Il valore `Sum`/`SampleCount` durante il periodo specificato. Confrontando questa statistica con `Minimum` e `Maximum`, puoi determinare l'ambito completo di un parametro e come l'uso della media sia vicino a `Minimum` e `Maximum`. Questo confronto consente di sapere quando aumentare o diminuire le risorsa in base alle esigenze.
`SampleCount`	Il conteggio (numero) dei punti dati utilizzato per il calcolo statistico.
`pNN.NN`	Il valore di uno specifico percentile. Puoi specificare qualsiasi percentile, utilizzando fino a due decimali (ad esempio, p95,45).

Ottenere le statistiche su un'istanza specifica

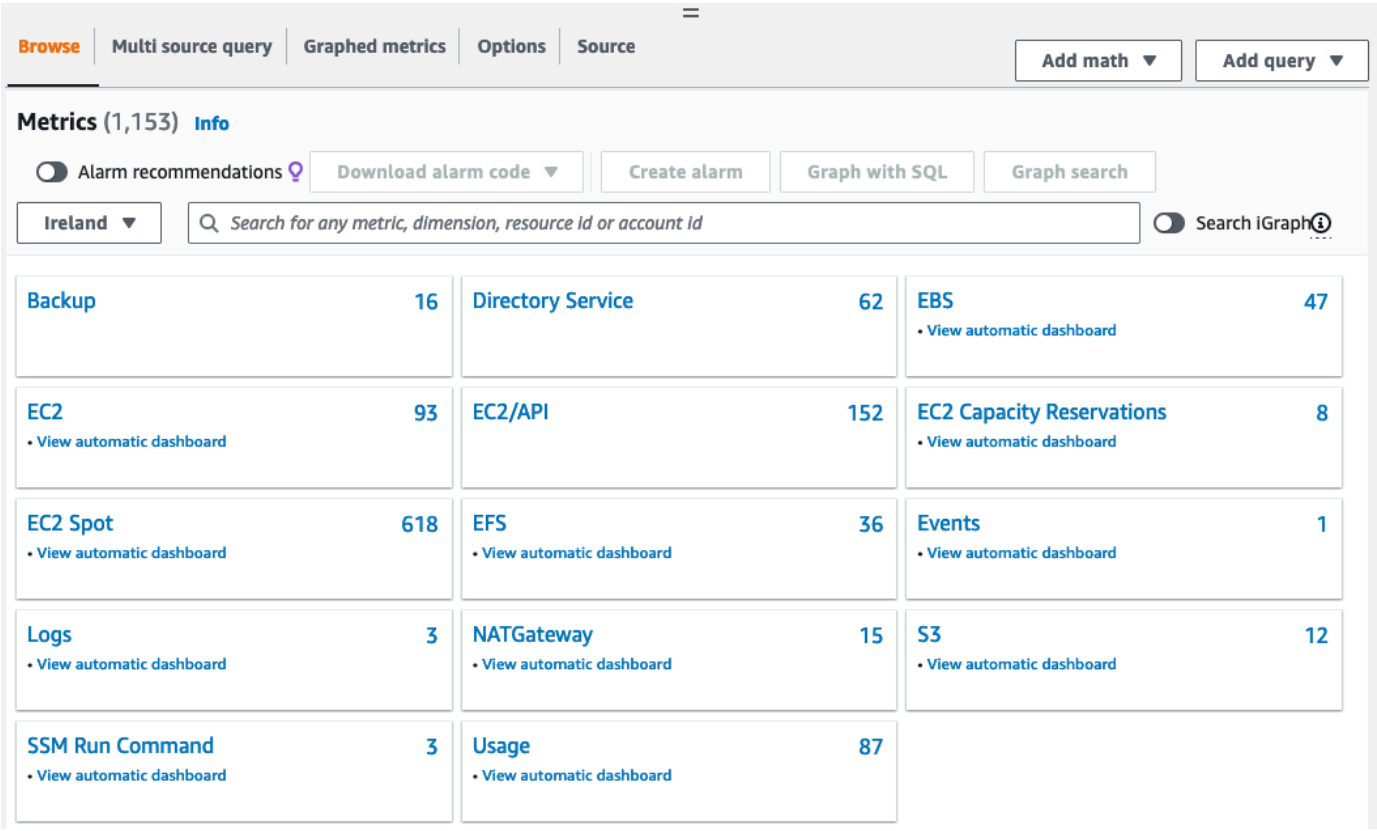
Gli esempi seguenti mostrano come utilizzare AWS Management Console o the per AWS CLI determinare l'utilizzo massimo della CPU di una specifica istanza EC2.

Requisiti

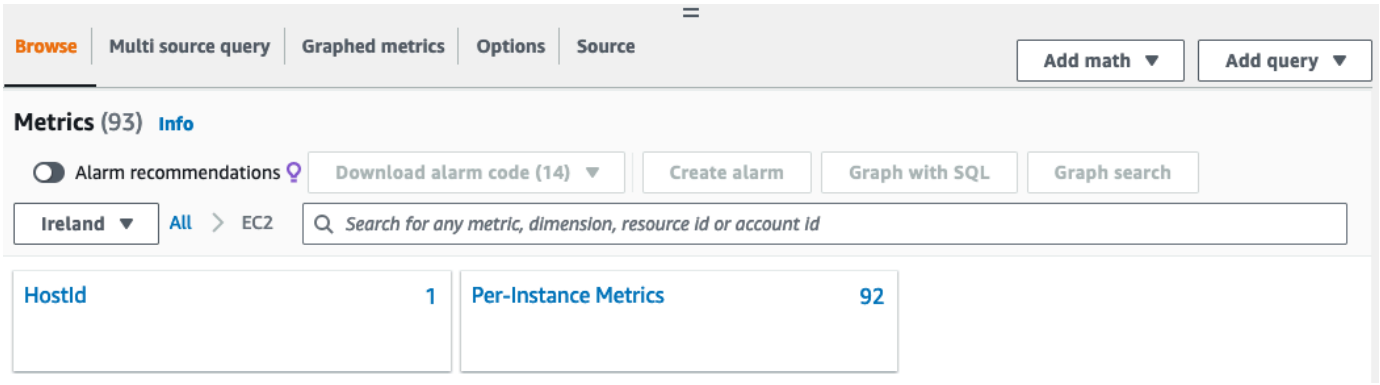
- Devi disporre dell'ID dell'istanza. Puoi ottenere l'ID dell'istanza tramite la AWS Management Console o il comando describe-instances.
- Per impostazione predefinita, il monitoraggio base è abilitato, ma puoi tuttavia abilitare il monitoraggio dettagliato. Per ulteriori informazioni, consulta Abilitazione o disabilitazione del monitoraggio dettagliato per le istanze.

Per visualizzare l'utilizzo della CPU di un'istanza specifica (console)

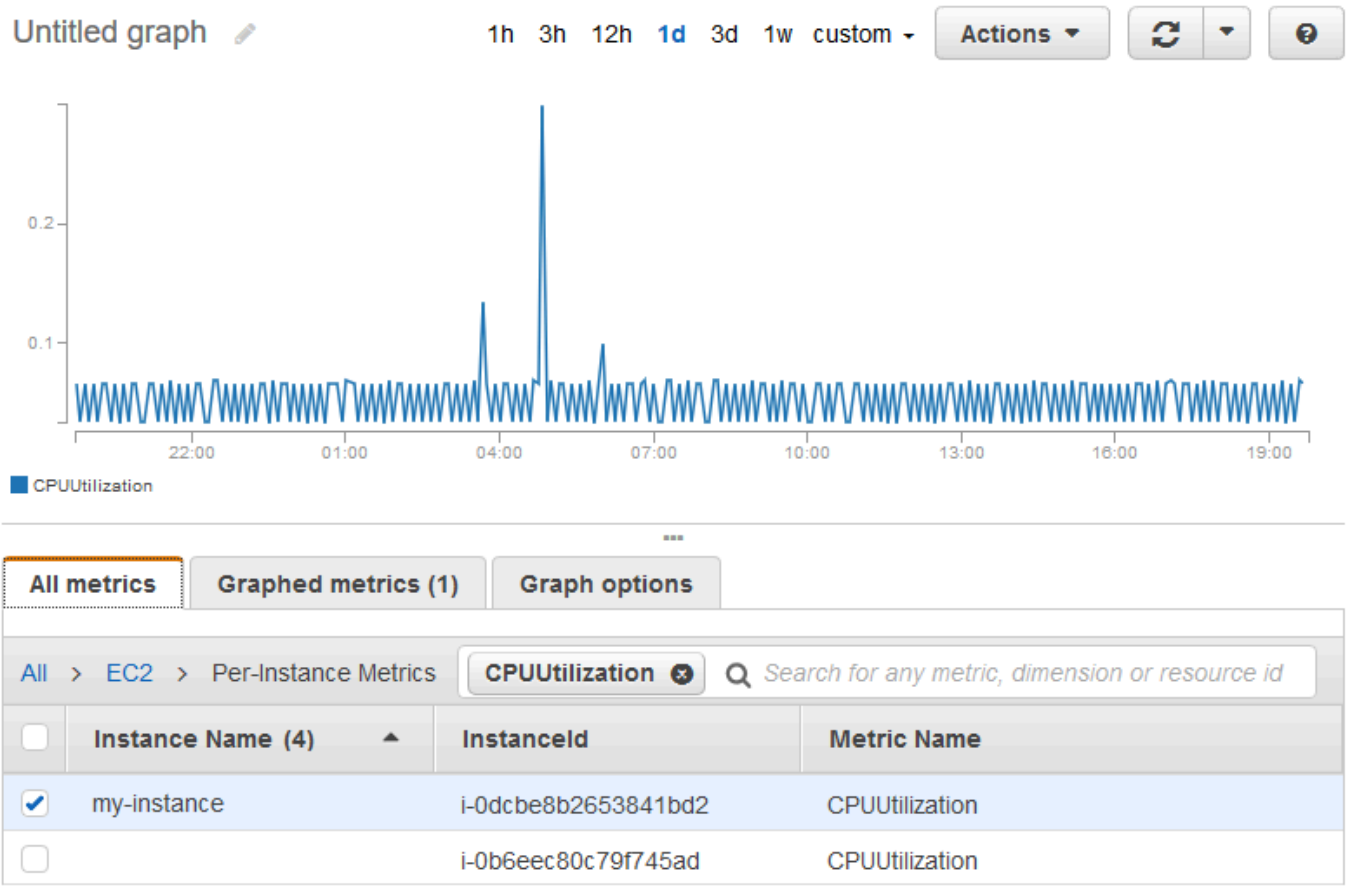
1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare il parametro namespace EC2.



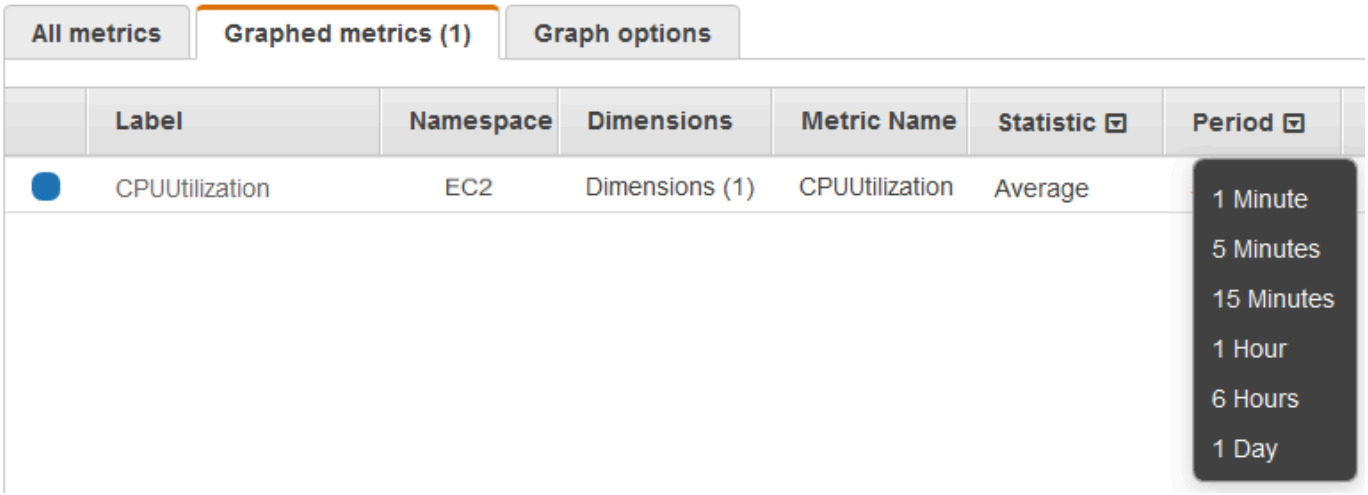
4. Selezionare la dimensione Per-Instance Metrics (Parametri per istanza).



5. Nel campo di ricerca digitare **`CPUUtilization`** e premere Invio. Selezionare la riga dell'istanza specifica, che mostra un grafico del parametro CPUUtilization dell'istanza. Per assegnare un nome al grafico, scegliere l'icona a forma di matita. Per modificare l'intervallo di tempo, selezionare uno dei valori predefiniti o scegliere custom (personalizzato).



6. Per modificare le statistiche o il periodo del parametro, scegliere la scheda Graphed metrics (Parametri nel grafico). Scegliere l'intestazione di colonna o un valore singolo, quindi scegliere un valore diverso.



Per ottenere l'utilizzo della CPU di un'istanza specifica (AWS CLI)

Utilizzate il get-metric-statisticscomando seguente per ottenere la metrica di utilizzo della CPU per l'istanza specificata, utilizzando il periodo e l'intervallo di tempo specificati:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

Di seguito è riportato un output di esempio. Ogni valore rappresenta la percentuale di utilizzo massimo della CPU di una singola istanza EC2.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
```

```
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Aggregazione di statistiche tra istanze

Le statistiche aggregate sono disponibili per le istanze per le quali è stato abilitato il monitoraggio dettagliato. Le istanze che utilizzano il monitoraggio base non sono incluse nelle aggregazioni. Prima di poter ottenere le statistiche aggregate per le istanze, devi abilitare il monitoraggio dettagliato (a un costo aggiuntivo), che fornisce i dati in periodi di 1 minuto.

Tieni presente che Amazon CloudWatch non può aggregare dati tra AWS regioni. I parametri sono completamente indipendenti tra le regioni.

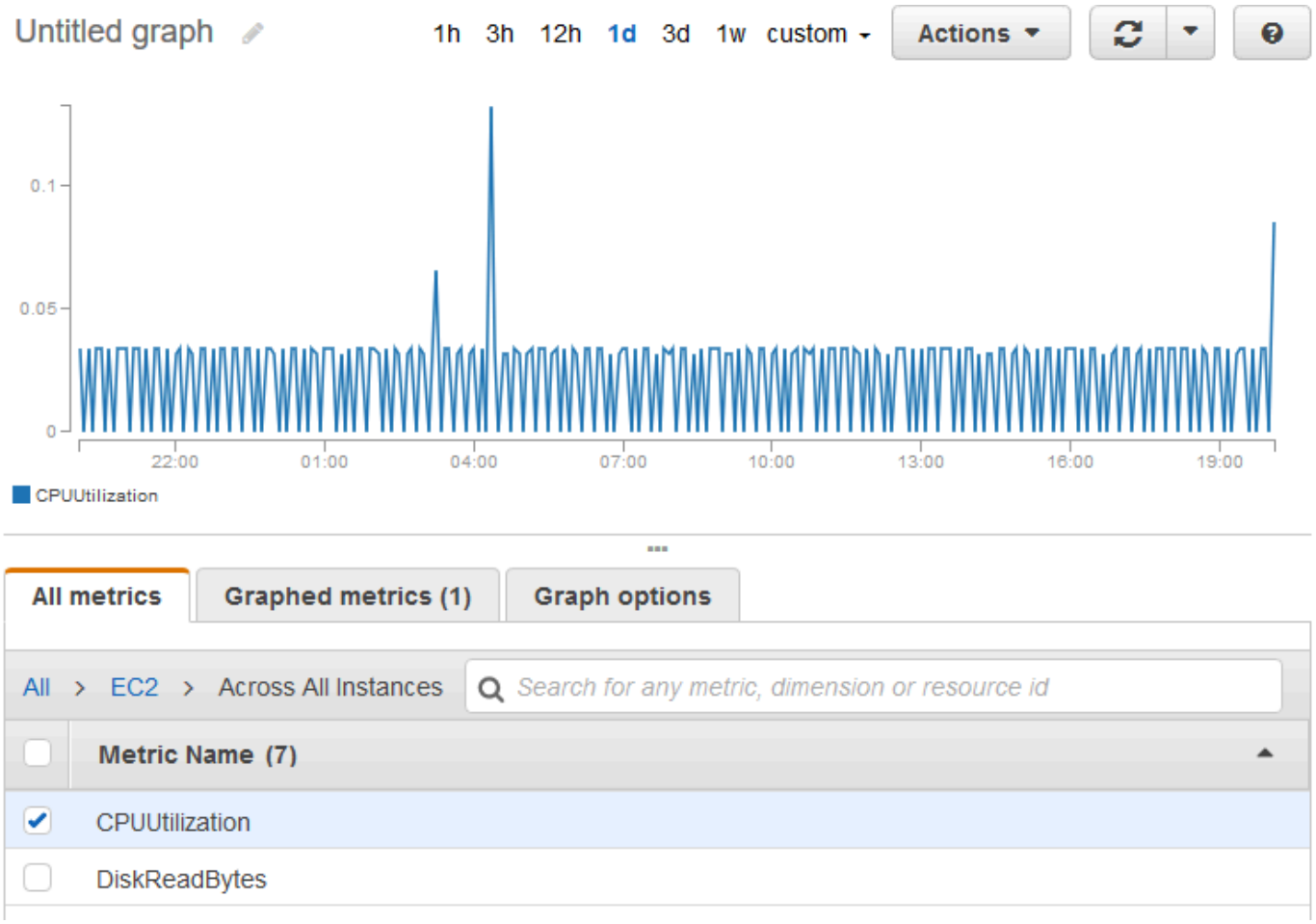
Questo esempio illustra come utilizzare il monitoraggio dettagliato per ottenere l'utilizzo medio della CPU delle istanze EC2. Poiché non è specificata alcuna dimensione, CloudWatch restituisce le statistiche per tutte le dimensioni nel `AWS/EC2` namespace.

> **Important**
>
> Questa tecnica per recuperare tutte le dimensioni in un AWS namespace non funziona per i namespace personalizzati pubblicati su Amazon. CloudWatch Con gli spazi dei nomi personalizzati, è necessario specificare il set completo delle dimensioni associate a un determinato punto dati per recuperare le statistiche comprendenti il punto dati.

Per visualizzare l'utilizzo medio della CPU nelle istanze (console)

1. Apri CloudWatch la console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare lo spazio dei nomi EC2, quindi selezionare Across All Instances (Per tutte le istanze).

4. Selezionare la riga contenente CPUUtilization, che mostra un grafico del parametro per tutte le istanze EC2. Per assegnare un nome al grafico, scegliere l'icona a forma di matita. Per modificare l'intervallo di tempo, selezionare uno dei valori predefiniti o scegliere custom (personalizzato).



5. Per modificare le statistiche o il periodo del parametro, scegliere la scheda Graphed metrics (Parametri nel grafico). Scegliere l'intestazione di colonna o un valore singolo, quindi scegliere un valore diverso.

Per ottenere l'utilizzo medio della CPU tra le istanze (AWS CLI)

Utilizza il get-metric-statisticscomando seguente per ottenere la media della metrica di utilizzo della CPU tra le tue istanze.

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
    --period 3600  --statistics "Average" "SampleCount" \
```

```
    --start-time 2022-10-11T23:18:00 \
    --end-time 2022-10-12T23:18:00
```

Di seguito è riportato un output di esempio:

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Aggregazione di statistiche per gruppo Auto Scaling

Puoi aggregare le statistiche per le istanze EC2 in un gruppo di Auto Scaling. Tieni presente che Amazon CloudWatch non può aggregare dati tra AWS regioni. I parametri sono completamente indipendenti tra le regioni.

Questo esempio illustra come recuperare il numero totale di byte scritti sul disco per un gruppo di Auto Scaling. Il totale viene calcolato per periodi di 1 minuto per un intervallo di 24 ore all'interno di tutte le istanze EC2 nel gruppo Auto Scaling specificato.

Da visualizzare DiskWriteBytes per le istanze in un gruppo Auto Scaling (console)

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Seleziona lo spazio dei nomi EC2, quindi seleziona By Auto Scaling Group (Per gruppo Auto Scaling).
4. Scegliete la riga per la DiskWriteBytesmetrica e il gruppo Auto Scaling specifico, che visualizza un grafico per la metrica per le istanze nel gruppo Auto Scaling. Per assegnare un nome al grafico, scegliere l'icona a forma di matita. Per modificare l'intervallo di tempo, selezionare uno dei valori predefiniti o scegliere custom (personalizzato).
5. Per modificare le statistiche o il periodo del parametro, scegliere la scheda Graphed metrics (Parametri nel grafico). Scegliere l'intestazione di colonna o un valore singolo, quindi scegliere un valore diverso.

Da visualizzare DiskWriteBytes per le istanze in un gruppo Auto Scaling ()AWS CLI

Utilizza il comando get-metric-statistics come riportato di seguito.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
 --period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

Di seguito è riportato un output di esempio:

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
```

```
    ],
    "Label": "DiskWriteBytes"
}
```

Aggregazione di statistiche per AMI

Puoi aggregare le statistiche sulle istanze per le quali è stato abilitato il monitoraggio dettagliato. Le istanze che utilizzano il monitoraggio base non sono incluse nelle aggregazioni. Prima di poter ottenere le statistiche aggregate per le istanze, devi abilitare il monitoraggio dettagliato (a un costo aggiuntivo), che fornisce i dati in periodi di 1 minuto.

Tieni presente che Amazon CloudWatch non può aggregare dati tra AWS regioni. I parametri sono completamente indipendenti tra le regioni.

Questo esempio illustra come determinare l'utilizzo medio della CPU per tutte le istanze che utilizzano un'Amazon Machine Image (AMI) specifica. La media supera intervalli di tempo di 60 secondi per un periodo di un giorno.

Per visualizzare l'utilizzo medio della CPU per AMI (console)

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare lo spazio dei nomi EC2, quindi selezionare By Image (AMI) Id (Per ID immagine (AMI)).
4. Selezionare la riga del parametro CPUUtilization e l'AMI specifica, che mostra un grafico del parametro per l'AMI specificata. Per assegnare un nome al grafico, scegliere l'icona a forma di matita. Per modificare l'intervallo di tempo, selezionare uno dei valori predefiniti o scegliere custom (personalizzato).
5. Per modificare le statistiche o il periodo del parametro, scegliere la scheda Graphed metrics (Parametri nel grafico). Scegliere l'intestazione di colonna o un valore singolo, quindi scegliere un valore diverso.

Per ottenere l'utilizzo medio della CPU per un'ID immagine (AWS CLI)

Utilizza il comando get-metric-statistics come riportato di seguito.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
```

```
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

Di seguito è riportato un output di esempio. Ogni valore rappresenta una percentuale di utilizzo medio della CPU per le istanze EC2 che eseguono l'AMI specificata.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-10T07:00:00Z",
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Rappresentazione grafica dei parametri delle istanze

Dopo aver avviato un'istanza, puoi aprire la console Amazon EC2 e visualizzare i relativi grafici di monitoraggio per l'istanza nella scheda Monitoring (Monitoraggio). Ciascun grafico si basa su uno dei parametri di Amazon EC2 disponibili.

Sono disponibili i seguenti grafici:

- Utilizzo medio della CPU (percentuale)
- Letture medie del disco (byte)
- Scritture medie sul disco (byte)
- Rete massima in entrata (byte)
- Rete massima in uscita (byte)

- Operazioni di lettura del disco di riepilogo (numero)
- Operazioni di scrittura sul disco di riepilogo (numero)
- Stato riepilogo (qualsiasi)
- Istanza dello stato di riepilogo (numero)
- Sistema dello stato di riepilogo (numero)

Per ulteriori informazioni sui parametri e i relativi dati visualizzati nei grafici, consulta Elenca le CloudWatch metriche disponibili per le tue istanze.

Rappresenta graficamente le metriche utilizzando la console CloudWatch

Puoi anche utilizzare la CloudWatch console per rappresentare graficamente i dati metrici generati da Amazon EC2 e AWS altri servizi. Per ulteriori informazioni, consulta la sezione Grafica delle metriche nella Amazon CloudWatch User Guide.

Crea un CloudWatch allarme per un'istanza

Puoi creare un CloudWatch allarme che monitora le CloudWatch metriche per una delle tue istanze. CloudWatchti invierà automaticamente una notifica quando la metrica raggiunge una soglia specificata. Puoi creare un CloudWatch allarme utilizzando la console Amazon EC2 o utilizzando le opzioni più avanzate fornite dalla CloudWatch console.

Per creare un allarme utilizzando la console CloudWatch

Per esempi, consulta Creating Amazon CloudWatch Alarms nella Amazon CloudWatch User Guide.

Per creare un allarme tramite la console Amazon EC2

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Azioni, Monitoraggio e risoluzione dei problemi, Gestione degli allarmi. CloudWatch
4. Nella pagina dei dettagli di Gestione CloudWatch degli allarmi, in Aggiungi o modifica allarme, seleziona Crea un avviso.
5. Per Notifica di allarme, scegli se configurare le notifiche Amazon Simple Notification Service (Amazon SNS). Immettere un argomento Amazon SNS esistente o immettere un nome per creare un nuovo argomento.

6. Per Operazione per gli allarmi, scegli se specificare un'operazione da effettuare quando viene attivato l'allarme. Scegli un'operazione dall'elenco.
7. Per Alarm thresholds (Soglie di allarme=, selezionare il parametro e i criteri per l'allarme. Ad esempio, per creare un allarme che viene attivato quando l'utilizzo della CPU raggiunge l'80% per un periodo di 5 minuti, procedi come segue:
   a. Mantieni l'impostazione predefinita per Raggruppa esempi per (Media) e Tipo di dati da campionare (Utilizzo CPU).
   b. Scegli >= per Allarme quando, quindi immetti **`0.80`** per Percentuale.
   c. Inserisci **`1`** per Periodo consecutivo e seleziona 5 minuti per Periodo.
8. (Facoltativo) Per Sample metric data (Dati dei parametri di esempio), scegliere Add to dashboard (Aggiungi al pannello di controllo).
9. Scegliere Create (Crea).

Puoi modificare le impostazioni CloudWatch degli allarmi dalla console Amazon EC2 o dalla CloudWatch console. Se desideri eliminare la sveglia, puoi farlo dalla CloudWatch console. Per ulteriori informazioni, consulta Modificare o eliminare un CloudWatch allarme nella Amazon CloudWatch User Guide.

Creazione di allarmi che arrestano, terminano, riavviano o recuperano un'istanza

Utilizzando Amazon CloudWatch Alarm Actions, puoi creare allarmi che interrompono, terminano, riavviano o ripristinano automaticamente le tue istanze. Puoi utilizzare le operazioni di arresto o termine per aiutarti a risparmiare denaro quando non necessiti più dell'esecuzione di un'istanza. Puoi utilizzare le operazioni di riavvio e recupero per riavviare automaticamente tali istanze o recuperarle in un nuovo hardware, se si verifica un danneggiamento del sistema.

> **Note**
>
> Per informazioni sulla fatturazione e sui prezzi di Amazon CloudWatch Alarms, consulta CloudWatch fatturazione e costi nella Amazon CloudWatch User Guide.

Il ruolo `AWSServiceRoleForCloudWatchEvents` collegato al servizio consente di eseguire azioni di allarme AWS per tuo conto. La prima volta che crei un allarme nell' AWS Management

Console API IAM o nell' AWS CLI API IAM, il ruolo collegato al servizio CloudWatch viene creato automaticamente.

Esistono diversi scenari in cui potresti voler arrestare o terminare automaticamente l'istanza. Ad esempio, potresti disporre di istanze dedicate a processi di elaborazione della retribuzione in batch o ad attività di calcolo scientifico che vengono eseguite per un periodo di tempo, dopodiché completano il proprio lavoro. Anziché lasciare tali istanze inattive (accumulando addebiti), puoi arrestarle o terminarle, ciò ti consente di risparmiare denaro. La differenza principale tra l'uso delle operazioni di allarme di arresto o di termine consiste nel poter avviare comodamente un'istanza arrestata se è necessario eseguirla in un secondo momento, mantenendo gli stessi ID istanza e volume radice. Tuttavia, non puoi avviare un'istanza terminata. Al contrario, è necessario avviare una nuova istanza. Quando un'istanza viene arrestata o terminata, i dati nei volumi dell'archivio dell'istanza vengono persi.

Puoi aggiungere le azioni di arresto, terminazione, riavvio o ripristino a qualsiasi allarme impostato su un parametro Amazon EC2 per istanza, inclusi i parametri di monitoraggio di base e dettagliati forniti da CloudWatch Amazon (nello spazio dei nomi), nonché qualsiasi parametro personalizzato che includa `AWS/EC2` la dimensione, purché `InstanceId` il relativo valore si riferisca a un'istanza Amazon EC2 valida in esecuzione.

> **Important**
>
> Gli allarmi di controllo dello stato possono entrare temporaneamente `INSUFFICIENT_DATA` nello stato se mancano punti dati metrici. Sebbene raro, ciò può accadere in caso di interruzione dei sistemi di reporting metrico, anche quando un'istanza è integra. Ti consigliamo di considerare lo `INSUFFICIENT_DATA` stato come dati mancanti anziché come una violazione dell'allarme, specialmente quando configuri l'allarme per arrestare, terminare, riavviare o ripristinare un'istanza.

Supporto della console

Puoi creare allarmi utilizzando la console Amazon EC2 o CloudWatch la console. Le procedure in questa documentazione utilizzano la console Amazon EC2. Per le procedure che utilizzano la CloudWatch console, consulta Creare allarmi per arrestare, terminare, riavviare o ripristinare un'istanza nella Amazon CloudWatch User Guide.

Autorizzazioni

È necessario che tu disponga del `iam:CreateServiceLinkedRole` per creare o modificare un allarme che esegue le operazioni di allarme EC2. Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

Indice

Aggiungi azioni di interruzione agli CloudWatch allarmi Amazon

Puoi creare un allarme per arrestare un'istanza Amazon EC2 al raggiungimento di una determinata soglia. Ad esempio, potresti eseguire istanze di sviluppo o di test e occasionalmente dimenticare di disattivarle. Puoi creare un allarme che viene attivato quando la percentuale di utilizzo medio della CPU è inferiore al 10% per 24 ore, segnalando che la CPU è inattiva e non più in uso. Puoi regolare la soglia, la durata e il periodo di tempo in base alle tue esigenze. Puoi inoltre aggiungere una notifica Amazon Simple Notification Service (Amazon SNS) in modo da ricevere un'e-mail all'attivazione dell'allarme.

Le istanze che utilizzano un volume Amazon EBS come dispositivo root possono essere arrestate o terminate, mentre le istanze che utilizzano l'instance store come dispositivo root possono solo essere terminate. Quando l'istanza viene terminata o arrestata, i dati nei volumi dell'archivio dell'istanza vengono persi.

Per creare un allarme per arrestare un'istanza inattiva (console Amazon EC2)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Azioni, Monitora e risolvi i problemi, Gestisci gli allarmi. CloudWatch

In alternativa, è possibile scegliere il segno più (

) nella colonna Alarm status (Stato allarme).

4. Nella pagina Gestisci gli CloudWatch allarmi, procedi come segue:

   a. Scegliere Create an alarm (Crea un allarme).

   b. Per ricevere un'e-mail quando viene attivato l'allarme, per Alarm notification (Notifica allarme), scegli un argomento Amazon SNS esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) nella Amazon Simple Notification Service Developer Guide.

   c. Attivare Alarm action (Azione Allarme)e scegliere Stop (Interrompi).

   d. Per Group samples by (Raggruppa campioni per) e Type of data to sample (Tipo di dati da campionare), scegliere una statistica e un parametro. In questo esempio, scegliere Average (Media) e CPU Utilization (Utilizzo CPU).

   e. Per Alarm When (Avvia allarme quando) e Percent (Percentuale), specificare la soglia del parametro. In questo esempio, specifica <= e 10%.

   f. Per Consecutive period (Periodo consecutivo) e Period (Periodo), specificare il periodo di valutazione per l'allarme. In questo esempio, specificare 1 periodo consecutivo di 5 minuti.

   g. Amazon crea CloudWatch automaticamente un nome di allarme per te. Per modificare il nome, immettere un nuovo nome in Alarm name (Nome allarme). I nomi degli allarmi devono contenere solo caratteri ASCII.

      > **Note**
      >
      > Puoi modificare la configurazione dell'allarme in base ai tuoi requisiti prima di creare l'allarme oppure puoi modificarlo in seguito. Questo include il parametro, la soglia, la durata, l'operazione e le impostazioni delle notifiche. Tuttavia, dopo aver creato l'allarme non è possibile modificarne il nome.

   h. Scegliere Create (Crea).

Aggiungi azioni di interruzione agli allarmi Amazon CloudWatch

Puoi creare un allarme per terminare automaticamente un'istanza EC2 al raggiungimento di una determinata soglia, purché non sia abilitata la protezione da cessazione dell'istanza. Ad esempio, potresti voler terminare un'istanza una volta che ha completato il suo lavoro e non averne più bisogno. Se intendessi utilizzare l'istanza in un secondo momento, sarebbe necessario arrestare l'istanza anziché terminarla. Quando un'istanza viene terminata, i dati nei volumi dell'archivio dell'istanza vengono persi. Per ulteriori informazioni sull'abilitazione e la disabilitazione della protezione da terminazione per un'istanza, consulta Abilitare la protezione da cessazione.

Per creare un allarme per arrestare un'istanza inattiva (console Amazon EC2)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Azioni, Monitora e risolvi i problemi, Gestisci gli allarmi. CloudWatch

   In alternativa, è possibile scegliere il segno più (

) nella colonna Alarm status (Stato allarme).
4. Nella pagina Gestisci gli CloudWatch allarmi, procedi come segue:

   a. Scegliere Create an alarm (Crea un allarme).

   b. Per ricevere un'e-mail quando viene attivato l'allarme, per Alarm notification (Notifica allarme), scegli un argomento Amazon SNS esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) nella Amazon Simple Notification Service Developer Guide.

   c. Attivare Alarm action (Azione allarme)e scegliere Terminate (Termina).

   d. Per Group samples by (Raggruppa campioni per) e Type of data to sample (Tipo di dati da campionare), scegliere una statistica e un parametro. In questo esempio, scegliere Average (Media) e CPU Utilization (Utilizzo CPU).

   e. Per Alarm When (Avvia allarme quando) e Percent (Percentuale), specificare la soglia del parametro. In questo esempio, specificare => e 10 percento.

   f. Per Consecutive period (Periodo consecutivo) e Period (Periodo), specificare il periodo di valutazione per l'allarme. In questo esempio, specificare 24 periodi consecutivi di 1 ora.

g. Amazon crea CloudWatch automaticamente un nome di allarme per te. Per modificare il nome, immettere un nuovo nome in Alarm name (Nome allarme). I nomi degli allarmi devono contenere solo caratteri ASCII.

> **Note**
>
> Puoi modificare la configurazione dell'allarme in base ai tuoi requisiti prima di creare l'allarme oppure puoi modificarlo in seguito. Questo include il parametro, la soglia, la durata, l'operazione e le impostazioni delle notifiche. Tuttavia, dopo aver creato l'allarme non è possibile modificarne il nome.

h. Scegliere Create (Crea).

Aggiungi azioni di riavvio agli allarmi Amazon CloudWatch

Puoi creare un CloudWatch allarme Amazon che monitora un'istanza Amazon EC2 e riavvia automaticamente l'istanza. L'operazione di allarme di riavvio è consigliata per gli errori di controllo dello stato dell'istanza (contrariamente all'operazione di allarme di recupero, adatta agli errori di controllo dello stato del sistema). Il riavvio di un'istanza equivale al riavvio di un sistema operativo. Nella maggior parte dei casi, sono necessari pochi minuti per riavviare l'istanza. Quando riavvii un'istanza, questa rimane sullo stesso host fisico, in modo che l'istanza conservi il proprio nome DNS pubblico, indirizzo IP privato e tutti i dati presenti nei volumi instance store.

A differenza dell'arresto e riavvio, il reboot di un'istanza non comporta l'inizio di un nuovo periodo di fatturazione oraria dell'istanza (con un addebito minimo di un minuto). Quando l'istanza viene riavviata, i dati nei volumi dell'archivio dell'istanza vengono conservati. I volumi dell'archivio dell'istanza devono essere rimontati nel file system dopo il riavvio. Per ulteriori informazioni, consulta Riavvio dell'istanza.

> **Important**
>
> Per evitare una race condition tra le operazioni di riavvio e di recupero, evita di impostare gli stessi periodi di valutazione per entrambi gli allarmi di riavvio e di recupero. È consigliabile impostare gli allarmi di riavvio su tre periodi di valutazione di un minuto ciascuno. Per ulteriori informazioni, consulta Evaluating an alarm nella Amazon CloudWatch User Guide.

Per creare un allarme per riavviare un'istanza (console Amazon EC2)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Azioni, Monitoraggio e risoluzione dei problemi, Gestione degli allarmi. CloudWatch

   In alternativa, è possibile scegliere il segno più (

) nella colonna Alarm status (Stato allarme).
4. Nella pagina Gestisci gli CloudWatch allarmi, procedi come segue:

   a. Scegliere Create an alarm (Crea un allarme).

   b. Per ricevere un'e-mail quando viene attivato l'allarme, per Alarm notification (Notifica allarme), scegli un argomento Amazon SNS esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) nella Amazon Simple Notification Service Developer Guide.

   c. Attivare Alarm action (Azione allarme)e scegliere Reboot (Riavvia).

   d. Per Group samples by (Raggruppa campioni per) e Type of data to sample (Tipo di dati da campionare), scegliere una statistica e un parametro. In questo esempio, scegliere Average (Media) e Status check failed: instance (Controllo stato fallito: istanza).

   e. Per Consecutive period (Periodo consecutivo) e Period (Periodo), specificare il periodo di valutazione per l'allarme. In questo esempio, inserisci 3 periodi consecutivi di 1 minuto. Se 1 Minuto è disabilitato, è necessario abilitare il monitoraggio dettagliato oppure è possibile scegliere invece 5 minuti.

   f. Amazon crea CloudWatch automaticamente un nome di allarme per te. Per modificare il nome, immettere un nuovo nome in Alarm name (Nome allarme). I nomi degli allarmi devono contenere solo caratteri ASCII.

   g. Scegliere Create (Crea).

Aggiungi azioni di ripristino agli CloudWatch allarmi Amazon

Puoi creare un CloudWatch allarme Amazon che monitora un'istanza Amazon EC2. Se l'istanza viene danneggiata a causa di un guasto hardware sottostante o di un problema che richiede AWS

la riparazione, puoi ripristinare automaticamente l'istanza. Le istanze terminate non possono essere recuperate. Un'istanza recuperata è identica all'istanza originale, incluso l'ID istanza, gli indirizzi IP privati, gli indirizzi IP elastici e tutti i metadati dell'istanza.

CloudWatch impedisce di aggiungere un'azione di ripristino a un allarme che si trova su un'istanza che non supporta le azioni di ripristino.

Quando viene attivato l'allarme `StatusCheckFailed_System` e viene avviata l'operazione di ripristino, riceverai una notifica dall'argomento Amazon SNS selezionato al momento della creazione dell'allarme e dell'associazione dell'operazione di ripristino. Durante il recupero dell'istanza, l'istanza viene migrata durante un riavvio di istanza e tutti i dati in memoria andranno persi. Una volta completato il processo, l'informazione viene pubblicata nell'argomento SNS configurato per l'allarme. Tutti coloro che hanno eseguito la sottoscrizione a questo argomento SNS ricevono una notifica e-mail che include lo stato del tentativo di recupero ed eventuali ulteriori istruzioni. Si nota riavvio di istanza nell'istanza recuperata.

> **Note**
>
> L'operazione di recupero può essere utilizzata solo con `StatusCheckFailed_System`, non con `StatusCheckFailed_Instance`.

I problemi seguenti possono causare il mancato superamento delle verifiche dello stato del sistema:

- Perdita di connettività di rete
- Perdita di alimentazione elettrica del sistema
- Problemi di software sull'host fisico
- Problemi hardware sull'host fisico che incidono sulla raggiungibilità della rete

L'operazione di recupero è supportata solo sulle istanze che soddisfano alcune caratteristiche. Per ulteriori informazioni, consulta Resilienza delle istanze.

Se la tua istanza dispone di un indirizzo IP pubblico, manterrà lo stesso indirizzo IP pubblico dopo il recupero.

> **Important**
>
> Per evitare una race condition tra le operazioni di riavvio e di recupero, evita di impostare gli stessi periodi di valutazione per entrambi gli allarmi di riavvio e di recupero. È consigliabile impostare gli allarmi di recupero su due periodi di valutazione di un minuto ciascuno. Per ulteriori informazioni, consulta Evaluating an alarm nella Amazon CloudWatch User Guide.

Per creare un allarme per recuperare un'istanza (console Amazon EC2)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e scegli Azioni, Monitoraggio e risoluzione dei problemi, Gestione degli allarmi. CloudWatch

   In alternativa, è possibile scegliere il segno più (
   
) nella colonna Alarm status (Stato allarme).
4. Nella pagina Gestisci gli CloudWatch allarmi, procedi come segue:

   a. Scegliere Create an alarm (Crea un allarme).

   b. Per ricevere un'e-mail quando viene attivato l'allarme, per Alarm notification (Notifica allarme), scegli un argomento Amazon SNS esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) nella Amazon Simple Notification Service Developer Guide.

   > **Note**
   >
   > Gli utenti devono sottoscrivere l'argomento SNS specificato per ricevere messaggi e-mail di notifica quando vengono attivati gli allarmi. Riceve Utente root dell'account AWS sempre notifiche e-mail quando si verificano azioni di ripristino automatico dell'istanza, anche se non è specificato un argomento SNS o l'utente root non è iscritto all'argomento SNS specificato.

   c. Attivare Alarm action (Azione allarme)e scegliere Recover (Recupera).

d. Per Group samples by (Raggruppa campioni per) e Type of data to sample (Tipo di dati da campionare), scegliere una statistica e un parametro. In questo esempio, scegliere Average (Media) e Status check failed: system (Controllo stato fallito: system).

e. Per Consecutive period (Periodo consecutivo) e Period (Periodo), specificare il periodo di valutazione per l'allarme. In questo esempio, inserisci 2 periodi consecutivi di 1 minuto. Se 1 Minuto è disabilitato, è necessario abilitare il monitoraggio dettagliato oppure è possibile scegliere invece 5 minuti.

f. Amazon crea CloudWatch automaticamente un nome di allarme per te. Per modificare il nome, immettere un nuovo nome in Alarm name (Nome allarme). I nomi degli allarmi devono contenere solo caratteri ASCII.

g. Scegliere Create (Crea).

Usa la CloudWatch console Amazon per visualizzare la cronologia degli allarmi e delle azioni

Puoi visualizzare la cronologia degli allarmi e delle azioni nella CloudWatch console Amazon. Amazon CloudWatch conserva la cronologia degli allarmi e delle azioni delle ultime due settimane.

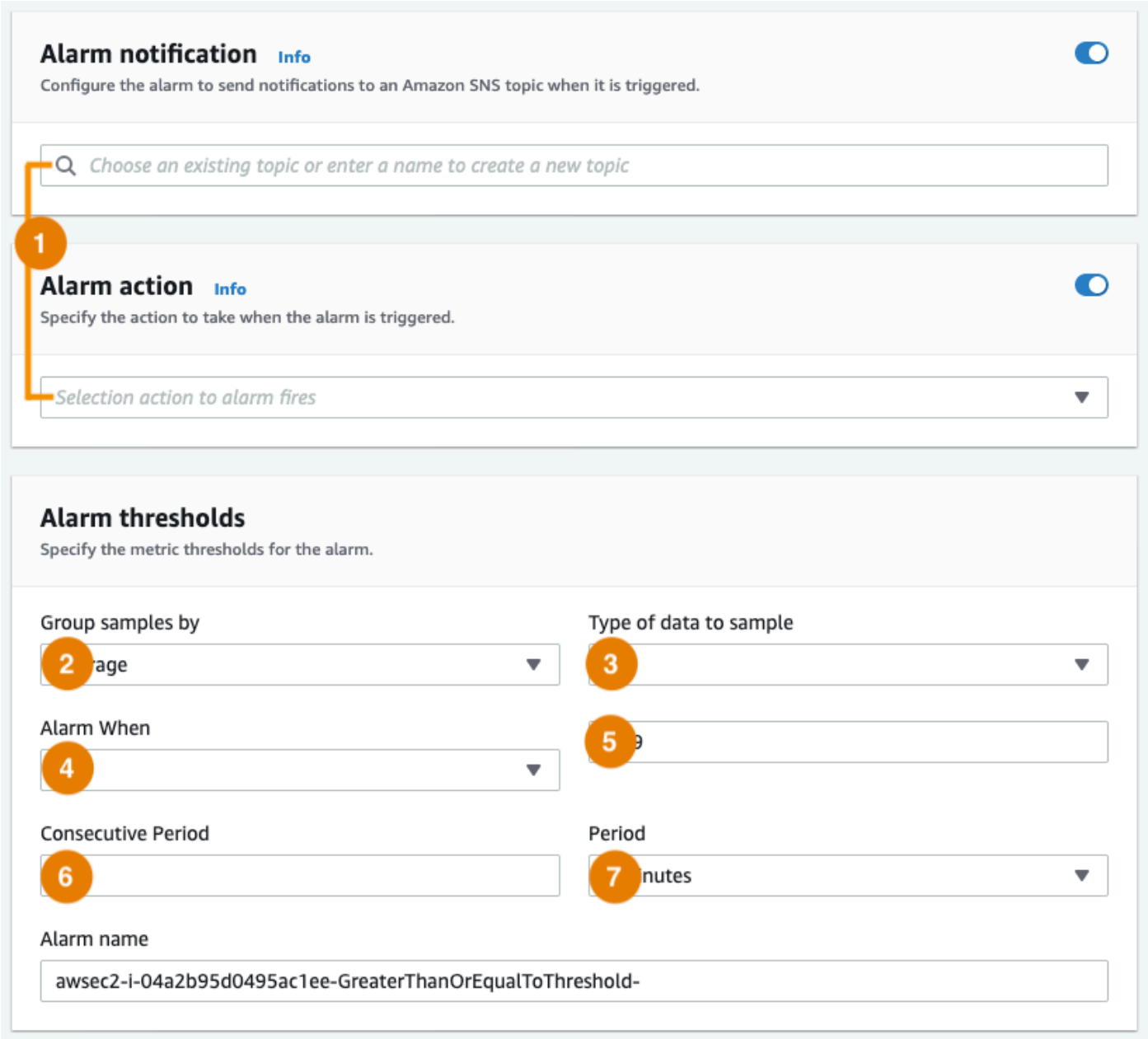
Per visualizzare la cronologia degli allarmi e delle azioni attivati (console) CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Alarms (Allarmi).
3. Seleziona un allarme.
4. La scheda Details (Dettagli) mostra lo stato di transizione più recente insieme ai valori di tempo e di parametro.
5. Scegliere la scheda History (Cronologia) per visualizzare le voci più recenti della cronologia.

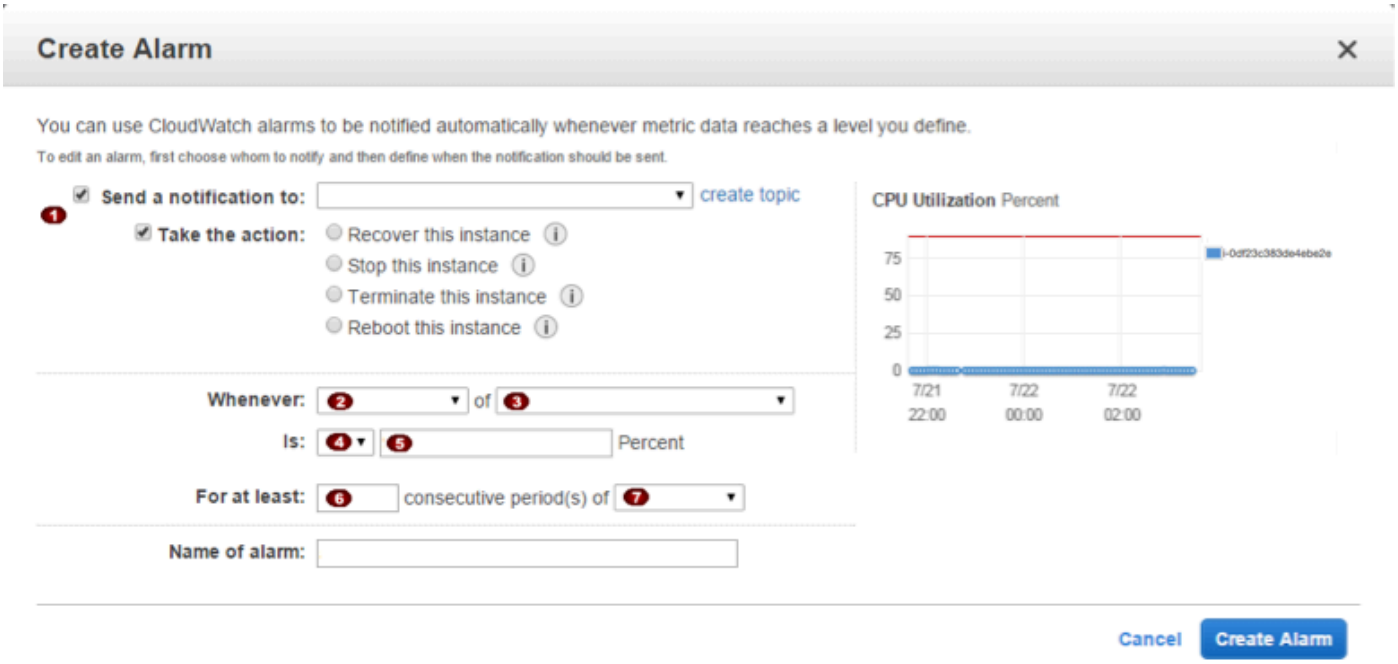
Scenari CloudWatch di azione degli allarmi di Amazon

È possibile utilizzare la console Amazon EC2 per creare operazioni dell'allarme che arrestano, avviano o terminano un'istanza Amazon EC2, se vengono soddisfatte determinate condizioni. Nello screen capture seguente della pagina della console dove configuri le operazioni dell'allarme, abbiamo numerato le impostazioni. Abbiamo anche numerato le impostazioni nello scenario che segue, per aiutarti a creare le operazioni appropriate.

New console


Alarm notification Info
Configure the alarm to send notifications to an Amazon SNS topic when it is triggered.
Choose an existing topic or enter a name to create a new topic
1
Alarm action Info
Specify the action to take when the alarm is triggered.
Selection action to alarm fires
Alarm thresholds
Specify the metric thresholds for the alarm.
Group samples by
2
Type of data to sample
3
Alarm When
4
5
Consecutive Period
6
Period
7
Alarm name
awsec2-i-04a2b95d0495ac1ee-GreaterThanOrEqualToThreshold-

Old console



Scenario 1: arrestare lo sviluppo inattivo e testare le istanze

Creare un allarme che fermi un'istanza utilizzata nello sviluppo software o testare quando è stata inattiva per almeno un'ora.

Impostazione	Valore
1	Interrompi
2	Massimo
3	Utilizzo CPU
4	<=
5	10%
6	1
7	1 ora

Scenario 2: interrompere le istanze inattive

Creare un allarme che fermi un'istanza e invii un'e-mail quando l'istanza è stata inattiva per 24 ore.

Impostazione	Valore
1	Arresto ed e-mail
2	Media
3	Utilizzo CPU
4	<=
5	5%
6	24
7	1 ora

Scenario 3: inviare un'e-mail riguardo i server Web con traffico elevato insolito

Creare un allarme che invii un'e-mail quando un'istanza eccede i 10 GB di traffico di rete in uscita al giorno.

Impostazione	Valore
1	E-mail
2	Somma
3	Rete in uscita
4	>
5	10 GB
6	24
7	1 ora

Scenario 4: interrompere i server Web con traffico elevato insolito

Creare un allarme che fermi un'istanza e invii un messaggio di testo (SMS) se il traffico di rete in uscita al giorno eccede 1 GB all'ora.

Impostazione	Valore
1	Arresto e invio SMS
2	Somma
3	Rete in uscita
4	>
5	1 GB
6	1
7	1 ora

Scenario 5: interrompere un'istanza danneggiata

Creare un allarme che fermi un'istanza che per tre volte consecutive fallisce la verifica di stato (effettuata con intervalli di 5 minuti).

Impostazione	Valore
1	Interrompi
2	Media
3	Verifica stato non riuscita: sistema
4	-
5	-
6	1

Impostazione	Valore
7	15 minuti

Scenario 6: terminare le istanze quando i processi delle elaborazioni in batch sono completati

Creare un allarme che termini un'istanza che esegue processi batch quando non invia più dati di risultati.

Impostazione	Valore
1	Interruzione
2	Massimo
3	Rete in uscita
4	<=
5	100.000 byte
6	1
7	5 minuti

Automatizza Amazon EC2 utilizzando EventBridge

Puoi utilizzare Amazon EventBridge per automatizzare Servizi AWS e rispondere automaticamente agli eventi di sistema, come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi creare regole che indichino a quali eventi sei interessato e quali operazioni automatizzate eseguire quando un evento corrisponde a una regola. Le azioni che possono essere attivate automaticamente includono le seguenti:

- Invoca una funzione AWS Lambda
- Richiamo del comando di esecuzione di Amazon EC2
- Inoltro dell'evento a flusso di dati Amazon Kinesis

- Attiva una macchina a AWS Step Functions stati
- Notifica di un argomento Amazon SNS
- Notifica di una coda Amazon SQS

Di seguito sono riportati alcuni esempi di utilizzo EventBridge con Amazon EC2:

- Attivazione di una funzione Lambda ogni volta che un'istanza entra in stato di esecuzione.
- Notifica di un argomento Amazon SNS quando un volume Amazon EBS viene creato o modificato.
- Invia un comando a una o più istanze Amazon EC2 utilizzando Amazon EC2 Run Command ogni volta che si verifica un determinato evento in un altro servizio. AWS

Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Tipi di eventi Amazon EC2

Amazon EC2 supporta i tipi di eventi seguenti:

- Cambio di stato dell'AMI EC2
- EC2 Fast Launch State-change Notification
- Errore parco istanze EC2
- Informazioni sul parco istanze EC2
- Modifica dell'istanza del parco istanze EC2
- Richiesta di modifica dell'istanza spot del parco istanze EC2
- Cambio di stato del parco istanze EC2
- Raccomandazione di ribilanciamento dell'istanza EC2
- Notifica sulla modifica dello stato dell'istanza EC2
- Errore della serie di istanze Spot EC2
- Informazioni sulla serie di istanze Spot EC2
- Modifica dell'istanza della serie di istanze Spot EC2
- Modifica della richiesta per l'istanza spot della serie di istanze Spot EC2
- Cambiamento dello stato della serie di istanze Spot EC2
- Avviso di interruzione dell'istanza spot EC2
- Evasione della richiesta di istanze spot EC2

- Notifica di sottoutilizzo prenotazione di capacità on demand EC2

Per informazioni sui tipi di eventi supportati da Amazon EBS, consulta EventBridge Amazon EBS.

Registra le chiamate API di Amazon EC2 utilizzando AWS CloudTrail

L'API Amazon EC2 è integrata con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o un. Servizio AWS CloudTrail acquisisce tutte le chiamate API per Amazon EC2 come eventi, incluse le chiamate dalla console e le chiamate di codice alle operazioni API. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata all'API Amazon EC2, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e così via.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Informazioni sull'API Amazon EC2 in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in Amazon EC2 e Amazon EBS, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con CloudTrail la cronologia degli eventi.

Per una registrazione continua degli eventi nell' Account AWS che includa eventi per Amazon EC2 e Amazon EBS, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consultare:

- Creare un percorso per il tuo Account AWS
- Servizio AWS integrazioni con log CloudTrail
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni di Amazon EC2 e le azioni di gestione di Amazon EBS vengono registrate CloudTrail e documentate nell'Amazon EC2 API Reference. Ad esempio, le chiamate a RunInstancesDescribeInstances, o CreateImageactions generano voci nei file di registro. CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

Per ulteriori informazioni, vedete l'CloudTrailuserIdentityelemento.

Comprendi le voci dei file di log dell'API Amazon EC2

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Il seguente record di file di log mostra che un utente ha terminato un'istanza.


```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
            "type":"Root",
            "principalId":"123456789012",
            "arn":"arn:aws:iam::123456789012:root",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"user"
         },
         "eventTime":"2016-05-20T08:27:45Z",
         "eventSource":"ec2.amazonaws.com",
         "eventName":"TerminateInstances",
```

```
        "awsRegion":"us-west-2",
        "sourceIPAddress":"198.51.100.1",
        "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
        "requestParameters":{
           "instancesSet":{
              "items":[{
                 "instanceId":"i-1a2b3c4d"
              }]
           }
        },
        "responseElements":{
           "instancesSet":{
              "items":[{
                 "instanceId":"i-1a2b3c4d",
                 "currentState":{
                    "code":32,
                    "name":"shutting-down"
                 },
                 "previousState":{
                    "code":16,
                    "name":"running"
                 }
              }]
           }
        },
        "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
        "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
     }
   ]
}
```


Utilizzato AWS CloudTrail per controllare le connessioni effettuate utilizzando EC2 Instance Connect

Utilizzalo AWS CloudTrail per controllare gli utenti che si connettono alle tue istanze tramite EC2 Instance Connect.

Per controllare l'attività SSH tramite EC2 Instance Connect utilizzando la console AWS CloudTrail

1. Apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.

2. Verificare di trovarsi nella regione appropriata.
3. Nel riquadro di navigazione scegliere Event history (Cronologia eventi).
4. Per Filtro, scegliere Event source (Origine evento), ec2-instance-connect.amazonaws.com.
5. (Facoltativo) Per Time range (Intervallo temporale), selezionare un intervallo di tempo.
6. Scegliere l'icona Refresh events (Aggiorna eventi).
7. La pagina visualizza gli eventi che corrispondono alle chiamate API SendSSHPublicKey. Espandi un evento utilizzando la freccia per visualizzare dettagli aggiuntivi, come il nome utente e la chiave di AWS accesso utilizzati per effettuare la connessione SSH e l'indirizzo IP di origine.
8. Per visualizzare informazioni complete sull'evento in formato JSON, scegliere View event (Visualizza evento). Il campo requestParameters contiene l'ID istanza di destinazione, il nome utente del sistema operativo e la chiave pubblica utilizzata per stabilire la connessione SSH.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
    "eventTime": "2018-09-21T21:38:00Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
```

```
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```

Se hai configurato il tuo AWS account per raccogliere CloudTrail eventi in un bucket S3, puoi scaricare e controllare le informazioni a livello di codice. Per ulteriori informazioni, consulta Ottenere e visualizzare i file di CloudTrail registro nella Guida per l'utente.AWS CloudTrail

Monitora le tue applicazioni.NET e SQL Server con Application Insights CloudWatch

CloudWatch Application Insights ti aiuta a monitorare le applicazioni.NET e SQL Server che utilizzano istanze Amazon EC2 insieme ad altre AWS risorse applicative. Identifica e configura i log dei parametri chiave tra risorse dell'applicazione e stack tecnologico (ad esempio, il database, Microsoft SQL Server, i server (IIS) web e di applicazione, il sistema operativo, i load balancer e le code). Controlla in modo continuo i parametri e i log per rilevare e correlare anomalie ed errori. Quando vengono rilevati errori e anomalie, Application Insights genera CloudWatch eventi che puoi utilizzare per impostare notifiche o intraprendere azioni. Per assistere nella risoluzione dei problemi, crea pannelli di controllo automatizzati per i problemi rilevati, che includono anomalie parametri ed errori di log correlati, insieme ad altri approfondimenti per il indirizzare verso la causa principale potenziale. I pannelli di controllo automatizzati consentono di eseguire operazioni di correzione rapide per mantenere le applicazioni integre e prevenire l'impatto sugli utenti finali dell'applicazione.

Per visualizzare un elenco completo dei log e dei parametri supportati, consulta Logs and Metrics Supported by Amazon Application Insights. CloudWatch

Informazioni fornite sui problemi rilevati

- Un breve riepilogo del problema
- L'ora e la data di inizio del problema
- La gravità del problema: forte/media/bassa
- Lo stato del problema rilevato: in corso/risolto
- Approfondimenti: approfondimenti generati automaticamente sul problema rilevato e la possibile causa principale

- Feedback sugli approfondimenti: feedback che hai fornito sull'utilità degli approfondimenti generati da CloudWatch Application Insights for .NET e SQL Server
- Osservazioni correlate: una vista dettagliata delle anomalie parametro e frammenti di errore di log pertinenti correlati al problema su vari componenti dell'applicazione

Feedback

Puoi fornire feedback sugli approfondimenti generati automaticamente sui problemi rilevati designandoli come utili o non utili. Il feedback sugli approfondimenti, insieme alla diagnostica dell'applicazione (anomalie parametri ed eccezioni di log), viene utilizzato per migliorare il rilevamento futuro di problemi simili.

Per ulteriori informazioni, consulta la documentazione di CloudWatchApplication Insights nella Amazon CloudWatch User Guide.

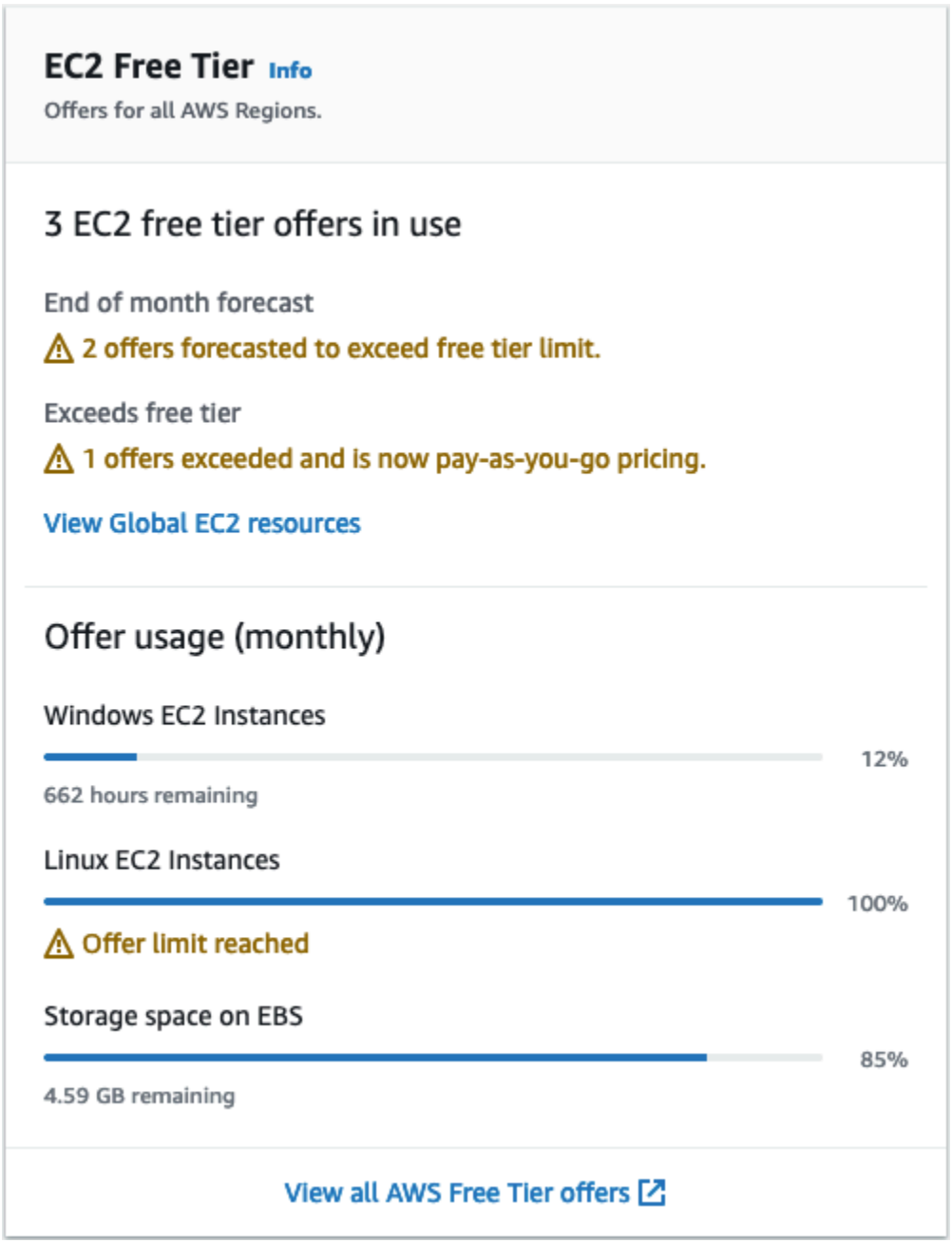
Tieni traccia dell'utilizzo del piano gratuito per Amazon EC2

Puoi utilizzare Amazon EC2 senza incorrere in addebiti se sei AWS cliente da meno di 12 mesi e rispetti i limiti di utilizzo. Piano gratuito di AWS È importante tenere traccia dell'utilizzo del piano gratuito per evitare sorprese di fatturazione. Se superi i limiti del piano gratuito, dovrai sostenere i costi standard. pay-as-go

> **Note**
>
> Se sei un AWS cliente da più di 12 mesi, non sei più idoneo all'utilizzo del piano gratuito e non visualizzerai il riquadro del piano gratuito EC2 descritto nella procedura seguente.

Monitoraggio dell'utilizzo del piano gratuito

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere EC2 Dashboard (Pannello di controllo EC2).
3. Individua la casella del piano gratuito EC2 (in alto a destra).



4. Nella casella del piano gratuito EC2, controlla l'utilizzo del piano gratuito, come segue:

   - Nella sezione Offerte del piano gratuito EC2 in uso, prendi nota dei seguenti avvisi:
     - Previsione di fine mese: ti avvisa che, se continui con il modello di utilizzo attuale, questo mese verranno addebitati degli importi.
     - Supera il piano gratuito: ti avvisa che hai superato i limiti del livello gratuito e che stai già incorrendo in addebiti.

- Nella sezione Utilizzo dell'offerta (mensile), prendi nota dell'utilizzo delle istanze Linux, delle istanze Windows e dello spazio di archiviazione EBS. La percentuale indica quanti limiti del piano gratuito hai utilizzato questo mese. Se hai raggiunto il 100%, ti verranno addebitati dei costi per un ulteriore utilizzo.

> **Note**
>
> Queste informazioni vengono visualizzate solo dopo aver creato un'istanza. Tuttavia, le informazioni sull'utilizzo non vengono aggiornate in tempo reale; ma sono aggiornate tre volte al giorno.

5. Per evitare di incorrere in ulteriori spese, elimina tutte le risorse che stanno attualmente incorrendo in addebiti o che potrebbero essere addebitate se superi il limite di utilizzo del piano gratuito.

   - Per le istruzioni su come eliminare l'istanza, consultaTermina le istanze Amazon EC2.
   - Per verificare se disponi di risorse in altre regioni che potrebbero essere soggette a costi, nella casella Piano gratuito EC2, scegli Visualizza risorse EC2 globali per aprire Vista globale EC2. Per ulteriori informazioni, consulta Amazon EC2 Global View.

6. Per visualizzare l'utilizzo delle risorse per tutti Servizi AWS Piano gratuito di AWS, seleziona Visualizza tutte le Piano gratuito di AWS offerte nella parte inferiore del riquadro EC2 Free Tier. Per ulteriori informazioni, consulta Utilizzo del Piano gratuito di AWS nella Guida per l'utente di Fatturazione AWS .

Reti in Amazon EC2

Amazon VPC ti consente di lanciare AWS risorse, come le istanze Amazon EC2, in una rete virtuale dedicata al AWS tuo account, nota come cloud privato virtuale (VPC). Quando si avvia un'istanza, è possibile selezionare una sottorete dal VPC. L'istanza è configurata con un'interfaccia di rete primaria, ovvero una scheda di rete virtuale logica. L'istanza riceve un indirizzo IP privato primario dall'indirizzo IPv4 della sottorete e viene assegnata all'interfaccia di rete primaria.

Puoi controllare se l'istanza riceve un indirizzo IP pubblico dal pool di indirizzi IP pubblici di Amazon. L'indirizzo IP pubblico di un'istanza è associato all'istanza solo fino a quando non questa viene arrestata o terminata. Se hai bisogno di un indirizzo IP pubblico persistente, puoi allocare un indirizzo IP elastico per il tuo AWS account e associarlo a un'istanza o un'interfaccia di rete. Un indirizzo IP elastico rimane associato al tuo AWS account fino a quando non lo rilasci e puoi spostarlo da un'istanza all'altra secondo necessità. Puoi inoltre portare il tuo intervallo di indirizzi IP all'interno dell'account AWS , dove viene visualizzato come pool di indirizzi; puoi quindi allocare degli indirizzi IP elastici da questo pool di indirizzi.

Per aumentare le prestazioni di rete e ridurre la latenza, puoi avviare istanze in un gruppo di posizionamento. Puoi ottenere prestazioni di pacchetto al secondo (PPS) significativamente più elevate utilizzando la connettività di rete migliorata. Utilizzando un Elastic Fabric Adapter (EFA), un dispositivo di rete che puoi collegare a un tipo di istanza supportato, puoi accelerare le applicazioni di machine learning e di elaborazione ad alte prestazioni.

Funzionalità

- Regioni e zone
- Indirizzamento IP per le istanze Amazon EC2
- Tipi di nomi host delle istanze Amazon EC2
- Utilizzare gli indirizzi IP personali (BYOIP) in Amazon EC2
- Indirizzi IP elastici
- Interfacce di rete elastiche
- Larghezza di banda di rete dell'istanza Amazon EC2
- Rete avanzata su Amazon EC2
- Elastic Fabric Adapter
- Topologia dell'istanza Amazon EC2

- Gruppi di collocamento
- Unità massima di trasmissione (MTU) di rete per istanza EC2
- Cloud privati virtuali per le tue istanze EC2

Regioni e zone

Amazon EC2 è ospitato in più località in tutto il mondo. Queste località sono composte da Availability Zones, Local Zones e Wavelength Zones. Regioni AWS AWS Outposts

- Ciascuna regione è un'area geografica distinta.
- Le zone di disponibilità sono più posizioni isolate all'interno di ogni regione.
- Le Local Zones offrono la possibilità di collocare le risorse, come calcolo e archiviazione, in più posizioni più vicine agli utenti finali.
- AWS Outposts offre AWS servizi, infrastrutture e modelli operativi nativi praticamente a qualsiasi data center, spazio di co-ubicazione o struttura locale.
- Le zone Wavelength consentono agli sviluppatori di creare applicazioni che offrono latenze molto basse a dispositivi 5G e utenti finali. Wavelength implementa servizi di elaborazione e archiviazione AWS standard ai margini delle reti 5G dei gestori di telecomunicazioni.

AWS gestisce data center state-of-the-art ad alta disponibilità. Anche se rari, i guasti che compromettono la disponibilità di istanze nella stessa ubicazione possono verificarsi. Se ospiti tutte le istanze in un'unica ubicazione in cui si verifica un guasto, nessuna di esse risulterà disponibile.

Per aiutarti a determinare quale distribuzione è più adatta a te, consulta le Domande frequenti su AWS Wavelength.

Indice

Regioni

Ogni regione è pensata per essere isolata dalle altre regioni . Ciò consente di raggiungere la maggiore stabilità e tolleranza ai guasti possibile.

Quando visualizzi le tue risorse, vedi soltanto le risorse legate alla regione specificata. Questo perché le regioni sono isolate l'una dall'altra e le risorse non vengono replicate in automatico tra le regioni.

Quando avvii un'istanza, è necessario selezionare un'AMI presente nella stessa regione. Se l'AMI si trova in una regione diversa, puoi copiare l'AMI nella regione utilizzata. Per ulteriori informazioni, consulta Copiare un'AMI.

Il trasferimento di dati tra regioni comporterà un addebito. Per ulteriori informazioni, consulta Prezzi di Amazon EC2 – Trasferimento dati.

Indice

Regioni disponibili

Il tuo account determina le regioni per te disponibili.

- An Account AWS fornisce più regioni in modo da poter avviare istanze Amazon EC2 in luoghi che soddisfano i tuoi requisiti. Ad esempio, potresti avviare istanze in Europa per esser più vicino ai clienti europei o per soddisfare i requisiti giuridici.
- Un account AWS GovCloud (Stati Uniti occidentali) fornisce l'accesso alla regione AWS GovCloud (Stati Uniti occidentali) e alla regione AWS GovCloud (Stati Uniti orientali). Per ulteriori informazioni, consulta AWS GovCloud (US).
- Un account Amazon AWS (Cina) consente l'accesso solo alle regioni di Pechino e Ningxia. Per ulteriori informazioni, consulta Amazon Web Services in Cina.

La tabella seguente elenca le regioni fornite da un. Account AWS Non puoi descrivere o accedere ad altre regioni da una Account AWS, come le AWS GovCloud (US) Regions o le regioni cinesi.

Per utilizzare una regione introdotta dopo il 20 marzo 2019, devi abilitarla. Per ulteriori informazioni, consulta Specificare AWS le regioni che il tuo account può utilizzare nella Guida AWS Account Management di riferimento.

Codice	Nome	Stato di opt-in
us-east-2	Stati Uniti orientali (Ohio)	Campo non obbligatorio
us-east-1	Stati Uniti orientali (Virginia)	Campo non obbligatorio
us-west-1	Stati Uniti occidentali (California settentrionale)	Campo non obbligatorio
us-west-2	US West (Oregon)	Campo non obbligatorio
af-south-1	Africa (Città del Capo)	Richiesto
ap-east-1	Asia Pacifico (Hong Kong)	Richiesto
ap-south-2	Asia Pacific (Hyderabad)	Richiesto
ap-southeast-3	Asia Pacifico (Giacarta)	Richiesto
ap-southeast-4	Asia Pacifico (Melbourne)	Richiesto
ap-south-1	Asia Pacifico (Mumbai)	Campo non obbligatorio
ap-northeast-3	Asia Pacifico (Osaka-Locale)	Campo non obbligatorio
ap-northeast-2	Asia Pacifico (Seoul)	Campo non obbligatorio
ap-southeast-1	Asia Pacifico (Singapore)	Campo non obbligatorio

Codice	Nome	Stato di opt-in
ap-southeast-2	Asia Pacifico (Sydney)	Campo non obbligatorio
ap-northeast-1	Asia Pacifico (Tokyo)	Campo non obbligatorio
ca-central-1	Canada (Centrale)	Campo non obbligatorio
ca-west-1	Canada occidentale (Calgary)	Richiesto
eu-central-1	Europa (Francoforte)	Campo non obbligatorio
eu-west-1	Europa (Irlanda)	Campo non obbligatorio
eu-west-2	Europa (Londra)	Campo non obbligatorio
eu-south-1	Europa (Milano)	Richiesto
eu-west-3	Europa (Parigi)	Campo non obbligatorio
eu-south-2	Europa (Spagna)	Richiesto
eu-north-1	Europa (Stoccolma)	Campo non obbligatorio
eu-central-2	Europa (Zurigo)	Richiesto
il-central-1	Israele (Tel Aviv)	Richiesto
me-south-1	Medio Oriente (Bahrein)	Richiesto
me-central-1	Medio Oriente (Emirati Arabi Uniti)	Richiesto

Codice	Nome	Stato di opt-in
sa-east-1	Sud America (San Paolo)	Campo non obbligato rio

Per ulteriori informazioni, consulta Infrastruttura globale di AWS.

Il numero e la mappatura delle zone di disponibilità per regione potrebbero variare tra Account AWS . Per ottenere un elenco delle zone di disponibilità disponibili per il tuo account, puoi utilizzare la console Amazon EC2 o l'interfaccia a riga di comando. Per ulteriori informazioni, consulta Descrizione delle regioni.

Regioni ed endpoint

Quando utilizzi un'istanza tramite l'interfaccia a riga di comando o le operazioni API, è necessario specificare il relativo endpoint regionale. Per ulteriori informazioni sugli endpoint e le regioni di Amazon EC2, consulta Endpoint e quote di Amazon EC2 nella Riferimenti generali di Amazon Web Services.

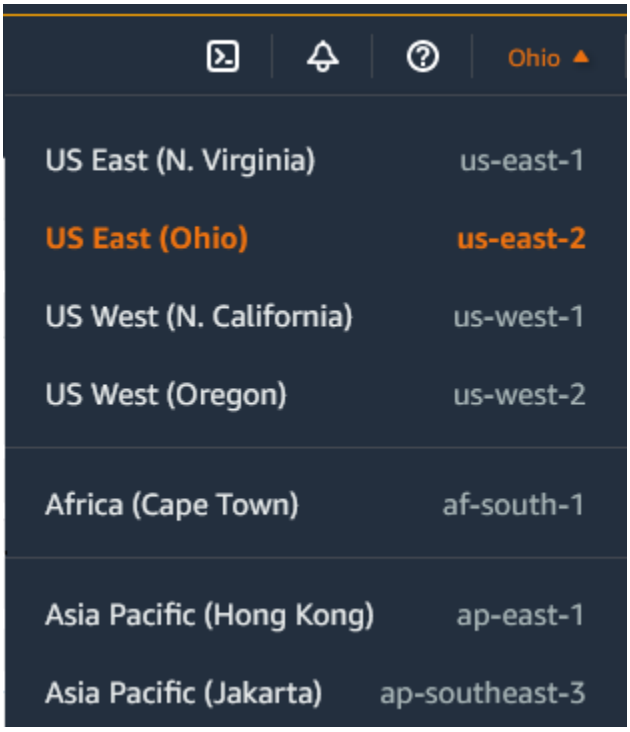
Per ulteriori informazioni sugli endpoint e i protocolli in AWS GovCloud (Stati Uniti occidentali), consulta Service Endpoints nella Guida per l'AWS GovCloud (US) utente.

Descrizione delle regioni

Puoi utilizzare la console Amazon EC2 o l'interfaccia a riga di comando per determinare quali regioni sono disponibili per il tuo account. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

Per trovare le regioni utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli il selettore Regioni.



3. Le risorse EC2 per questa regione vengono visualizzate nella sezione Risorse del Pannello di controllo EC2.

Per trovare le tue regioni, utilizza il AWS CLI

Utilizzare il comando describe-regions come riportato di seguito per descrivere le regioni abilitate per l'account.

```
aws ec2 describe-regions
```

Per descrivere tutte le regioni, incluse le regioni disabilitate per l'account, aggiungere l'opzione `--all-regions` come segue.

```
aws ec2 describe-regions --all-regions
```

Visualizzazione del nome della regione

È possibile utilizzare AWS Systems Manager Parameter Store per visualizzare il nome visualizzato di una regione. Ogni regione riporta i parametri pubblici nel percorso seguente.

```
/aws/service/global-infrastructure/regions/region-code
```

I parametri pubblici di una regione includono quanto segue:

- /aws/service/global-infrastructure/regions/*region-code*/domain
- /aws/service/global-infrastructure/regions/*region-code*/geolocationCountry
- /aws/service/global-infrastructure/regions/*region-code*/geolocationRegion
- /aws/service/global-infrastructure/regions/*region-code*/longName
- /aws/service/global-infrastructure/regions/*region-code*/partition

Il parametro `longName` contiene il nome visualizzato della regione. Il get-parameters-by-pathcomando seguente restituisce il nome visualizzato della `af-south-1` regione. Utilizza l'opzione `--query` per definire l'output in base al nome della regione. È necessario racchiudere la stringa di query tra virgolette singole su Linux. Per eseguire questo comando utilizzando il prompt dei comandi di Windows, ometti le virgolette singole o modificale in virgolette doppie.

AWS CLI on Linux

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/regions/af-south-1 \
    --query 'Parameters[?Name.contains(@,`longName`)].Value' \
    --output text
```

AWS CLI on Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/regions/af-south-1 ^
    --query "Parameters[?Name.contains(@,`longName`)].Value" ^
    --output text
```

Tools for PowerShell

Se non è installato, installa AWS.Tools. SimpleSystemsManagementmodulo su Tools for PowerShell eseguendo. `Install-AWSToolsModule AWS.Tools.SimpleSystemsManagement -CleanUp`

```
$parameterPath = "/aws/service/global-infrastructure/regions/af-south-1"
$substringToMatch = "longName"
$filteredParameters = Get-SSMParametersByPath -Path $parameterPath `
| Where-Object { $_.Name -like "*$substringToMatch*" } `
| ForEach-Object { Write-Output $_.Value }
```

```
$filteredParameters
```

Di seguito è riportato un output di esempio.

```
Africa (Cape Town)
```

Per ulteriori informazioni, consulta la pagina Utilizzo dei parametri pubblici nella Guida per l'utente di AWS Systems Manager .

Specificazione della regione di una risorsa

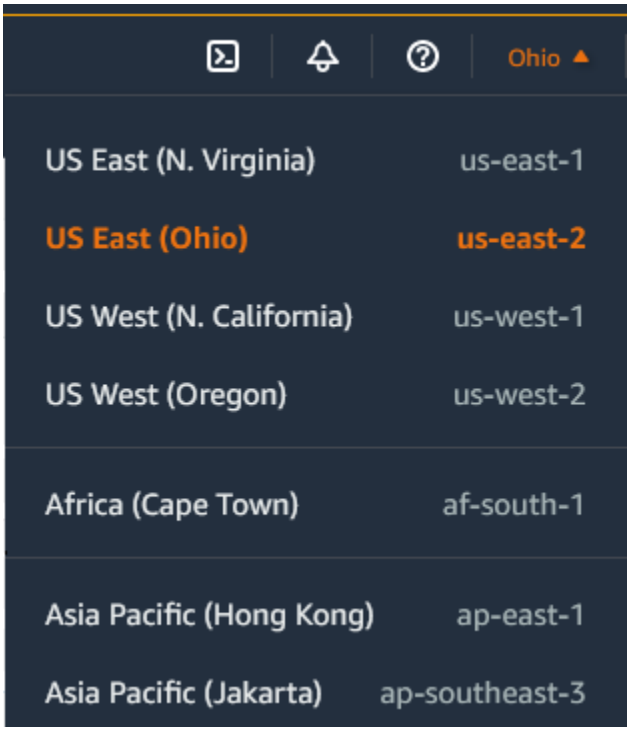
Ogni volta che crei una risorsa Amazon EC2, puoi specificare la regione per la risorsa. È possibile specificare la regione per una risorsa utilizzando AWS Management Console o la riga di comando.

Considerazioni

Alcune AWS risorse potrebbero non essere disponibili in tutte le regioni. Prima di avviare un'istanza, assicurati di poter creare le risorse necessarie nelle regioni desiderate.

Specifica della regione per una risorsa tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli il selettore Regions (Regioni) e seleziona la regione.



Specifica della regione predefinita tramite la riga di comando

Puoi impostare il valore di una variabile di ambiente sull'endpoint regionale desiderato, ad esempio, `https://ec2.us-east-2.amazonaws.com`):

- `AWS_DEFAULT_REGION` (AWS CLI)
- `Set-AWSDefaultRegion` (AWS Tools for Windows PowerShell)

In alternativa, è possibile utilizzare l'opzione della riga di comando `--region` (AWS CLI) o `-Region` (AWS Tools for Windows PowerShell) con ciascun singolo comando. Ad esempio, `--region us-east-2`.

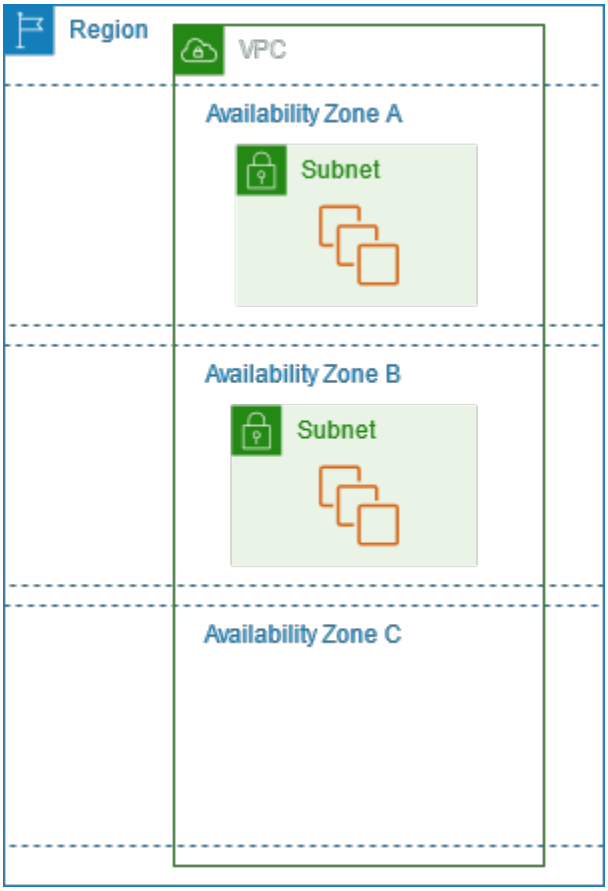
Per ulteriori informazioni sugli endpoint per Amazon EC2, consulta Endpoint e quote di Amazon EC2 nel. Riferimenti generali di AWS

Zone di disponibilità

Ciascuna regione presenta più località isolate, conosciute come zone di disponibilità. Il codice per la zona di disponibilità è il codice della Regione seguito da un identificatore con una lettera. Ad esempio, `us-east-1a`.

Quando avvii un'istanza, selezioni una Regione e un cloud privato virtuale (VPC), quindi puoi selezionare una sottorete da una delle zone di disponibilità o lasciarcene scegliere una per te. Se distribuisci le istanze tra più zone di disponibilità e un'istanza ha esito negativo, puoi progettare l'applicazione affinché un'istanza di un'altra zona di disponibilità gestisca le richieste. Puoi inoltre utilizzare indirizzi IP elastici per mascherare il guasto di un'istanza in una zona di disponibilità mappando nuovamente in modo rapido l'indirizzo a un'istanza in un'altra zona di disponibilità.

Il diagramma seguente illustra più zone di disponibilità in una regione. AWS La zona di disponibilità A e la zona di disponibilità B hanno ciascuna una sottorete e ogni sottorete contiene istanze. La zona di disponibilità C non ha sottoreti, pertanto non puoi avviare istanze in questa zona di disponibilità.



Poiché le zone di disponibilità crescono nel corso del tempo, la nostra capacità di espanderle può divenire limitata. Se ciò accade, potremmo impedire l'avvio di un'istanza in una zona di disponibilità limitata, a meno che tu non disponga già di un'istanza in tale zona di disponibilità. Infine, potremmo rimuovere la zona di disponibilità vincolata dall'elenco delle zone di disponibilità per i nuovi account. Pertanto, il tuo account potrebbe presentare una quantità diversa di zone di disponibilità disponibili in una regione rispetto a un altro account.

Indice

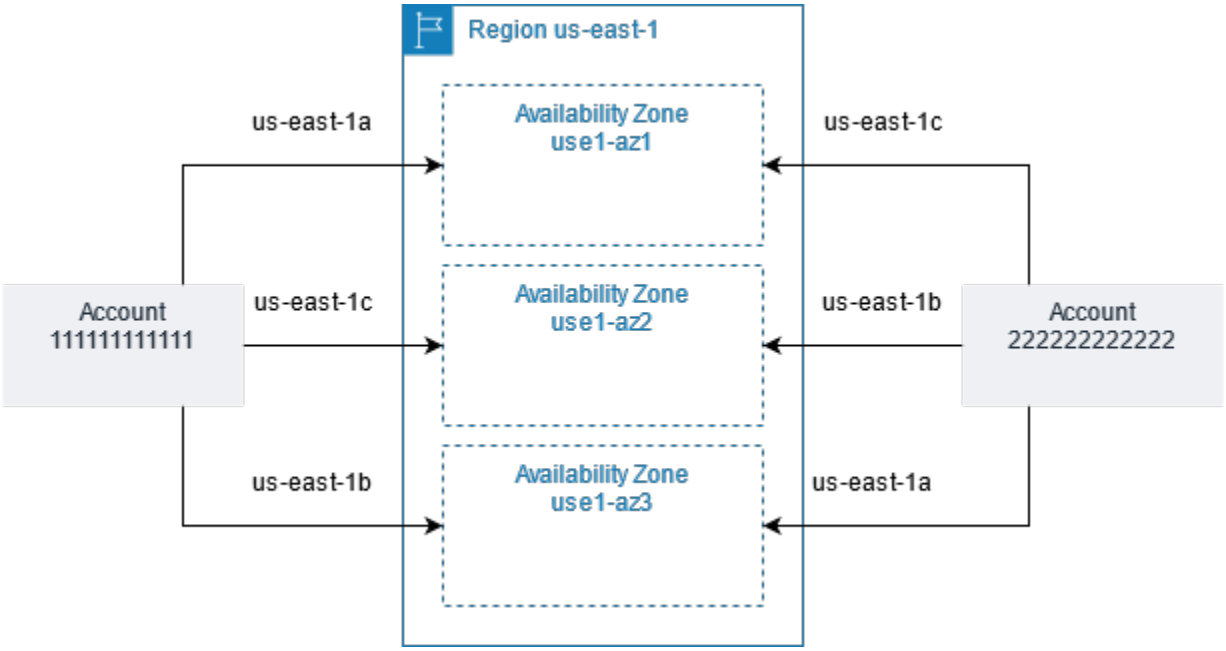
ID delle zone di disponibilità

Per garantire che le risorse siano distribuite tra le zone di disponibilità di una regione, associamo in modo indipendente le zone di disponibilità ai codici di ciascuna Account AWS delle nostre regioni

più vecchie. Ad esempio, la `us-east-1a` tua sede Account AWS potrebbe non essere la stessa ubicazione fisica `us-east-1a` di un'altra Account AWS.

Per coordinare le zone di disponibilità tra gli account in tutte le regioni, anche quelli che mappano le zone di disponibilità, utilizza gli ID AZ, che sono identificatori univoci e coerenti per una zona di disponibilità. Ad esempio, `use1-az1` è un ID AZ per la `us-east-1` regione e ha la stessa posizione fisica in ogni Account AWS regione. Puoi visualizzare gli ID della zona di disponibilità del tuo account per stabilire la posizione fisica delle tue risorse rispetto alle risorse in un altro account. Ad esempio, se condividi una sottorete nella zona di disponibilità con l'ID AZ `use1-az2` con un altro account, questa sottorete è disponibile per tale account nella zona di disponibilità il cui ID AZ è anche `use1-az2`.

Il diagramma seguente illustra due account con mappature diverse del codice della zona di disponibilità per l'ID della zona di disponibilità.



Descrizione delle zone di disponibilità

Puoi utilizzare la console Amazon EC2 o l'interfaccia a riga di comando per determinare quali zone di disponibilità sono disponibili per il tuo account. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

Per trovare le zone di disponibilità utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli il selettore Regions (Regioni) e seleziona la regione.

3. Nel riquadro di navigazione selezionare EC2 Dashboard (Pannello di controllo EC2).
4. Le zone di disponibilità sono elencate nel riquadro Service health (Stato servizio).

Per trovare le tue zone di disponibilità, utilizza il AWS CLI

- Utilizza il describe-availability-zonescomando seguente per descrivere le zone di disponibilità all'interno della regione specificata che sono abilitate per il tuo account.

```
aws ec2 describe-availability-zones --region region-name
```

- Utilizzate il describe-availability-zonescomando come segue per descrivere le zone di disponibilità indipendentemente dallo stato di attivazione.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Avvio di istanze in una zona di disponibilità

All'avvio di un'istanza, seleziona una regione che collochi le istanze più vicine a clienti specifici o che soddisfi i requisiti giuridici o di altro tipo. Avviando le istanze in zone di disponibilità separate, puoi proteggere le tue applicazioni dai guasti di una singola ubicazione.

Quando avvii un'istanza, puoi opzionalmente specificare una zona di disponibilità nella regione utilizzata. Se non specifichi una zona di disponibilità, ne viene selezionata una automaticamente. Quando avvii le istanze iniziali, ti consigliamo di accettare la zona di disponibilità predefinita. Questo ci consente di selezionare per te la miglior zona di disponibilità a seconda dello stato del sistema e della capacità disponibile. Se avvii istanze aggiuntive, specifica una zona di disponibilità solo se le nuove istanze devono essere vicine alle istanze in esecuzione o separate da esse.

Migrazione di un'istanza verso un'altra zona di disponibilità

Se necessario, puoi eseguire la migrazione di un'istanza da una zona di disponibilità a un'altra. Ad esempio, se provi a modificare il tipo di istanza della tua istanza e non possiamo avviare un'istanza del nuovo tipo nella zona di disponibilità corrente, puoi eseguire la migrazione dell'istanza a una zona di disponibilità con capacità per il nuovo tipo di istanza.

Il processo di migrazione comporta:

- Creazione di un'AMI dall'istanza originale

- Avvio di un'istanza nella nuova zona di disponibilità
- Aggiornamento della configurazione della nuova istanza, come illustrato nella procedura seguente

Per migrare un'istanza verso un'altra zona di disponibilità

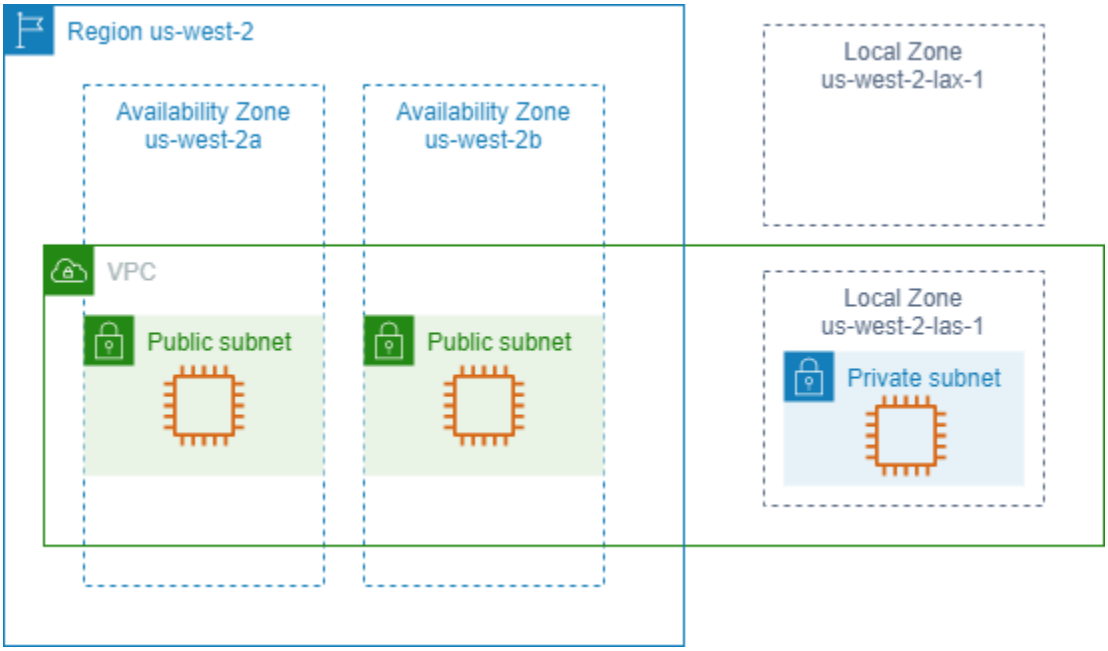
1. Creare un'AMI dall'istanza. La procedura dipende dal tipo di volume del dispositivo root per l'istanza. Per ulteriori informazioni, consultate la documentazione corrispondente al volume del dispositivo root:
   - Crea un'AMI supportata da Amazon EBS
   - Creazione di un'AMI Linux supportata da un instance store
2. Se occorre conservare l'indirizzo IPv4 privato dell'istanza, è necessario eliminare la sottorete nella zona di disponibilità corrente, quindi creare una sottorete nella nuova zona di disponibilità con lo stesso intervallo di indirizzi IPv4 della sottorete originale. È necessario terminare tutte le istanze in una sottorete prima di poterle eliminare. Devi quindi creare AMI da tutte le istanze nella sottorete in modo da poter spostare tutte le istanze dalla sottorete corrente a quella nuova.
3. Avviare un'istanza dall'AMI appena creata, specificando la nuova zona di disponibilità o sottorete. Puoi utilizzare lo stesso tipo di istanza dell'istanza originale o selezionare un nuovo tipo di istanza. Per ulteriori informazioni, consulta Avvio di istanze in una zona di disponibilità.
4. Se l'istanza originale dispone di un indirizzo IP elastico associato, associarlo alla nuova istanza. Per ulteriori informazioni, consulta Annullare l'associazione di un indirizzo IP elastico.
5. Se l'istanza originale è un'Istanza riservata, modificare la zona di disponibilità per la prenotazione. Se hai modificato anche il tipo di istanza, puoi inoltre modificare il tipo di istanza della prenotazione. Per ulteriori informazioni, consulta Inviare richieste di modifica.
6. (Opzionale) Terminare l'istanza originale. Per ulteriori informazioni, consulta Terminare un'istanza.

Zone locali

Una zona locale è un'estensione di una AWS regione situata in prossimità geografica degli utenti. Le Local Zone dispongono di connessioni proprie a Internet e all'assistenza AWS Direct Connect, in modo che le risorse create in una Local Zone possano servire gli utenti locali con comunicazioni a bassa latenza. Per ulteriori informazioni, consulta What is AWS Local Zones? nella AWS Local Zones User Guide.

Il codice di una zona locale è il relativo codice della Regione seguito da un identificatore che ne indica la posizione fisica. Ad esempio, `us-west-2-lax-1` a Los Angeles.

Il diagramma seguente illustra la AWS regione`us-west-2`, due delle relative zone di disponibilità e due delle relative zone locali. Il VPC copre le zone di disponibilità e una delle zone locali. Ogni zona del VPC contiene una sottorete e ogni sottorete contiene un'istanza.



Per utilizzare Local Zone, occorre dapprima abilitarlo. Per ulteriori informazioni, consulta the section called “Adesione alle Local Zones”. Creare una sottorete nella Local Zone. Infine, avvia le risorse nella sottorete della zona locale, ad esempio le istanze, in modo che le applicazioni siano vicine ai tuoi utenti.

Indice

Zone locali disponibili

Puoi utilizzare la console di Amazon EC2 o l'interfaccia a riga di comando per determinare le zone locali disponibili per il tuo account. Per un elenco completo, consulta Posizioni delle zone locali di AWS.

Per trovare le Local Zones utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli il selettore Regioni e seleziona la regione principale.
3. Nel riquadro di navigazione selezionare EC2 Dashboard (Pannello di controllo EC2).
4. Nell'angolo in alto a destra della pagina scegliere Account Attributes (Attributi account), Zones (Zone).

Per trovare le tue Local Zones usando il AWS CLI

Utilizzate il describe-availability-zonescomando come segue per descrivere tutte le Local Zones nella regione specificata, anche se non sono abilitate. Per descrivere solo le zone locali che hai abilitato, ometti l'opzione `--all-availability-zones`.

```
aws ec2 describe-availability-zones --region region-name --filters Name=zone-
type,Values=local-zone --all-availability-zones
```

Adesione alle Local Zones

Prima di specificare una zona locale per una risorsa o un servizio, è necessario aderire esplicitamente a Local Zones (Zone locali).

Considerazione

Alcune AWS risorse potrebbero non essere disponibili in tutte le regioni. Assicurarsi di poter creare le risorse necessarie nelle Regioni o Local Zones desiderate prima di avviare un'istanza in una specifica Local Zone. Per un elenco di servizi supportati in ogni zona locale, consulta Funzioni delle zone locali di AWS.

Per aderire alle Local Zones utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nell'angolo superiore sinistro della pagina, seleziona New EC2 Experience (Nuova esperienza EC2). Non è possibile completare questa attività utilizzando la vecchia esperienza della console.
3. Nella barra di navigazione, scegli il selettore Regions (Regioni) e seleziona la regione principale.
4. Nel riquadro di navigazione selezionare EC2 Dashboard (Pannello di controllo EC2).
5. Nell'angolo in alto a destra della pagina scegliere Account Attributes (Attributi account), Zones (Zone).

6. Scegli una zona locale e scegli Azione > Gestisci gruppo di zone.
7. In Stato di attivazione, scegli Abilita.
8. Scegli Aggiorna.

Per attivare l'accesso a Local Zones utilizzando il AWS CLI

Utilizza il comando modify-availability-zone-group.

Avvio di istanze in una Local Zone

Quando avvii un'istanza puoi specificare una sottorete che si trova in una Local Zone. Puoi allocare un indirizzo IP da un gruppo di confine di rete. Un gruppo di confine di rete è un insieme univoco di zone di disponibilità, Local Zones o zone Wavelength da cui AWS pubblicizza gli indirizzi IP, ad esempio `us-west-2-lax-1a`.

Puoi allocare gli indirizzi IP seguenti da un gruppo di confine di rete:

- Indirizzi IPv4 elastici forniti da Amazon
- Indirizzi VPC IPv6 forniti da Amazon (disponibili solo nelle zone di Los Angeles)

Per ulteriori informazioni su come avviare un'istanza in una Local Zone, consulta Getting started with AWS Local Zones nella AWS Local Zones User Guide.

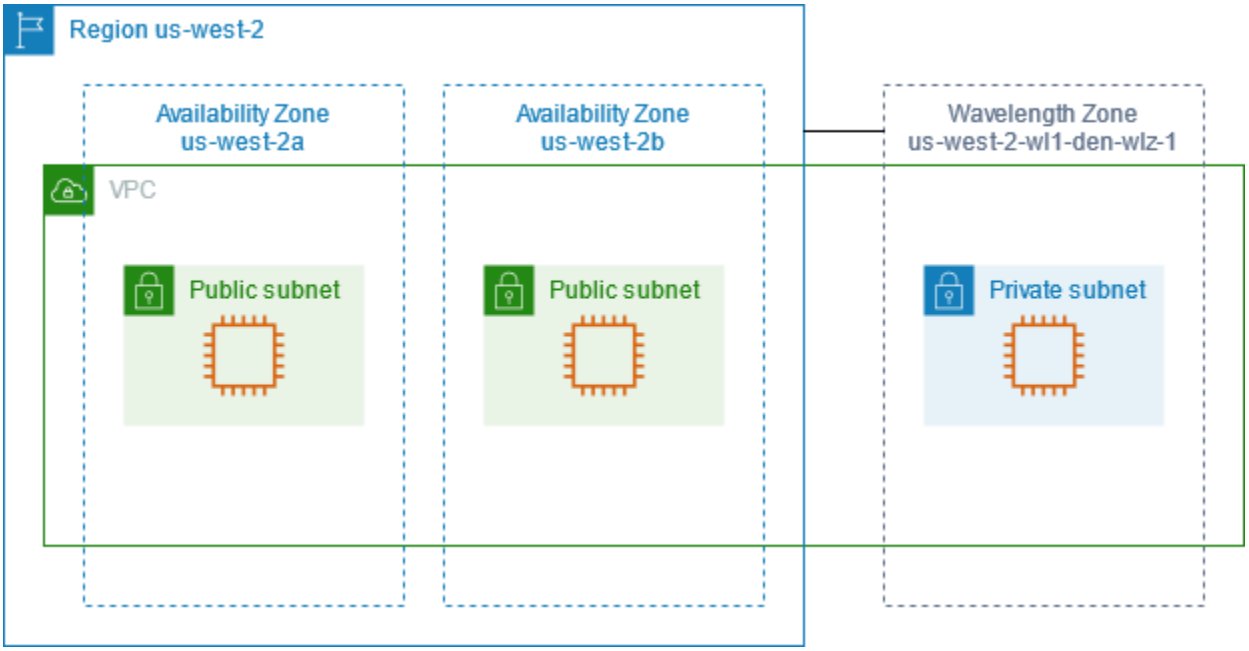
Zone Wavelength

AWS Wavelength consente agli sviluppatori di creare applicazioni che offrono latenze estremamente basse ai dispositivi mobili e agli utenti finali. Wavelength implementa servizi di elaborazione e archiviazione AWS standard ai margini delle reti 5G dei gestori di telecomunicazioni. Gli sviluppatori possono estendere un cloud privato virtuale (VPC) a una o più Wavelength Zone e quindi utilizzare risorse come le istanze AWS Amazon EC2 per eseguire applicazioni che richiedono una latenza estremamente bassa e una connessione ai servizi della regione. AWS

Una zona Wavelength è una zona isolata nella posizione carrier in cui viene distribuita l'infrastruttura Wavelength. Le zone Wavelength sono legate a una regione. Una zona Wavelength è un'estensione logica di una regione ed è gestita dal piano di controllo nella regione.

Il codice di una zona Wavelength è il relativo codice della Regione seguito da un identificatore che ne indica la posizione fisica. Ad esempio, `us-east-1-wl1-bos-wlz-1` a Boston.

Il diagramma seguente illustra la AWS regione`us-west-2`, due delle sue zone di disponibilità e una zona di Wavelength. Il VPC copre le zone di disponibilità e la zona Wavelength. Ogni zona del VPC contiene una sottorete e ogni sottorete contiene un'istanza.



Per utilizzare una zona Wavelength, devi prima accettare esplicitamente la zona. Per ulteriori informazioni, consulta the section called “Abilitazione delle zone Wavelength”. Crea quindi una sottorete nella zona Wavelength. Infine, avvia le risorse nella sottorete delle zone Wavelength in modo che le applicazioni siano più vicine agli utenti finali.

Le zone Wavelength non sono disponibili in tutte le regioni. Per informazioni sulle regioni che supportano le zone Wavelength, consulta Zone Wavelength disponibili nella Guida per gli sviluppatori di AWS Wavelength .

Indice

Descrizione delle zone Wavelength

Puoi utilizzare la console Amazon EC2 o l'interfaccia a riga di comando per determinare quali Wavelength sono disponibili per il tuo account. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

Per trovare le zone Wavelength utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli il selettore Regions (Regioni) e seleziona la regione.
3. Nel riquadro di navigazione selezionare EC2 Dashboard (Pannello di controllo EC2).
4. Nell'angolo in alto a destra della pagina scegliere Account Attributes (Attributi account), Zones (Zone).

Per trovare le tue Wavelength Zone usando il AWS CLI

- Usa il describe-availability-zonescomando seguente per descrivere le Wavelength Zone all'interno della regione specificata che sono abilitate per il tuo account.

```
aws ec2 describe-availability-zones --region region-name
```

- Utilizzate il describe-availability-zonescomando come segue per descrivere le Wavelength Zones indipendentemente dallo stato dell'opt-in.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Abilitazione delle zone Wavelength

Prima di specificare una zona Wavelength per una risorsa o un servizio, è necessario abilitare le zone Wavelength.

Considerazioni

- Alcune AWS risorse non sono disponibili in tutte le regioni. Assicurati di poter creare le risorse necessarie nella regione o nella zona Wavelength desiderata prima di avviare un'istanza in una zona Wavelength specifica.

Per l'accettazione esplicita delle zone Wavelength utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nell'angolo superiore sinistro della pagina, seleziona New EC2 Experience (Nuova esperienza EC2). Non è possibile completare questa attività utilizzando la vecchia esperienza della console.
3. Nella barra di navigazione, scegli il selettore Regioni e seleziona la regione.

4. Nel riquadro di navigazione selezionare EC2 Dashboard (Pannello di controllo EC2).
5. Nell'angolo in alto a destra della pagina scegliere Account Attributes (Attributi account), Zones (Zone).
6. Scegliete una Wavelength Zone e scegliete Azione > Gestisci gruppo Zone.
7. In Stato di attivazione, scegli Abilita.
8. Scegli Aggiorna.

Per abilitare Wavelength Zones utilizzando il AWS CLI

Utilizza il comando modify-availability-zone-group.

Avvio di istanze in una zona Wavelength

Quando avvii un'istanza puoi specificare una sottorete che si trova in una zona Wavelength. Inoltre puoi assegnare un indirizzo IP da un gruppo di confine di rete, che è un insieme univoco di zone di disponibilità, zone locali o zone Wavelength da cui AWS pubblicizza gli indirizzi IP, ad esempio `us-east-1-wl1-bos-wlz-1`.

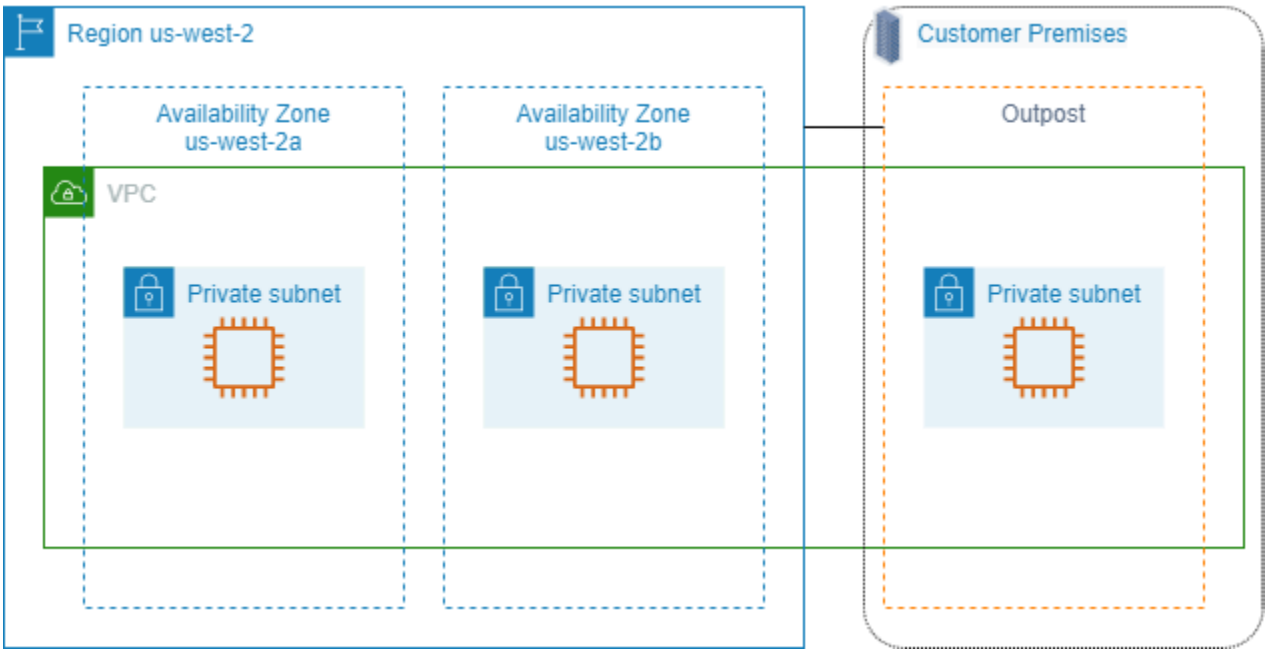
Per informazioni su come avviare un'istanza in una zona Wavelength, consulta Nozioni di base su AWS Wavelength nella Guida per gli sviluppatori di AWS Wavelength .

AWS Outposts

AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura, i servizi, le API e gli strumenti alle sedi dei clienti. Fornendo l'accesso locale all'infrastruttura AWS gestita, AWS Outposts consente ai clienti di creare ed eseguire applicazioni in locale utilizzando le stesse interfacce di programmazione AWS delle regioni, utilizzando al contempo risorse di elaborazione e archiviazione locali per esigenze di elaborazione dati locali e latenza inferiori.

Un Outpost è un pool di capacità di AWS elaborazione e archiviazione distribuito presso la sede di un cliente. AWS gestisce, monitora e gestisce questa capacità come parte di una regione. AWS Puoi creare sottoreti su Outpost e specificarle quando crei risorse. AWS Le istanze nelle sottoreti Outpost comunicano con altre istanze della AWS regione utilizzando indirizzi IP privati, tutti all'interno dello stesso VPC.

Il diagramma seguente illustra la AWS regione`us-west-2`, due delle sue zone di disponibilità e un Outpost. Il VPC copre le zone di disponibilità e l'Outpost. L'Outpost si trova in un data center locale del cliente. Ogni zona del VPC contiene una sottorete e ogni sottorete contiene un'istanza.



Per iniziare a utilizzarlo AWS Outposts, devi creare un Outpost e ordinare la capacità di Outpost. Per ulteriori informazioni sulle configurazioni degli Outpost, consulta il nostro catalogo. Dopo aver installato l'apparecchiatura Outpost, la capacità di calcolo e archiviazione è disponibile quando avvii le istanze Amazon EC2 sul tuo Outpost.

Avvio di istanze su un Outpost

Puoi avviare istanze EC2 nella sottorete Outpost che hai creato. I gruppi di sicurezza controllano il traffico in entrata e in uscita per le istanze con interfaccia di rete elastica in una sottorete Outpost, come per le istanze di una sottorete zona di disponibilità. Per connettersi a un'istanza EC2 in una sottorete Outpost, puoi specificare una coppia di chiavi quando avvii l'istanza, come fai per le istanze in una sottorete zona di disponibilità.

Si consiglia di limitare il volume root di un'istanza su un rack Outpost a 30 GiB o inferiore. È possibile specificare i volumi di dati nel mappatura dei dispositivi a blocchi dell'AMI o dell'istanza per fornire ulteriore archiviazione. Per eliminare i blocchi inutilizzati dal volume di avvio, consulta How to Build Sparse EBS Volumes nel Partner Network Blog. AWS

Si consiglia di aumentare il timeout NVMe per il volume root. Per ulteriori informazioni, consulta Timeout delle operazioni di I/O.

Per informazioni su come creare un Outpost, consulta Nozioni di base su AWS Outposts nella Guida per l'utente di AWS Outposts .

Creazione di un volume in un rack Outpost

AWS Outposts offre fattori di forma per rack e server. Se la capacità si trova su un rack Outpost, puoi creare volumi EBS nella sottorete Outpost che hai creato. Quando crei il volume, specifica il nome della risorsa Amazon (ARN) dell'Outpost.

Il seguente comando create-volume crea un volume vuoto di 50 GB nell'Outpost specificato.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

Puoi modificare dinamicamente la dimensione dei tuoi volumi gp2 Amazon EBS senza scollegarli. Per ulteriori informazioni sulla modifica di un volume senza scollegarlo, consulta Richiedere modifiche ai volumi EBS.

Indirizzamento IP per le istanze Amazon EC2

Amazon EC2 e Amazon VPC supportano entrambi i protocolli di indirizzamento IPv4 e IPv6. Per impostazione predefinita, Amazon VPC utilizza il protocollo di indirizzamento IPv4; tale comportamento non può essere disabilitato. Quando crei un VPC, devi specificare un blocco CIDR IPv4 (un intervallo di indirizzi IPv4 privati). Facoltativamente, è possibile decidere di assegnare un blocco CIDR IPv6 al VPC e alle sottoreti e di assegnare gli indirizzi IPv6 del blocco alle istanze presenti nelle sottoreti.

Indice

Indirizzi IPv4 privati

Un indirizzo IPv4 privato è un indirizzo IP non raggiungibile tramite Internet. Si possono utilizzare gli indirizzi IPv4 privati per la comunicazione tra istanze nello stesso VPC. Per ulteriori informazioni sugli standard e sulle specifiche degli indirizzi IPv4 privati, consulta RFC 1918. Gli indirizzi IPv4 privati vengono allocati sulle istanze tramite DHCP.

> **Note**
>
> Puoi creare un VPC dotato di un blocco CIDR instradabile pubblicamente che non rientra negli intervalli di indirizzi IPv4 privati specificati in RFC 1918. Tuttavia, per gli scopi di questa documentazione, ci riferiamo agli indirizzi IPv4 privati (o "Indirizzi IP privati") come agli indirizzi IP compresi nell'intervallo CIDR IPv4 del tuo VPC.

Le sottoreti VPC possono essere dei seguenti tipi:

Le sottoreti VPC possono essere dei seguenti tipi:

- Sottoreti solo IPv4: è possibile creare risorse in queste sottoreti solo con indirizzi IPv4 assegnati.
- Sottoreti solo IPv6: è possibile creare risorse in queste sottoreti solo con indirizzi IPv6 assegnati.
- Sottoreti IPv4 e IPv6: è possibile creare risorse in queste sottoreti sia con gli indirizzi IPv4 che IPv6 assegnati.

Quando si avvia un'istanza EC2 in una sottorete solo IPv4 o dual stack (IPv4 e IPv6), l'istanza riceve un indirizzo IP privato primario dall'intervallo di indirizzi IPv4 della sottorete. Per ulteriori informazioni, consulta la sezione Assegnazione di indirizzi IP nella Guida per l'utente di Amazon VPC. Se quando avvii l'istanza non specifichi un indirizzo IP privato primario, saremo noi a selezionare per tuo conto un indirizzo IP disponibile nell'intervallo IPv4 della sottorete. Ogni istanza dispone di un'interfaccia di rete predefinita (eth0) a cui è assegnato l'indirizzo IPv4 privato primario. Si possono anche specificare ulteriori indirizzi IPv4 privati, i cosiddetti indirizzi IPv4 privati secondari. A differenza di quelli primari, gli indirizzi IP privati secondari possono essere riassegnati da un'istanza all'altra. Per ulteriori informazioni, consulta Indirizzi IP multipli per le tue istanze EC2.

Un indirizzo IPv4 privato, a prescindere che si tratti di un indirizzo primario o secondario, rimane associato all'interfaccia di rete quando l'istanza viene arrestata e riavviata o ibernata e avviata, e viene rilasciato quando l'istanza viene terminata.

Indirizzi IPv4 pubblici

Un indirizzo IP pubblico è un indirizzo IPv4 raggiungibile tramite Internet. Puoi utilizzare gli indirizzi pubblici per la comunicazione tra le istanze e Internet.

Quando avvii un'istanza in un VPC predefinito, viene assegnato un indirizzo IP pubblico per impostazione predefinita. Quando avvii un'istanza in un VPC non predefinito, la sottorete ha un attributo che determina se le istanze avviate in quella sottorete ricevono un indirizzo IP pubblico dal pool di indirizzi IPv4 pubblici. Per impostazione predefinita, alle istanze avviate in una sottorete non predefinita non vengono assegnati indirizzi IP pubblici.

Puoi controllare se la tua istanza riceve un indirizzo IP pubblico come segue:

- Modificando l'attributo di indirizzamento IP pubblico della sottorete. Per ulteriori informazioni, consulta Modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici della sottorete nella Guida per l'utente di Amazon VPC.
- Abilitando o disabilitando la funzione di indirizzamento IP pubblico durante l'avvio, funzione che sostituisce l'attributo di indirizzamento IP pubblico della sottorete. Per ulteriori informazioni, consulta Assegnare un indirizzo IPv4 pubblico durante l'avvio dell'istanza.
- Puoi annullare l'assegnazione di un indirizzo IP pubblico alla tua istanza dopo l'avvio gestendo gli indirizzi IP associati a un'interfaccia di rete.

Un indirizzo IP pubblico viene assegnato alla tua istanza dal pool di indirizzi IPv4 pubblici di Amazon e non è associato al tuo account. AWS Quando un indirizzo IP pubblico viene disassociato dalla tua istanza, viene reinserito nel pool di indirizzi IPv4 pubblici e non potrai riutilizzarlo.

In alcuni casi, rilasciamo l'indirizzo IP pubblico dalla tua istanza o gliene assegniamo uno nuovo:

- Rilasciamo l'indirizzo IP pubblico dell'istanza quando viene arrestata, ibernata o terminata. L'istanza arrestata o ibernata riceve un nuovo indirizzo IP pubblico all'avvio.
- L'indirizzo IP pubblico dell'istanza viene rilasciato quando associ un indirizzo IP elastico alla tua istanza. Quando disassoci l'indirizzo IP elastico dall'istanza, questa riceve un nuovo indirizzo IP pubblico.
- Se è stato rilasciato l'indirizzo IP pubblico dell'istanza in un VPC, l'istanza non ne riceverà uno nuovo se è collegata a più di una interfaccia di rete.
- Se l'indirizzo IP pubblico dell'istanza viene rilasciato quando l'istanza ha un indirizzo IP privato secondario associato a un indirizzo IP elastico, l'istanza non riceve un nuovo indirizzo IP pubblico.

Se ti occorre un indirizzo IP pubblico persistente che puoi associare o dissociare in base alle tue esigenze, utilizza un indirizzo IP elastico.

Se utilizzi il DNS dinamico per mappare un nome DNS esistente a un indirizzo IP pubblico di una nuova istanza, potrebbero essere necessarie fino a 24 ore affinché l'indirizzo IP venga propagato in Internet. Come risultato, le nuove istanze potrebbero non ricevere traffico e quelle terminate continuerebbero a ricevere richieste. Per risolvere questo problema, utilizza un indirizzo IP elastico. Puoi allocare un tuo indirizzo IP elastico e associarlo all'istanza in uso. Per ulteriori informazioni, consulta Indirizzi IP elastici.

> **Note**
>
> - AWS costi per tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.
> - Alle istanze che accedono ad altre istanze tramite l'indirizzo IP NAT pubblico vengono addebitati i costi per il trasferimento di dati Internet o regionali, a seconda che le istanze si trovino nella stessa regione o meno.

Ottimizzazione degli indirizzi IPv4 pubblici

AWS costi per tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.

L'elenco seguente contiene le azioni che è possibile intraprendere per ottimizzare il numero di indirizzi IPv4 pubblici utilizzati:

- Utilizza un sistema di bilanciamento del carico elastico per bilanciare il carico del traffico verso le tue istanze EC2 e disabilita l'assegnazione automatica dell'IP pubblico sull'ENI principale assegnato alle istanze. I sistemi di bilanciamento del carico utilizzano un unico indirizzo IPv4 pubblico, in modo da ridurre il numero di indirizzi IPv4 pubblici. Potresti anche voler consolidare i sistemi di bilanciamento del carico esistenti per ridurre ulteriormente il numero di indirizzi IPv4 pubblici.
- Se l'unico motivo per utilizzare un gateway NAT è accedere tramite SSH a un'istanza EC2 in una sottorete privata per manutenzione o emergenze, prendi in considerazione l'utilizzo di EC2

Instance Connect Endpoint. Con EC2 Instance Connect Endpoint, puoi connetterti a un'istanza da Internet senza richiedere che l'istanza abbia un indirizzo IPv4 pubblico.

- Se le istanze EC2 si trovano in una sottorete pubblica a cui sono assegnati indirizzi IP pubblici, valuta la possibilità di spostare le istanze in una sottorete privata, di rimuovere gli indirizzi IP pubblici e di utilizzare un gateway NAT pubblico per consentire l'accesso da e verso le istanze EC2. Esistono considerazioni relative ai costi per l'utilizzo dei gateway NAT. Utilizzate questo metodo di calcolo per decidere se i gateway NAT sono convenienti. È possibile ottenere i dati `Number of public IPv4 addresses` necessari per questo calcolo creando un rapporto sui costi di AWS fatturazione e sull'utilizzo.

```
NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing
 public IP cost
```

  Dove:

  - `NAT gateway per hour = $0.045 * 730 hours in a month * Number of Availability Zones the NAT gateways are in`
  - `NAT gateway public IPs = $0.005 * 730 hours in a month * Number of IPs associated with your NAT gateways`
  - `NAT gateway transfer = $0.045 * Number of GBs that will go through the NAT gateway in a month`
  - `Existing public IP cost = $0.005 * 730 hours in a month * Number of public IPv4 addresses`

  Se il totale è inferiore a 1, i gateway NAT sono più economici degli indirizzi IPv4 pubblici.
- Utilizzali AWS PrivateLinkper connetterti privatamente a AWS servizi o servizi ospitati da altri AWS account anziché utilizzare indirizzi IPv4 pubblici e gateway Internet.
- Porta il tuo intervallo di indirizzi IP (BYOIP) AWS e utilizza l'intervallo per gli indirizzi IPv4 pubblici anziché utilizzare gli indirizzi IPv4 pubblici di proprietà di Amazon.
- Disattiva l'assegnazione automatica dell'indirizzo IPv4 pubblico per le istanze avviate nelle sottoreti. Questa opzione è generalmente disabilitata per impostazione predefinita per i VPC quando crei una sottorete, ma dovresti controllare le sottoreti esistenti per assicurarti che sia disabilitata.
- Se disponi di istanze EC2 che non richiedono indirizzi IPv4 pubblici, verifica che l'assegnazione automatica degli IP pubblici sia disattivata sulle interfacce di rete collegate alle istanze.
- Configura gli endpoint di accelerazione AWS Global Accelerator per le istanze EC2 in sottoreti private per consentire al traffico Internet di fluire direttamente verso gli endpoint nei tuoi VPC

senza richiedere indirizzi IP pubblici. Puoi anche trasferire i tuoi indirizzi AWS Global Accelerator e utilizzare i tuoi indirizzi IPv4 per gli indirizzi IP statici dell'acceleratore.

Indirizzi IP elastici (IPv4)

Un indirizzo IP elastico è un indirizzo IPv4 pubblico che puoi allocare nel tuo account. Puoi associarlo e dissociarlo dalle istanze in base alle esigenze. Viene assegnato al tuo account fino a quando non scegli di rilasciarlo. Per ulteriori informazioni sugli indirizzi IP elastici e su come utilizzarli, consulta Indirizzi IP elastici.

IPv6 non supporta gli indirizzi IP elastici.

Indirizzi IPv6

È possibile scegliere di associare un blocco CIDR IPv6 al tuo VPC e di associare blocchi CIDR IPv6 alle proprie sottoreti. Il blocco CIDR IPv6 per il VPC è assegnato automaticamente dal pool di indirizzi IPv6 di Amazon; non è possibile scegliere da soli l'intervallo. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di Amazon VPC:

- Indirizzi IP per VPC e sottoreti
- Aggiunta di un blocco CIDR IPv6 a un VPC
- Aggiunta di un blocco CIDR IPv6 a una sottorete

Gli indirizzi IPv6 sono univoci a livello globale, e possono essere configurati per rimanere privati o essere raggiungibili via Internet. L'istanza riceve un indirizzo IPv6 se al VPC e alla sottorete è associato un blocco CIDR IPv6 e se una delle seguenti condizioni è vera:

- La tua sottorete è configurata per assegnare automaticamente un indirizzo IPv6 a un'istanza durante l'avvio. Per ulteriori informazioni, consulta la sezione Modifica dell'attributo di assegnazione degli indirizzi IPv6 della sottorete.
- Assegni un indirizzo IPv6 alla tua istanza durante l'avvio.
- Assegni un indirizzo IPv6 all'interfaccia di rete primaria dell'istanza dopo l'avvio.
- Assegni un indirizzo IPv6 a un'interfaccia di rete nella stessa sottorete e colleghi l'interfaccia di rete all'istanza dopo l'avvio.

Quando l'istanza riceve un indirizzo IPv6 durante l'avvio, l'indirizzo viene associato all'interfaccia di rete primaria (eth0) dell'istanza. Puoi gestire gli indirizzi IPv6 per l'interfaccia di rete primaria (eth0) delle istanze nei seguenti modi:

- Assegna o annulla l'assegnazione di indirizzi IPv6 dall'interfaccia di rete. Il numero di indirizzi IPv6 che puoi assegnare a un'interfaccia di rete e il numero di interfacce di rete collegabili a un'istanza variano a seconda del tipo di istanza. Per ulteriori informazioni, consulta Indirizzi IP per interfaccia di rete per tipo di istanza.
- Abilita un indirizzo IPv6 primario. Un indirizzo IPv6 primario ti consente di evitare l'interruzione del traffico verso istanze o ENI. Per ulteriori informazioni, consulta Creazione di un'interfaccia di rete o Gestire gli indirizzi IP.

Un indirizzo IPv6 persiste quando arresti e avvii o iberni e avvii un'istanza e viene rilasciato quando la termini. Non è possibile riassegnare un indirizzo IPv6 mentre è già assegnato a un'altra interfaccia di rete: devi prima annullare l'assegnazione.

Puoi verificare se le istanze sono raggiungibili tramite i loro indirizzi IPv6 controllando il routing della sottorete o tramite le regole del gruppo di sicurezza e della lista di controllo accessi di rete. Per ulteriori informazioni, consulta Riservatezza del traffico Internet nella Guida per l'utente di Amazon VPC.

Per ulteriori informazioni sugli intervalli di indirizzi IPv6 riservati, consulta Registro degli indirizzi a scopi speciali IPv6 IANA e RFC4291.

Utilizzo degli indirizzi IPv4 per le istanze

È possibile assegnare un indirizzo IPv4 pubblico all'istanza al momento dell'avvio. È possibile visualizzare gli indirizzi IPv4 per l'istanza nella console tramite la pagina Instances (Istanze) o Network Interfaces (Interfacce di rete).

Indice

Visualizzare gli indirizzi IPv4

Puoi utilizzare la console Amazon EC2 per visualizzare gli indirizzi IPv4 pubblici e privati delle tue istanze. Puoi anche determinare gli indirizzi IPv4 privati e pubblici dall'interno dell'istanza utilizzandone i metadati. Per ulteriori informazioni, consulta Utilizzo dei metadati delle istanze.

L'indirizzo IPv4 pubblico viene mostrato come proprietà dell'interfaccia di rete nella console, ma è mappato sull'indirizzo IPv4 privato primario tramite NAT. Perciò, se ispezioni le proprietà dell'interfaccia di rete dell'istanza, ad esempio, tramite `ifconfig` (Linux) o `ipconfig` (Windows), l'indirizzo IPv4 pubblico non viene mostrato. Per determinare l'indirizzo IPv4 pubblico dell'istanza da un'istanza, utilizzare i metadati dell'istanza.

Per visualizzare gli indirizzi IPv4 di un'istanza utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell).

Per determinare gli indirizzi IPv4 pubblici dell'istanza tramite i suoi metadati

1. Connettiti alla tua istanza. Per ulteriori informazioni, consulta Connect alla tua istanza EC2.
2. Utilizzate il seguente comando per accedere all'indirizzo IP privato.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/local-ipv4
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
   ```

3. Utilizzare il comando seguente per accedere all'indirizzo IP pubblico. Se un indirizzo IP elastico è associato all'istanza, il valore restituito è quello dell'indirizzo IP elastico.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/public-ipv4
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-ipv4
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
   ```

Assegnare un indirizzo IPv4 pubblico durante l'avvio dell'istanza

Ogni sottorete ha un attributo che determina se alle istanze in essa avviate viene assegnato un indirizzo IP pubblico. Per impostazione predefinita, le sottoreti non predefinite hanno questo attributo impostato su false, mentre le sottoreti predefinite lo hanno impostato su true. Quando avvii un'istanza, hai anche a disposizione una funzione di indirizzamento IPv4 pubblico per controllare se all'istanza è stato assegnato un indirizzo IPv4 pubblico; è possibile sostituire il comportamento predefinito dell'attributo di indirizzamento IP della sottorete. L'indirizzo IPv4 pubblico viene assegnato dal pool di Amazon degli indirizzi IPv4 pubblici e viene assegnato all'interfaccia di rete con indice di dispositivo pari a eth0. Questa funzione dipende da alcune condizioni al momento dell'avvio dell'istanza.

Considerazioni

- È possibile annullare l'assegnazione dell'indirizzo IP pubblico all'istanza dopo l'avvio gestendo gli indirizzi IP associati a un'interfaccia di rete. Per ulteriori informazioni sugli indirizzi IPv4 pubblici, consulta Indirizzi IPv4 pubblici.
- Non è possibile assegnare automaticamente un indirizzo IP pubblico se specifichi più di un'interfaccia di rete. Inoltre, non è possibile sostituire l'impostazione della sottorete utilizzando la

funzione di assegnamento automatico dell'IP pubblico se specifichi un'interfaccia di rete esistente per eth0.

- Indipendentemente dal fatto che assegni o meno un indirizzo IP pubblico alla tua istanza durante l'avvio, puoi associare un indirizzo IP elastico all'istanza dopo l'avvio. Per ulteriori informazioni, consulta Indirizzi IP elastici. Puoi anche modificare il comportamento di indirizzamento IPv4 pubblico della sottorete. Per ulteriori informazioni, consulta Modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici della sottorete.

Assegnazione di un indirizzo IPv4 pubblico durante l'avvio dell'istanza utilizzando la console

Segui la procedura per avviare un'istanza e quando configuri Network Settings (Impostazioni di rete), scegli l'opzione Auto-assign Public IP (Assegna automaticamente un IP pubblico).

Per abilitare o disabilitare la funzione di indirizzamento di IP pubblici tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- Utilizzare le opzioni `--associate-public-ip-address` o `--no-associate-public-ip-address` con il comando run-instances (AWS CLI)
- Utilizzate il `-AssociatePublicIp` parametro con il New-EC2Instancecomando ()AWS Tools for Windows PowerShell

Utilizzo degli indirizzi IPv6 per le istanze

È possibile visualizzare gli indirizzi IPv6 assegnati all'istanza, assegnare un indirizzo IPv6 pubblico all'istanza o annullare l'assegnazione di un indirizzo IPv6 dall'istanza. È possibile visualizzare questi indirizzi nella console tramite la pagina Instances (Istanze) o Network Interfaces (Interfacce di rete).

Indice

Visualizzare gli indirizzi IPv6

Puoi utilizzare la console Amazon EC2 e i metadati dell'istanza per visualizzare gli indirizzi IPv6 delle tue istanze. AWS CLI

Per visualizzare gli indirizzi IPv6 di un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Nella scheda Networking (Reti) individuare gli IPv6 addresses (Indirizzi IPv6).

Per visualizzare gli indirizzi IPv6 di un'istanza utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell).

Per visualizzare gli indirizzi IPv6 per un'istanza utilizzando i metadati dell'istanza

1. Connettiti alla tua istanza. Per ulteriori informazioni, consulta Connect alla tua istanza EC2.
2. Ottieni l'indirizzo MAC dell'istanza da. `http://169.254.169.254/latest/meta-data/network/interfaces/macs/`
3. Utilizzate il seguente comando per visualizzare l'indirizzo IPv6.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/network/interfaces/macs/mac-address/ipv6s
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
   macs/mac-address/ipv6s
   ```

Tools for Windows PowerShell

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/network/
interfaces/macs/mac-address/ipv6s
```

Assegnazione di un indirizzo IPv6 a un'istanza

Se il VPC e la sottorete hanno blocchi CIDR IPv6 a loro associati, puoi assegnare all'istanza un indirizzo IPv6 durante o dopo l'avvio. L'indirizzo IPv6 viene assegnato dall'intervallo di indirizzi IPv6 della sottorete e viene assegnato all'interfaccia di rete con indice di dispositivo pari a eth0.

Assegnazione di un indirizzo IPv6 durante l'avvio dell'istanza

Segui la procedura per avviare un'istanza e quando configuri Network Settings (Impostazioni di rete), scegli l'opzione Auto-assign IPv6 IP (Assegna automaticamente un IP IPv6).

Assegnazione di un indirizzo IPv6 dopo l'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare l'istanza e scegliere Actions (Operazioni), Networking (Reti), Manage IP addresses (Gestisci indirizzi IP).
4. Espandere l'interfaccia di rete. In IPv6 Addresses (Indirizzi IPv6) selezionare Assign new IP address (Assegna nuovo indirizzo IP). Inserire un indirizzo IPv6 dall'intervallo della sottorete o lasciare vuoto il campo per consentire ad Amazon di scegliere un indirizzo IPv6 per conto dell'utente.
5. Selezionare Salva.

Per assegnare un indirizzo IPv6 utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- Utilizzare l'opzione `--ipv6-addresses` con il comando run-instances. (AWS CLI)
- Utilizzate la `Ipv6Addresses` proprietà for `-NetworkInterface` nel New-EC2Instancecomando ()AWS Tools for Windows PowerShell

- assign-ipv6-addresses (AWS CLI)
- Register-EC2IpvAddressList(6AWS Tools for Windows PowerShell)

Annullare l'assegnazione di un indirizzo IPv6 a un'istanza

È possibile annullare l'assegnazione di un indirizzo IPv6 da un'istanza in qualsiasi momento.

Annullamento dell'assegnazione di un indirizzo IPv6 a un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare l'istanza e scegliere Actions (Operazioni), Networking (Reti), Manage IP addresses (Gestisci indirizzi IP).
4. Espandere l'interfaccia di rete. In IPv6 Addresses (Indirizzi IPv6), selezionare Unassign (Annulla l'assegnazione) accanto all'indirizzo IPv6.
5. Selezionare Salva.

Puoi annullare l'assegnazione di un indirizzo IPv6 a un'istanza utilizzando la riga di comando.

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- unassign-ipv6-addresses (AWS CLI)
- Unregister-EC2IpvAddressList(6AWS Tools for Windows PowerShell).

Indirizzi IP multipli per le tue istanze EC2

È possibile specificare più indirizzi IPv4 e IPv6 privati per le tue istanze. Il numero di interfacce di rete e di indirizzi IPv4 e IPv6 privati che si possono specificare per un'istanza dipende dal tipo di istanza. Per ulteriori informazioni, consulta Indirizzi IP per interfaccia di rete per tipo di istanza.

Può essere utile assegnare più indirizzi IP a un'istanza nel VPC per eseguire le seguenti operazioni:

- Ospitare più siti Web su un solo server utilizzando più certificati SSL su un unico server e associando ciascun certificato a un indirizzo IP specifico.
- Gestire appliance di rete, come firewall o load balancer, che hanno più indirizzi IP per ogni interfaccia di rete.

- Reindirizzare il traffico interno verso un'istanza in standby in caso di esito negativo dell'istanza riassegnando l'indirizzo IP secondario all'istanza in standby.

Indice

Funzionamento degli indirizzi IP multipli

Il seguente elenco spiega come funzionano gli indirizzi IP multipli con le interfacce di rete:

- Puoi assegnare un indirizzo IPv4 privato secondario a qualsiasi interfaccia di rete.
- Puoi assegnare più indirizzi IPv6 a un'interfaccia di rete che si trova in una sottorete a cui è associato un blocco CIDR IPv6.
- Devi scegliere l'indirizzo IPv4 secondario dall'intervallo del blocco CIDR IPv4 della sottorete dell'interfaccia di rete.
- Devi scegliere gli indirizzi IPv6 dall'intervallo del blocco CIDR IPv6 della sottorete dell'interfaccia di rete.
- È possibile associare i gruppi di sicurezza con le interfacce di rete e non ai singoli indirizzi IP. Pertanto, ogni indirizzo IP specificato in un'interfaccia di rete è soggetto al gruppo di sicurezza dell'interfaccia di rete.
- Gli indirizzi IP multipli possono essere assegnati e tolti alle interfacce di rete collegate a istanze in esecuzione o arrestate.
- Gli indirizzi IPv4 privati secondari assegnati a un'interfaccia di rete possono essere riassegnati a un'altra interfaccia se lo consenti in modo esplicito.
- Un indirizzo IPv6 non può essere riassegnato a un'altra interfaccia di rete; devi prima annullare l'assegnazione dell'indirizzo IPv6 dall'interfaccia di rete esistente.
- Se assegni più indirizzi IP a un'interfaccia di rete utilizzando gli strumenti a riga di comando o l'API, l'intera operazione non va a buon fine se uno degli indirizzi IP non può essere assegnato.
- Gli indirizzi IPv4 privati primari e secondari, gli indirizzi IP elastici e gli indirizzi IPv6 rimangono con l'interfaccia di rete quando l'interfaccia di rete secondaria quando viene scollegata da un'istanza o è collegata a un'istanza.

- Anche se non puoi scollegare l'interfaccia di rete primaria da un'istanza, puoi riassegnare l'indirizzo IPv4 privato secondario dell'interfaccia di rete primaria a un'altra interfaccia di rete.

Il seguente elenco spiega come funzionano gli indirizzi IP multipli con gli indirizzi IP elastici (solo IPv4):

- Ogni indirizzo IPv4 privato può essere associato a un solo indirizzo IP elastico e viceversa.
- Quando un indirizzo IPv4 privato secondario viene riassegnato a un'altra interfaccia, mantiene la sua associazione con un indirizzo IP elastico.
- Quando viene annullata l'assegnazione a un'interfaccia di un indirizzo IPv4 privato secondario, viene automaticamente dissociato l'indirizzo IP elastico associato all'indirizzo IPv4 privato secondario.

Utilizzo di più indirizzi IPv4

Puoi assegnare a un'istanza un indirizzo IPv4 privato secondario, associare un indirizzo IPv4 elastico a un indirizzo IPv4 privato e annullare l'assegnazione di un indirizzo IPv4 privato secondario.

Attività

- Assegnazione di un indirizzo IPv4 privato secondario
- Configurare il sistema operativo per riconoscere gli indirizzi IPv4 privati secondari
- Associazione di un indirizzo IP elastico all'indirizzo IPv4 privato secondario
- Visualizzazione di indirizzi IPv4 privati secondari
- Annullare l'assegnazione di un indirizzo IPv4 privato secondario

Assegnazione di un indirizzo IPv4 privato secondario

Puoi assegnare l'indirizzo IPv4 privato secondario all'interfaccia di rete per un'istanza quando la avvii o quando è in esecuzione.

Per assegnare un indirizzo IPv4 privato secondario quando avvii un'istanza

1. Segui la procedura per avviare un'istanza. Per Impostazioni di rete, scegli Modifica.
2. Seleziona un VPC e una sottorete.
3. Expand Configurazione di rete avanzata.

4. Per IP secondario, scegli Assegna automaticamente e inserisci il numero di indirizzi IP (Amazon assegna automaticamente gli indirizzi IPv4 secondari) oppure scegli Assegna e inserisci manualmente gli indirizzi IPv4.
5. Completa i passaggi restanti per avviare l'istanza.

Per assegnare un indirizzo IPv4 secondario durante l'avvio utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- L'opzione `--secondary-private-ip-addresses` con il comando run-instances (AWS CLI)
- Definite `-NetworkInterface` e specificate il parametro con il `PrivateIpAddresses` comando (). New-EC2InstanceAWS Tools for Windows PowerShell

Per assegnare un indirizzo IPv4 privato secondario a un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Interfacce di rete, quindi seleziona l'interfaccia di rete per l'istanza.
3. Scegliere Actions (Operazioni), Manage IP Addresses (Gestisci indirizzi IP).
4. Espandere l'interfaccia di rete. In Indirizzi IPv4, scegli Assegna nuovo indirizzo IP.
5. Inserisci un indirizzo IPv4 specifico all'interno dell'intervallo di sottorete dell'istanza o lascia il campo vuoto per consentire ad Amazon di selezionare un indirizzo IPv4 per te.
6. (Facoltativo) Seleziona Consenti per consentire la riassegnazione dell'indirizzo IP privato secondario se è già assegnato a un'altra interfaccia di rete.
7. Selezionare Salva.

In alternativa puoi assegnare un indirizzo IPv4 privato secondario a un'istanza. Seleziona Istanze nel riquadro di navigazione, seleziona l'istanza, quindi Operazioni, Reti, Gestisci indirizzi IP. Puoi configurare le stesse informazioni come nei passaggi sopraindicati. L'indirizzo IP viene assegnato all'interfaccia di rete primaria (eth0) dell'istanza.

Per assegnare un indirizzo IPv4 privato secondario a un'istanza esistente utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- assign-private-ip-addresses (AWS CLI)
- Register-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Configurare il sistema operativo per riconoscere gli indirizzi IPv4 privati secondari

Dopo che hai assegnato un indirizzo IPv4 privato secondario a un'istanza, devi configurare il sistema operativo dell'istanza per riconoscere l'indirizzo IP privato secondario.

Istanze Linux

- Se utilizzi Amazon Linux, il pacchetto ec2-net-utils può occuparsi di questo passaggio al posto tuo. Configura altre interfacce di rete da collegare mentre l'istanza è in esecuzione, aggiorna gli indirizzi IPv4 secondari durante il rinnovo della locazione DHCP e le relative regole di routing. È possibile aggiornare immediatamente l'elenco delle interfacce utilizzando il comando `sudo service network restart` e quindi visualizzare l'elenco utilizzando. up-to-date `ip addr li` Se preferisci il controllo manuale della configurazione di rete, puoi rimuovere il pacchetto ec2-net-utils. Per ulteriori informazioni, consulta Configurazione dell'interfaccia di rete tramite ec2-net-utils per Amazon Linux 2.
- Se utilizzi un'altra distribuzione Linux, consulta la relativa documentazione. Cerca le informazioni sulla configurazione di altre interfacce di rete e di indirizzi IPv4 secondari. Se l'istanza ha due o più interfacce nella stessa sottorete, cerca le informazioni sull'utilizzo delle regole di routing per risolvere il routing asimmetrico.

Istanze Windows

Per ulteriori informazioni, consulta Configurazione di un indirizzo IPv4 privato secondario per l'istanza Windows.

Associazione di un indirizzo IP elastico all'indirizzo IPv4 privato secondario

Per associare un indirizzo IP elastico a un indirizzo IPv4 privato secondario

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Seleziona la casella di controllo per l'indirizzo IP elastico
4. Scegli Azioni, Associa indirizzo IP elastico.
5. Per Tipo di risorsa, scegli Interfaccia di rete. Seleziona l'interfaccia di rete, quindi seleziona l'indirizzo IP secondario dall'elenco degli indirizzi IP privati.
6. Per Interfaccia di rete, seleziona l'interfaccia di rete. Seleziona l'indirizzo IP secondario dall'elenco degli indirizzi IP privati.
7. Per Indirizzo IP privato, selezionare l'indirizzo IP secondario.
8. Selezionare Associate (Associa).

Per associare un indirizzo IP elastico a un indirizzo IPv4 privato secondario utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Visualizzazione di indirizzi IPv4 privati secondari

Per visualizzare gli indirizzi IPv4 privati assegnati a un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo per l'interfaccia di rete.
4. Nella scheda Dettagli, in Indirizzi IP, individua Indirizzo IPv4 privato e Indirizzi IPv4 privati secondari.

Per visualizzare gli indirizzi IPv4 privati assegnati a un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona la casella per l'istanza.

4. Nella scheda Rete, in Dettagli di rete, individua gli indirizzi IPv4 privati e gli indirizzi IPv4 privati secondari.

Annullare l'assegnazione di un indirizzo IPv4 privato secondario

Se non è più necessario un indirizzo IPv4 privato secondario, puoi annullarne l'assegnazione dall'istanza o dall'interfaccia di rete. Quando viene annullata l'assegnazione di un indirizzo IPv4 privato secondario a un'interfaccia di rete, viene dissociato anche l'indirizzo IP elastico (se presente).

Per annullare l'assegnazione a un'istanza di un indirizzo IPv4 privato secondario

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona un'istanza, scegli Operazioni, Reti, Gestisci indirizzi IP.
4. Espandere l'interfaccia di rete. Per gli indirizzi IPv4, scegli Annulla assegnazione per annullare l'assegnazione dell'indirizzo IPv4.
5. Selezionare Salva.

Per annullare l'assegnazione a un'interfaccia di rete di un indirizzo IPv4 privato secondario

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Seleziona l'interfaccia di rete, scegli Azioni, Gestisci indirizzi IP.
4. Espandere l'interfaccia di rete. Per gli indirizzi IPv4, scegli Annulla assegnazione per annullare l'assegnazione dell'indirizzo IPv4.
5. Selezionare Salva.

Per annullare l'assegnazione di un indirizzo IPv4 utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- unassign-private-ip-addresses (AWS CLI)
- Unregister-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Utilizzo di più indirizzi IPv6

Puoi assegnare più indirizzi IPv6 a un'istanza, visualizzare gli indirizzi IPv6 assegnati all'istanza e annullare l'assegnazione di indirizzi IPv6.

Indice

Assegnazione di più indirizzi IPv6

Puoi assegnare uno o più indirizzi IPv6 a un'istanza durante o dopo l'avvio. Per assegnare a un'istanza un indirizzo IPv6, il VPC e la sottorete in cui avvii l'istanza devono avere un blocco CIDR IPv6 associato.

Per assegnare più indirizzi IPv6 durante l'avvio

1. Segui la procedura per avviare un'istanza. Per Impostazioni di rete, scegli Modifica.
2. Seleziona un VPC e una sottorete.
3. Expand Configurazione di rete avanzata.
4. Per gli IP IPv6, scegli Assegna automaticamente e il numero di indirizzi IP (Amazon assegna automaticamente gli indirizzi IPv6) oppure scegli Assegna e inserisci manualmente gli indirizzi IPv6.
5. Completa i passaggi restanti per avviare l'istanza.

È possibile utilizzare la schermata Instances (Istanze) nella console Amazon EC2 per assegnare più indirizzi IPv6 a un'istanza esistente. In questo modo vengono assegnati gli indirizzi IPv6 all'interfaccia di rete primaria (eth0) dell'istanza. Per assegnare all'istanza un indirizzo IPv6 specifico, verifica che l'indirizzo IPv6 non sia stato già assegnato a un'altra istanza o interfaccia di rete.

Per assegnare più indirizzi IPv6 a un'istanza esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona la tua istanza, scegli Azioni, Rete, Gestisci indirizzi IP.

4. Espandere l'interfaccia di rete. Per gli indirizzi IPv6, scegli Assegna un nuovo indirizzo IP per ogni indirizzo IPv6 da aggiungere. Puoi specificare un indirizzo IPv6 dall'intervallo della sottorete o lasciare il campo vuoto per consentire ad Amazon di scegliere un indirizzo IPv6 per te.
5. Selezionare Salva.

In alternativa, puoi assegnare più indirizzi IPv6 a un'interfaccia di rete esistente. L'interfaccia di rete deve essere stata creata in una sottorete che ha un blocco CIDR IPv6 associato. Per assegnare all'interfaccia di rete un indirizzo IPv6 specifico, verifica che l'indirizzo IPv6 non sia stato già assegnato a un'altra interfaccia di rete.

Per assegnare più indirizzi IPv6 a un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Seleziona l'interfaccia di rete, scegli Azioni, Gestisci indirizzi IP.
4. Espandere l'interfaccia di rete. Per gli indirizzi IPv6, scegli Assegna un nuovo indirizzo IP per ogni indirizzo IPv6 da aggiungere. Puoi specificare un indirizzo IPv6 dall'intervallo della sottorete o lasciare il campo vuoto per consentire ad Amazon di scegliere un indirizzo IPv6 per te.
5. Selezionare Salva.

Panoramica di CLI

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- Assegnare un indirizzo IPv6 durante l'avvio:
  - Utilizzare le opzioni `--ipv6-addresses` o `--ipv6-address-count` con il comando run-instances (AWS CLI)
  - Definisci `-NetworkInterface` e specifica i `Ipv6AddressCount` parametri `Ipv6Addresses` o con il comando (). New-EC2InstanceAWS Tools for Windows PowerShell
- Assegnare un indirizzo IPv6 a un'interfaccia di rete:
  - assign-ipv6-addresses (AWS CLI)
  - Register-EC2IpvAddressList(6AWS Tools for Windows PowerShell)

Visualizzazione degli indirizzi IPv6

Puoi visualizzare gli indirizzi IPv6 di un'istanza o di un'interfaccia di rete.

Per visualizzare gli indirizzi IPv6 assegnati a un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona la casella di controllo relativa all'istanza.
4. Nella scheda Rete, individua il campo degli indirizzi IPv6.

Per visualizzare gli indirizzi IPv6 assegnati a un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Nella scheda Dettagli, in Indirizzi IP, individua il campo Indirizzi IPv6.

Panoramica di CLI

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- Visualizzare gli indirizzi IPv6 di un'istanza:
  - describe-instances (AWS CLI)
  - Get-EC2Instance (AWS Tools for Windows PowerShell).
- Visualizzare gli indirizzi IPv6 di un'interfaccia di rete:
  - describe-network-interfaces (AWS CLI)
  - Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Annullare l'assegnazione di un indirizzo IPv6

Puoi annullare l'assegnazione di un indirizzo IPv6 all'interfaccia di rete primaria di un'istanza o annullarne l'assegnazione a un'interfaccia di rete.

Per annullare l'assegnazione di un indirizzo IPv6 a un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona la casella di controllo relativa all'istanza, quindi scegli Azioni, Rete, Gestisci indirizzi IP.
4. Espandere l'interfaccia di rete. In IPv6 Addresses (Indirizzi IPv6), selezionare Unassign (Annulla l'assegnazione) accanto all'indirizzo IPv6.
5. Selezionare Salva.

Per annullare l'assegnazione di indirizzo IPv6 a un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete, quindi scegli Azioni, Gestisci indirizzi IP.
4. Espandere l'interfaccia di rete. In IPv6 Addresses (Indirizzi IPv6), selezionare Unassign (Annulla l'assegnazione) accanto all'indirizzo IPv6.
5. Selezionare Salva.

Panoramica di CLI

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- unassign-ipv6-addresses (AWS CLI)
- Unregister-EC2IpvAddressList(6AWS Tools for Windows PowerShell)

Configurazione di un indirizzo IPv4 privato secondario per l'istanza Windows

Puoi specificare più indirizzi IPv4 privati per le tue istanze. Dopo aver assegnato un indirizzo IPv4 privato secondario a un'istanza, devi configurare il sistema operativo dell'istanza per riconoscere l'indirizzo IPv4 privato secondario.

> **Note**
>
> Queste istruzioni si basano su Windows Server 2022. L'implementazione di questi passaggi può variare in base al sistema operativo dell'istanza di Windows.

Attività

Prerequisiti

1. Assegna l'indirizzo IPv4 privato secondario all'interfaccia di rete dell'istanza. Puoi assegnare l'indirizzo IPv4 privato secondario all'interfaccia di rete quando avvii l'istanza o quando è in esecuzione. Per ulteriori informazioni, consulta Assegnazione di un indirizzo IPv4 privato secondario.
2. Alloca un indirizzo IP elastico e associalo all'indirizzo IPv4 privato secondario. Per ulteriori informazioni, consulta Allocare un indirizzo IP elastico e Associazione di un indirizzo IP elastico all'indirizzo IPv4 privato secondario.

Passaggio 1: configura l'indirizzamento IP statico nella tua istanza

Per abilitare l'istanza Windows all'utilizzo di più indirizzi IP, devi configurare l'istanza per l'utilizzo degli indirizzi IP statici anziché di un server DHCP.

> **Important**
>
> Quando configuri l'indirizzo IP statico nella tua istanza, l'indirizzo IP deve corrispondere esattamente a quello mostrato nella console, nella CLI o nell'API. Se immetti questi indirizzi IP in modo errato, l'istanza potrebbe diventare irraggiungibile.

Per configurare gli indirizzi IP statici su un'istanza Windows

1. Connettiti alla tua istanza.
2. Cercare l'indirizzo IP, una subnet mask e gli indirizzi gateway di default per l'istanza eseguendo le fasi seguenti:

   - Esegui il seguente comando in PowerShell:

     ```
     ipconfig /all
     ```

     Esamina l'output e annota i valori dell'indirizzo IPv4, della subnet mask, del gateway predefinito e dei server DNS per l'interfaccia di rete. L'output dovrebbe essere simile al seguente esempio:

     ```
     ...

     Ethernet adapter Ethernet 4:

        Connection-specific DNS Suffix  . : us-west-2.compute.internal
        Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
        Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
        IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Lease Obtained. . . . . . . . . . : Monday, April 8, 2024 12:19:29 PM
        Lease Expires . . . . . . . . . . : Monday, April 8, 2024 4:49:30 PM
        Default Gateway . . . . . . . . . : 10.200.0.1
        DHCP Server . . . . . . . . . . . : 10.200.0.1
        DHCPv6 IAID . . . . . . . . . . . : 151166011
        DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
     E7
        DNS Servers . . . . . . . . . . . : 10.200.0.2
        NetBIOS over Tcpip. . . . . . . . : Enabled
     ```

3. Aprire il Centro connessioni di rete e condivisione eseguendo il seguente comando in PowerShell:

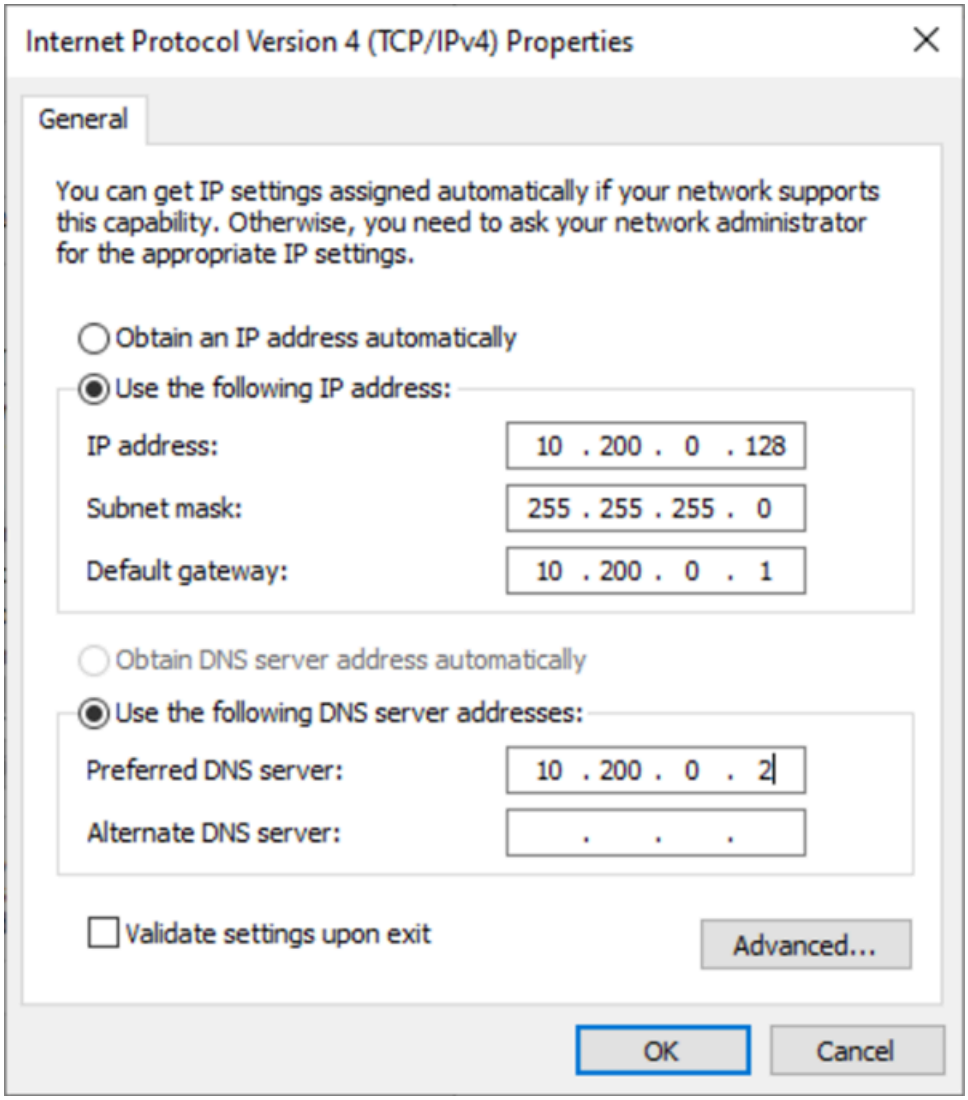
   ```
   & $env:SystemRoot\system32\control.exe ncpa.cpl
   ```

4. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per l'interfaccia di rete (Connessione alla rete locale o Ethernet) e scegli Proprietà.
5. Scegliere Internet Protocol Version 4 (TCP/IPv4), Properties (Proprietà).
6. Nella finestra di dialogo Internet Protocol Version 4 (TCP/IPv4) Properties (Internet Protocol Version 4 (TCP/IPv4) - Proprietà), scegliere Use the following IP address (Usa il seguente indirizzo IP), immettere i seguenti valori, quindi scegliere OK.

Campo	Valore
IP address (Indirizzo IP)	Indirizzo IPv4 annotato nella precedente fase 2.
Maschera sottorete	Subnet mask annotata nella precedente fase 2.
Default gateway (Gateway predefinito)	Indirizzo del gateway di default annotato nella precedente fase 2.
Preferred DNS server (Server DNS preferito)	Server DNS annotato nella precedente fase 2.
Alternate DNS server (Server DNS alternativo)	Server DNS alternativo annotato nella precedente fase 2. Se nell'output non è visualizzato alcun server DNS alternativo, lasciare vuoto questo campo.

Important

Se si imposta l'indirizzo IP su un qualsiasi valore diverso dall'indirizzo IP corrente, la connettività all'istanza andrà perduta.



Si perderà la connettività RDP all'istanza Windows per alcuni secondi mentre l'istanza viene convertita dall'uso di DHCP all'uso degli indirizzi statici. L'istanza conserva le stesse informazioni sugli indirizzi IP di prima, ma ora queste informazioni sono statiche e non sono gestite da DHCP.

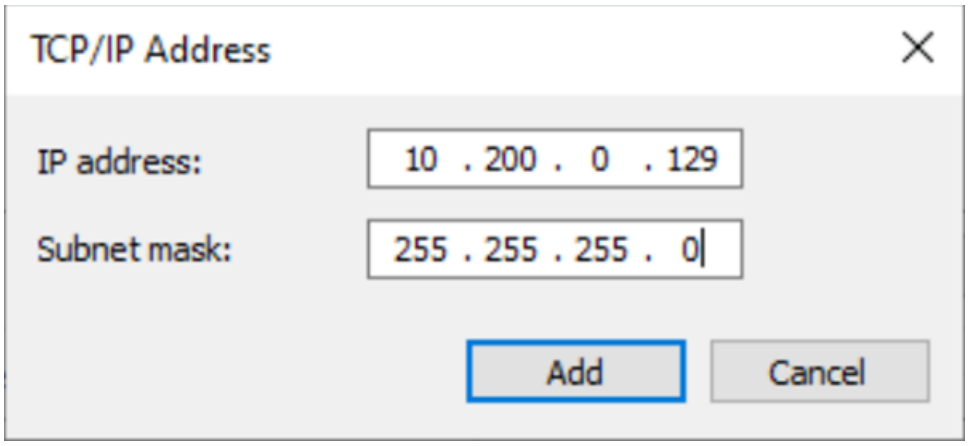
Fase 2: configurazione di un indirizzo IP privato secondario per l'istanza

Dopo aver configurato gli indirizzi IP statici sull'istanza Windows, prepara un indirizzo IP privato secondario.

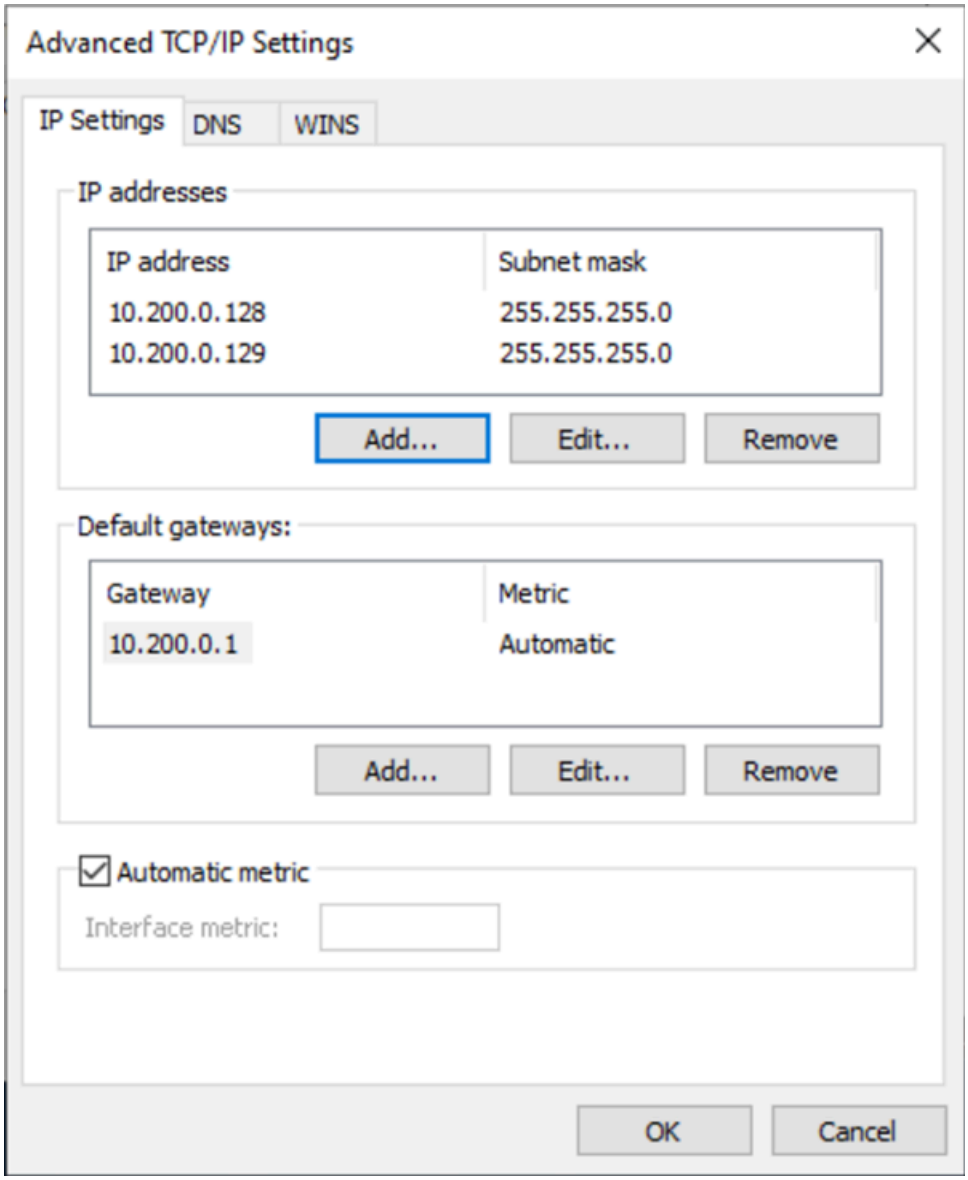
Per configurare un indirizzo IP secondario

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, selezionare Instances (Istanze) e selezionare l'istanza.
3. In Networking (Rete), prendere nota dell'indirizzo IP secondario.
4. Connettiti alla tua istanza.
5. Nell'istanza di Windows scegliere Start, Control Panel (Pannello di controllo).
6. Scegliere Network and Internet (Rete e Internet), Network and Sharing Center (Centro connessioni di rete e condivisione).
7. Seleziona l'interfaccia di rete (Connessione alla rete locale o Ethernet) e scegli Proprietà.
8. Nella pagina Local Area Connection Properties (Proprietà connessione alla rete locale) scegliere Internet Protocol Version 4 (TCP/IPv4), Properties (Proprietà), Advanced (Avanzate).
9. Scegliere Aggiungi.
10. Nella finestra di dialogo TCP/IP Address (Indirizzo TCP/IP), digitare l'indirizzo IP privato secondario in IP address (Indirizzo IP). Per Subnet mask (Maschera sottorete), immettere la stessa subnet mask specificata per l'indirizzo IP privato principale nella Passaggio 1: configura l'indirizzamento IP statico nella tua istanza, quindi scegliere Add (Aggiungi).



11. Verificare le impostazioni dell'indirizzo IP e scegliere OK.



12. Scegliere OK, Close (Chiudi).
13. Per confermare che l'indirizzo IP secondario è stato aggiunto al sistema operativo, esegui il `ipconfig /all` comando in PowerShell. L'output visualizzato dovrebbe essere simile al seguente:

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

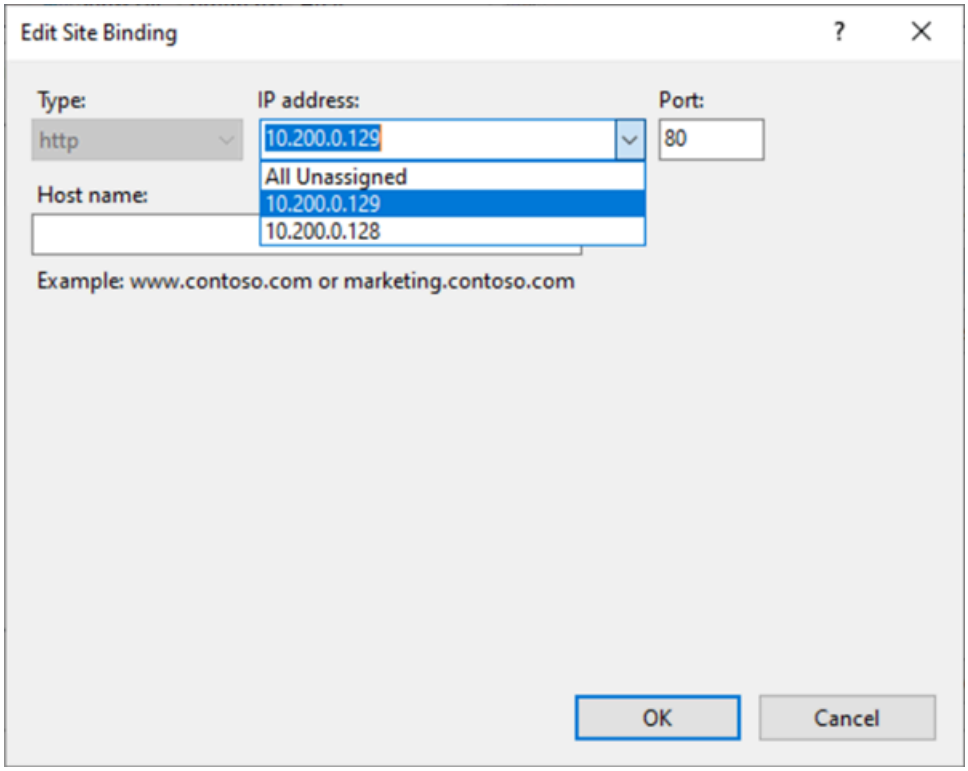
```
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.200.0.129(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Fase 3: configurazione delle applicazioni per l'utilizzo dell'indirizzo IP privato secondario

Puoi configurare qualsiasi applicazione per l'utilizzo dell'indirizzo IP privato secondario. Ad esempio, se l'istanza esegue un sito Web su IIS, puoi configurare IIS per l'uso dell'indirizzo IP privato secondario.

Per configurare IIS per l'utilizzo dell'indirizzo IP privato secondario

1. Connettiti alla tua istanza.
2. Aprire Internet Information Services (IIS) Manager (Gestione Internet Information Services [IIS]).
3. Nel riquadro Connections (Connessioni) espandere Sites (Siti).
4. Aprire il menu contestuale (pulsante destro del mouse) per il sito Web e scegliere Edit Bindings (Modifica binding).
5. Nella finestra di dialogo Site Bindings (Binding sito), per Type (Tipo) scegliere http, Edit (Modifica).
6. Nella finestra di dialogo Edit Site Binding (Modifica binding sito), selezionare l'indirizzo IP privato secondario in IP address (Indirizzo IP). Per impostazione di default, ogni sito Web accetta richieste HTTP da tutti gli indirizzi IP.



7. Scegliere OK, Close (Chiudi).

Nomi host per le istanze EC2

Quando crei un'istanza EC2, AWS crea un nome host per quell'istanza. Per ulteriori informazioni sui tipi di nomi host e su come vengono forniti, consulta. AWSTipi di nomi host delle istanze Amazon EC2 Amazon offre un server DNS che risolve i nomi host forniti da Amazon in indirizzi IPv4 e IPv6. Il server DNS Amazon si trova alla base dell'intervallo di rete VPC più due. Per ulteriori informazioni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC.

Indirizzi link local

Gli indirizzi link local sono indirizzi IP noti e non instradabili. Amazon EC2 utilizza gli indirizzi dello spazio degli indirizzi link local per fornire servizi accessibili solo da un'istanza EC2. Questi servizi non vengono eseguiti sull'istanza, ma sull'host sottostante. Quando accedi agli indirizzi link local per questi servizi, comunichi con l'hypervisor Xen o il controller Nitro.

Intervalli di indirizzi link local

- IPv4: 169.254.0.0/16 (da 169.254.0.0 a 169.254.255.255)
- IPv6: fe80::/10

Servizi a cui si accede utilizzando gli indirizzi link local

- Servizio di metadati dell'istanza
- Amazon Route 53 Resolver (noto anche come server Amazon DNS)
- Servizio di sincronizzazione oraria di Amazon

Tipi di nomi host delle istanze Amazon EC2

In questa sezione sono descritti i tipi di nomi host del sistema operativo guest delle istanze Amazon EC2 disponibili quando le istanze vengono avviate nelle sottoreti VPC.

Il nome host distingue le istanze EC2 sulla rete. Puoi utilizzare il nome host di un'istanza se, ad esempio, desideri eseguire script per comunicare con alcune o tutte le istanze della rete.

Indice

Tipi di nomi host per EC2

Esistono due tipi di nome host per il nome host del sistema operativo guest quando le istanze EC2 vengono avviate in un VPC:

- IP name (Nome IP): lo schema di denominazione legacy in cui, quando si avvia un'istanza, l'indirizzo IPv4 privato dell'istanza è incluso nel nome host dell'istanza. Il nome IP esiste per tutta la durata dell'istanza EC2. Se utilizzato come nome host DNS privato, restituirà solo l'indirizzo IPv4 privato (record A).
- Resource name (Nome risorsa): quando avvii un'istanza, il campo EC2 instance ID (ID istanza EC2) è incluso nel nome host dell'istanza. Il nome risorsa esiste per tutta la durata dell'istanza EC2. Se utilizzato come nome host DNS privato, può restituire sia l'indirizzo IPv4 privato (record A) sia l'indirizzo IPv6 Global Unicast (record AAAA).

Il nome host del sistema operativo guest dell'istanza EC2 dipende dalle impostazioni della sottorete:

- Se l'istanza viene avviata in una sottorete solo IPv4, puoi selezionare il nome IP o il nome risorsa.
- Se l'istanza viene avviata in una sottorete dual-stack (IPv4+IPv6), puoi selezionare il nome IP o il nome risorsa.
- Se l'istanza viene avviata in una sottorete solo IPv6, viene utilizzato automaticamente il nome risorsa.

Indice

Nome IP

Quando avvii un'istanza EC2 con Hostname type (Tipo di nome host) uguale a IP name (Nome IP), il nome host del sistema operativo guest è configurato per utilizzare l'indirizzo IPv4 privato.

- Formato per un'istanza in us-east-1: *private-ipv4-address*.ec2.internal
- Esempio: *ip-10-24-34-0*.ec2.internal
- Formato per un'istanza in qualsiasi altra AWS regione: *private-ipv4-address.region*.compute.internal
- Esempio: *ip-10-24-34-0.us-west-2*.compute.internal

Nome risorsa

Quando avvii istanze EC2 nelle sottoreti solo IPv6, Hostname type (Tipo di nome host) di Resource name (Nome risorsa) è selezionato per impostazione predefinita. Quando avvii un'istanza nelle sottoreti solo IPv4 o dual-stack (IPv4+IPv6), Resource name (Nome risorsa) è un'opzione che puoi selezionare. Dopo aver avviato un'istanza, puoi gestire la configurazione del nome host. Per ulteriori informazioni, consulta Modifica delle configurazioni del tipo di nome host e del nome host DNS.

Quando avvii un'istanza EC2 con Hostname type (Tipo di nome host) di Resource name (Nome risorsa), il nome host del sistema operativo guest è configurato per utilizzare l'ID dell'istanza EC2.

- Formato per un'istanza in us-east-1: *ec2-instance-id*.ec2.internal
- Esempio: *i-0123456789abcdef*.ec2.internal

- Formato per un'istanza in qualsiasi altra AWS regione: *ec2-instance-id.region*.compute.internal
- Esempio: *i-0123456789abcdef.us-west-2*.compute.internal

Differenza tra nome IP e nome risorsa

Le query DNS per i nomi IP e nomi risorsa coesistono per garantire la compatibilità con le versioni precedenti e consentire la migrazione dai nomi host basati su IP alla denominazione basata su risorse. Per i nomi host DNS privati basati su nomi IP, non è possibile configurare se una query di record DNS A per l'istanza riceve una risposta o meno. Le query del record DNS A ricevono sempre una risposta indipendentemente dalle impostazioni del nome host del sistema operativo guest. Al contrario, per i nomi host DNS privati basati sul nome risorsa, è possibile configurare se le query DNS A e/o DNS AAAA per l'istanza ricevono una risposta. È possibile configurare il comportamento della risposta quando si avvia un'istanza o si modifica una sottorete. Per ulteriori informazioni, consulta Modifica delle configurazioni del tipo di nome host e del nome host DNS.

Dove vengono visualizzati il nome risorsa e il nome IP

In questa sezione vengono descritti gli scenari in cui vengono visualizzati i tipi di nome host nome risorsa e nome IP nella console EC2.

Indice

Creazione di un'istanza EC2

Quando crei un'istanza EC2, a seconda del tipo di sottorete selezionato, l'opzione Hostname type (Tipo di nome host) di Resource name (Nome risorsa) potrebbe essere disponibile oppure potrebbe essere selezionata e non modificabile. In questa sezione vengono descritti gli scenari in cui vengono visualizzati i tipi di nome host nome risorsa e nome IP.

Scenario 1

Crea un'istanza EC2 nella procedura guidata (consulta la sezione Avvio di un'istanza tramite la procedura guidata di avvio istanza) e, quando configuri i dettagli, scegli una sottorete configurata solo per IPv6.

In questo caso, l'opzione Hostname type (Tipo di nome host) di Resource name (Nome risorsa) è selezionata automaticamente e non è modificabile. Le opzioni DNS Hostname (Nome host DNS) di Enable IP name IPv4 (A record) DNS requests (Abilita richieste DNS IPv4 [record A] basate sul nome IP) e di Enable resource-based IPv4 (A record) DNS requests (Abilita richieste DNS IPv4 [record A] basate sulle risorse) sono deselezionate automaticamente e non sono modificabili. L'opzione Enable resource-based IPv6 (AAAA record) DNS requests (Abilita richieste DNS IPv6 [record AAAA] basate sulle risorse) è selezionata di default ma è modificabile. Se l'opzione è selezionata, le richieste DNS al nome risorsa verranno risolte all'indirizzo IPv6 (record AAAA) di questa istanza EC2.

Scenario 2

Crea un'istanza EC2 nella procedura guidata (consulta la sezione Avvio di un'istanza tramite la procedura guidata di avvio istanza) e, quando configuri i dettagli, scegli una sottorete configurata con un blocco CIDR IPv4 o un blocco CIDR IPv4 e IPv6 ("dual stack").

L'opzione Enable IP name IPv4 (A record) DNS requests (Abilita richieste DNS IPv4 [record A] basate sul nome IP) è selezionata automaticamente e non può essere modificata. Ciò significa che le richieste al nome IP risolveranno l'indirizzo IPv4 (record A) di questa istanza EC2.

Le opzioni sono predefinite per le configurazioni della sottorete, ma puoi modificare le opzioni per l'istanza a seconda delle impostazioni della sottorete:

- Hostname type (Tipo di nome host): determina se desideri che il nome host del sistema operativo guest dell'istanza EC2 sia il nome risorsa o il nome IP. Il valore predefinito è IP name (Nome IP).
- Enable resource-based IPv4 (A record) DNS requests (Abilita richieste DNS IPv4 [record A] basate sulle risorse): determina se le richieste al nome risorsa vengono risolte con l'indirizzo IPv4 privato (record A) di questa istanza EC2. Questa opzione non è selezionata di default.
- Enable resource-based IPv6 (AAAA record) DNS requests (Abilita richieste DNS IPv6 [record AAAA] basate sulle risorse): determina se le richieste al nome risorsa vengono risolte con l'indirizzo GUA IPv6 (record AAAA) di questa istanza EC2. Questa opzione non è selezionata di default.

Quando si visualizzano i dettagli di un'istanza EC2 esistente

Puoi visualizzare i valori del nome host per un'istanza EC2 esistente nella scheda Details (Dettagli) dell'istanza EC2:

- Hostname type (Tipo di nome host): il nome host nel formato del nome IP o del nome risorsa.

- Private IP DNS name (IPv4 only) (Nome DNS IP privato [solo IPv4]): il nome IP che verrà sempre risolto all'indirizzo IPv4 privato dell'istanza.
- Private resource DNS name (Nome DNS risorsa privato): il nome risorsa che può essere risolto ai record DNS selezionati per l'istanza.
- Answer private resource DNS name (Rispondi al nome DNS delle risorse private): il nome risorsa risolve i record DNS IPv4 (A), IPv6 (AAAA) o IPv4 e IPv6 (A e AAAA).

Inoltre, se ti connetti all'istanza EC2 direttamente tramite SSH e inserisci il comando `hostname`, visualizzerai il nome host nel formato nome IP o nome risorsa.

Come stabilire se scegliere il nome risorsa o il nome IP

Quando avvii un'istanza EC2 (consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza), se scegli l'opzione Hostname type (Tipo di nome host) di Resource name (Nome risorsa), l'istanza EC2 viene avviata con un nome host nel formato del nome risorsa. In questi casi, anche il record DNS per l'istanza EC2 può indicare il nome risorsa. Ciò offre la flessibilità di scegliere se tale nome host si risolve all'indirizzo IPv4, all'indirizzo IPv6 o sia all'indirizzo IPv4 sia all'indirizzo IPv6 dell'istanza. Se prevedi di utilizzare IPv6 in futuro o se stai già utilizzando sottoreti dual-stack, è meglio usare l'opzione Hostname type (Tipo di nome host) di Resource name (Nome risorsa) in modo tale da modificare la risoluzione DNS per i nomi host delle istanze senza apportare modifiche ai record DNS stessi. Il nome risorsa consente di aggiungere e rimuovere la risoluzione DNS IPv4 e IPv6 su un'istanza EC2.

Se invece scegli un Hostname type (Tipo di nome host) di IP name (Nome IP) e lo utilizzi come nome host DNS, esso può risolvere solo all'indirizzo IPv4 dell'istanza. Non risolverà all'indirizzo IPv6 dell'istanza anche se all'istanza sono associati sia un indirizzo IPv4 sia un indirizzo IPv6.

Modifica delle configurazioni del tipo di nome host e del nome host DNS

Segui la procedura descritta in questa sezione per modificare le configurazioni del tipo di nome host e del nome host DNS per sottoreti o istanze EC2 dopo l'avvio.

Indice

Sottoreti

Modifica le configurazioni per una sottorete selezionando una sottorete nella console VPC e scegliendo Actions (Operazioni), quindi Edit subnet settings (Modifica impostazioni della sottorete).

> **Note**
>
> La modifica delle impostazioni della sottorete non modifica la configurazione delle istanze EC2 già avviate nella sottorete.

- Hostname type (Tipo di nome host): determina se desideri che l'impostazione di default del nome host del sistema operativo guest dell'istanza EC2 avviata nella sottorete sia il nome risorsa o il nome IP.
- Abilita richieste IPv4 (record a) del nome host DNS: determina se le richieste/query DNS per il nome della risorsa vengono risolte nell'indirizzo IPv4 privato (record A) di questa istanza EC2.
- Enable resource-based IPv6 (A record) DNS requests (Abilita richieste DNS IPv6 [A record]): determina se le richieste/query DNS per il nome della risorsa vengono risolte con l'indirizzo IPv6 privato (record A) di questa istanza EC2.

Istanze EC2

Segui le procedure descritte in questa sezione per modificare le configurazioni del tipo di nome host e del nome host DNS per un'istanza EC2.

> **Important**
>
> - Per modificare l'impostazione Use resource based naming as guest OS hostname (Usa denominazione basata sulle risorse come nome host del sistema operativo guest), prima devi arrestare l'istanza. Per modificare le impostazioni Answer DNS hostname IPv4 (A record) request (Risposta alla richiesta del nome host DNS IPv4 (record A) o Answer DNS hostname IPv6 (AAAA record) requests (Risposta alle richieste di nome host DNS IPv6 [record AAAA]), non è necessario arrestare l'istanza.
> - Per modificare una qualsiasi delle impostazioni per i tipi di istanza EC2 non supportati da EBS, non è possibile arrestare l'istanza. Devi terminare l'istanza e avviarne una nuova con le configurazioni del tipo di nome host e del nome host DNS desiderate.

Come modificare le configurazioni del tipo di nome host e del nome host DNS per un'istanza EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Se hai intenzione di modificare l'impostazione Use resource based naming as guest OS hostname (Usa denominazione basata sulle risorse come nome host del sistema operativo guest), prima devi arrestare l'istanza EC2. In caso contrario, puoi ignorare questo passaggio.

   Per arrestare l'istanza, selezionare l'istanza e scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).
3. Selezionare l'istanza, quindi scegliere Actions (Operazioni), Instance settings (Impostazioni dell'istanza), Change resource based naming options (Modifica delle opzioni di denominazione basate sulle risorse).

   - Use resource based naming as guest OS hostname (Usa denominazione basata sulle risorse come nome host del sistema operativo guest): determina se desideri che il nome host del sistema operativo guest dell'istanza EC2 sia il nome risorsa o il nome IP.
   - Rispondi a richieste IPv4 (record A) del nome host DNS: determina se le richieste/query DNS per il nome della risorsa vengono risolte nell'indirizzo IPv4 di questa istanza EC2.
   - Answer DNS hostname IPv6 (AAAA record) requests (Risposta alle richieste di nome host DNS IPv6 [record AAAA]): determina se le richieste/query DNS per il nome della risorsa vengono risolte con l'indirizzo IPv6 privato (record AAAA) di questa istanza EC2.
4. Selezionare Salva.
5. Dopo aver arrestato l'istanza, avviarla di nuovo.

Utilizzare gli indirizzi IP personali (BYOIP) in Amazon EC2

Puoi trasferire parte o tutto l'intervallo di indirizzi IPv4 o IPv6 instradabile pubblicamente dalla rete locale al tuo account. AWS Continui a controllare l'intervallo di indirizzi e puoi pubblicizzarlo su Internet tramite. AWS Dopo aver impostato l'intervallo di indirizzi su AWS, questo viene visualizzato nel tuo AWS account come pool di indirizzi.

Per un elenco di regioni in cui BYOIP è disponibile, consulta la pagina Disponibilità regionale.

Note

- I passaggi su questa pagina descrivono come portare il proprio intervallo di indirizzi IP da utilizzare solo in Amazon EC2.
- Per inserire il tuo intervallo di indirizzi IP da utilizzare AWS Global Accelerator, consulta Bring your own IP address (BYOIP) nella AWS Global Accelerator Developer Guide.
- Per utilizzare il tuo intervallo di indirizzi IP Amazon VPC IP Address Manager, consulta Tutorial: Bring your IP address to IPAM nella Amazon VPC IPAM User Guide.

Indice

Definizioni BYOIP

- Certificato autofirmato X.509: uno standard di certificato più comunemente usato per crittografare e autenticare i dati all'interno di una rete. È un certificato utilizzato da per AWS convalidare il controllo sullo spazio IP da un record RDAP. Per ulteriori informazioni sui certificati X.509, consulta RFC 3280.
- Numero di sistema autonomo (ASN): identificatore univoco globale che definisce un gruppo di prefissi IP gestiti da uno o più operatori di rete che mantengono un'unica policy di instradamento chiaramente definita.
- Registro Internet regionale (RIR): un'organizzazione che gestisce l'allocazione e la registrazione di indirizzi IP e ASN in una regione del mondo.

- Registry Data Access Protocol (RDAP): un protocollo di sola lettura per interrogare i dati di registrazione correnti all'interno di un RIR. Le voci all'interno del database RIR interrogato vengono denominate "record RDAP". Alcuni tipi di record devono essere aggiornati dai clienti tramite un meccanismo fornito da RIR. Questi record vengono interrogati AWS per verificare il controllo di uno spazio di indirizzi nel RIR.
- Autorizzazione origine percorso (ROA): un oggetto creato dai RIR per i clienti allo scopo di autenticare la pubblicità IP, in sistemi autonomi particolari. Per una panoramica, consulta Route Origin Authorizations (ROAs) sul sito Web ARIN.
- Registro Internet locale (LIR): organizzazioni come i provider di servizi Internet che allocano un blocco di indirizzi IP da un RIR per i propri clienti.

Requisiti e quote

- L'intervallo di indirizzi deve essere registrato nel Regional Internet Registry (RIR). Consulta il tuo RIR per eventuali politiche relative alle aree geografiche. Al momento il BYOIP supporta la registrazione in American Registry for Internet Numbers (ARIN), Réseaux IP Européens Network Coordination Centre (RIPE) o Asia-Pacific Network Information Centre (APNIC). Deve essere registrato in un'entità aziendale o istituzionale e non può essere registrato per una persona fisica.
- L'intervallo di indirizzi IPv4 più specifico che puoi portare è /24.
- L'intervallo di indirizzi IPv6 più specifico che puoi fornire è /48 per i CIDR pubblicizzabili pubblicamente e /56 per i CIDR che non lo sono.
- I ROA non sono richiesti per gli intervalli CIDR che non sono pubblicizzabili pubblicamente, ma i record RDAP devono ancora essere aggiornati.
- È possibile assegnare ogni intervallo di indirizzi a una regione alla volta. AWS
- Puoi aggiungere al tuo account un totale di cinque intervalli di indirizzi BYOIP IPv4 e IPv6 per regione. AWS AWS Non è possibile modificare le quote per i CIDR BYOIP utilizzando la console Service Quotas, ma è possibile richiedere un aumento della quota contattando il AWS Support Center come descritto nelle quote di servizio nel.AWSRiferimenti generali di AWS
- Non puoi condividere il tuo intervallo di indirizzi IP con altri account AWS RAM a meno che non utilizzi Amazon VPC IP Address Manager (IPAM) e integri IPAM con Organizations. AWS Per ulteriori informazioni, consulta Integrate IPAM with AWS Organizations nella Amazon VPC IPAM User Guide.

- Gli indirizzi nell'intervallo di indirizzi IP deve avere una cronologia pulita. È opportuno esaminare la reputazione dell'intervallo di indirizzi IP e riservarti il diritto di rifiutare un intervallo di indirizzi IP se contiene un indirizzo IP che ha scarsa reputazione o è associato a un comportamento dannoso.
- Lo spazio di indirizzi legacy, ovvero lo spazio di indirizzi IPv4 distribuito dal registro centrale della Internet Assigned Numbers Authority (IANA) prima della formazione del sistema Regional Internet Registry (RIR), richiede ancora un oggetto ROA corrispondente.
- Per i LIR, è comune che usino un processo manuale per aggiornare i record. L'implementazione può richiedere giorni, a seconda del LIR.
- Per un blocco CIDR di grandi dimensioni sono necessari un singolo oggetto ROA e un record RDAP. Puoi trasferire più blocchi CIDR più piccoli da quell'intervallo verso AWS, anche tra più AWS regioni, utilizzando un unico oggetto e record.
- BYOIP non è supportato per Wavelength Zones o no. AWS Outposts
- Non apportare modifiche manuali al BYOIP nel RADb o in qualsiasi altro IRR. Il BYOIP aggiornerà automaticamente il RADb. Qualsiasi modifica manuale che includa l'ASN BYOIP causerà un errore nell'operazione di provisioning del BYOIP.
- Una volta impostato un intervallo di indirizzi IPv4 AWS, è possibile utilizzare tutti gli indirizzi IP dell'intervallo, incluso il primo indirizzo (l'indirizzo di rete) e l'ultimo indirizzo (l'indirizzo di trasmissione).

Prerequisiti di onboarding per l'intervallo di indirizzi BYOIP

Il processo di onboarding per BYOIP prevede due fasi, per le quali è necessario eseguire tre passaggi. Questi passaggi corrispondono ai passaggi descritti nel diagramma seguente. In questa documentazione sono inclusi i passaggi manuali; tuttavia, per aiutarti a eseguire questi passaggi, è possibile che il tuo RIR offra servizi gestiti.

Fase di preparazione

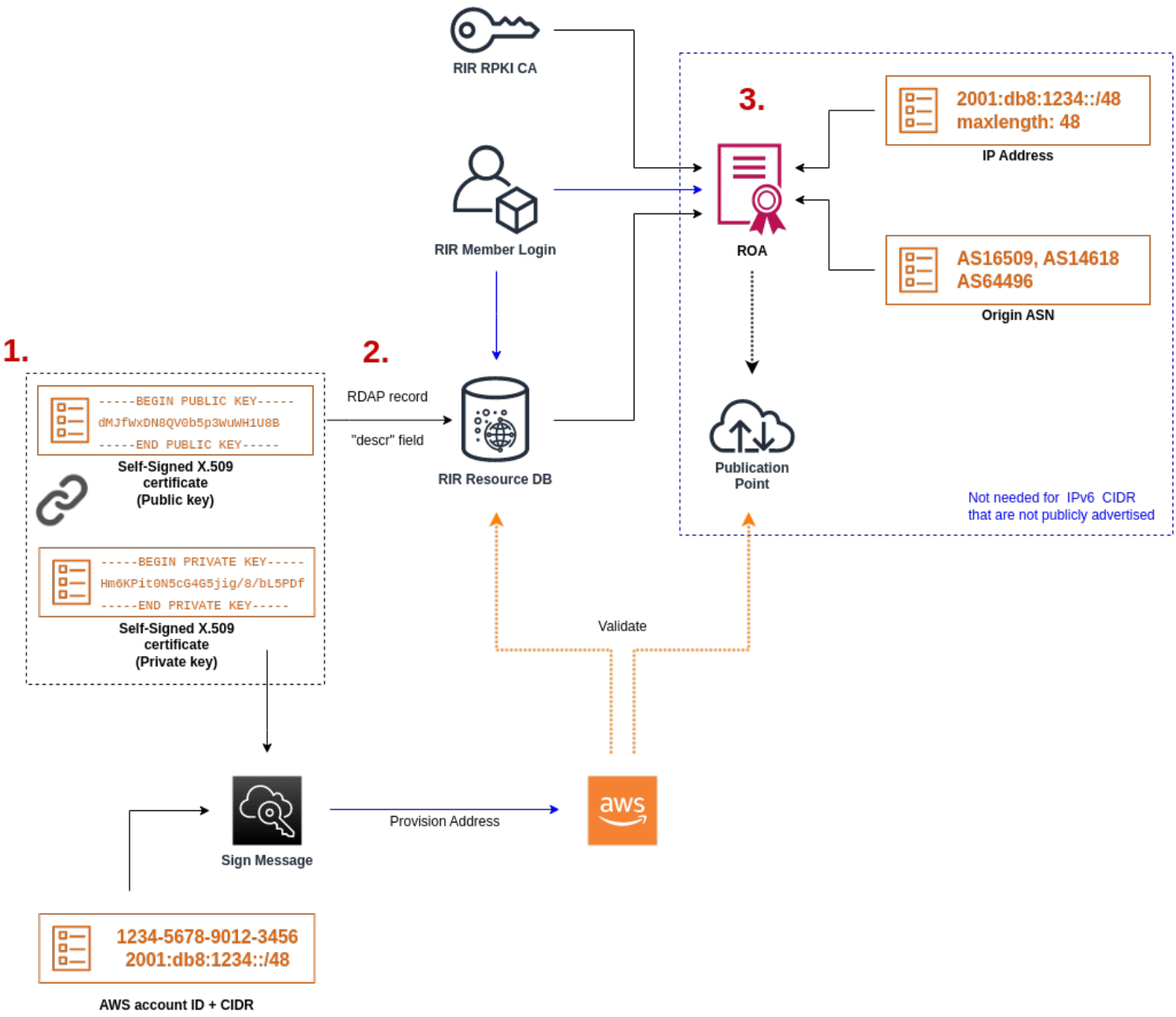
1. Crea una chiave privata e utilizzala per generare un certificato X.509 autofirmato a scopo di autenticazione. Questo certificato viene utilizzato solo durante la fase di provisioning.

Fase di configurazione RIR

2. Carica il certificato autofirmato nei commenti dei record RDAP.

3. Creazione di un oggetto ROA nel RIR. Il ROA definisce l'intervallo di indirizzi desiderato, i numeri ASN (Autonomous System Number) (ASN) autorizzati a pubblicizzare l'intervallo di indirizzi e una data di scadenza da registrare con l'RPKI (Resource Public Key Infrastructure) del tuo RIR.

> **Note**
>
> Non è richiesto un ROA per lo spazio di indirizzi IPv6 non pubblicizzabile pubblicamente.



Per attivare più intervalli di indirizzi non contigui, devi ripetere questo processo con ogni intervallo di indirizzi. Tuttavia, non è necessario ripetere i passaggi di preparazione e configurazione RIR se si divide un blocco contiguo in diverse regioni. AWS

L'attivazione di un intervallo di indirizzi non ha alcun effetto sugli intervalli di indirizzi attivati in precedenza.

> **Important**
>
> Prima di effettuare l'onboarding dell'intervallo di indirizzi, completa i prerequisiti seguenti. Le attività in questa sezione richiedono un terminale Linux e possono essere eseguite utilizzando Linux AWS CloudShell, o il sottosistema Windows per Linux.

1. Crea una chiave privata e genera un certificato X.509

Utilizza la seguente procedura per creare un certificato autofirmato X.509 e aggiungerlo al record RDAP per il RIR. Questa coppia di chiavi viene utilizzata per autenticare l'intervallo di indirizzi con il RIR. I comandi openssl richiedono OpenSSL versione 1.0.2 o successive.

Copia i comandi seguenti e sostituisci solo i valori segnaposto (testo in corsivo colorato).

Questa procedura segue le best practice per crittografare la chiave RSA privata e richiedere una passphrase per accedervi.

1. Genera una chiave privata RSA a 2048 bit come segue.

```
$ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out
 private-key.pem
```

   Il parametro `-aes256` specifica l'algoritmo utilizzato per crittografare la chiave privata. Il comando restituisce l'output seguente, inclusi i prompt per impostare una passphrase:

```
......+++
.+++
Enter PEM pass phrase: xxxxxxx
Verifying - Enter PEM pass phrase: xxxxxxx
```

   Puoi scaricare la chiave pubblica utilizzando il comando seguente:

```
$ openssl pkey -in private-key.pem -text
```

Questo restituisce un prompt della passphrase e il contenuto della chiave, che deve essere simile al seguente:

```
Enter pass phrase for private-key.pem: xxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
```

```
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
```

```
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

Custodisci la tua chiave privata in un luogo sicuro quando non è in uso.

2. Genera un certificato X.509 utilizzando la chiave privata creata nel passaggio precedente. In questo esempio, il certificato scade tra 365 giorni; dopo tale data diventa inaffidabile. Assicurarsi

di impostare la scadenza in modo appropriato. Il certificato deve essere valido solo per la durata del processo di fornitura. È possibile rimuovere il certificato dal record del RIR dopo il completamento del provisioning. Il comando `tr -d "\n"` rimuove i caratteri di nuova riga (interruzioni di riga) dall'output. Quando richiesto, è necessario fornire un nome comune, ma gli altri campi possono essere lasciati vuoti.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
 certificate.pem
```

Viene restituito un output simile al seguente:

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

> **Note**
>
> Il nome comune non è necessario per AWS il provisioning. Può essere qualsiasi nome di dominio interno o pubblico.

Puoi verificare il certificato utilizzando il comando seguente:

```
$ cat certificate.pem
```

L'output dovrebbe essere una stringa lunga con codifica PEM senza interruzioni di riga, preceduta da `-----BEGIN CERTIFICATE-----` e seguita da `-----END CERTIFICATE-----`.

2. Carica il certificato X.509 nel record RDAP nel RIR

Aggiungere il certificato creato in precedenza al record RDAP per il RIR. Assicurati di includere le stringhe `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` prima e dopo la porzione codificata. Tutto questo contenuto deve trovarsi su un'unica linea lunga. La procedura per l'aggiornamento di RDAP dipende dal RIR:

- Per ARIN, utilizza il portale Account Manager per aggiungere il certificato nella sezione "Commenti pubblici" per l'oggetto "Informazioni di rete" che rappresenta l'intervallo di indirizzi. Non aggiungerlo alla sezione commenti dell'organizzazione.
- Per RIPE, aggiungi il certificato come nuovo campo "descr" all'oggetto "inetnum" o "inet6num" che rappresenta il tuo intervallo di indirizzi. Di solito si trovano nella sezione "Le mie risorse" del portale del database RIPE. Non aggiungerlo alla sezione commenti della tua organizzazione o al campo "commenti" degli oggetti sopra indicati.
- Per APNIC, inviare per email il certificato a helpdesk@apnic.net per aggiungerlo manualmente al campo "osservazioni" per l'intervallo di indirizzi. Inviare l'e-mail utilizzando il contatto autorizzato APNIC per gli indirizzi IP.

Puoi rimuovere il certificato dal record dei Registri Internet Regional (RIR) dopo aver completato la fase di provisioning riportata di seguito.

3. Creazione di un oggetto ROA nel RIR

Crea un oggetto ROA per autorizzare Amazon ASN 16509 e 14618 a pubblicizzare l'intervallo di indirizzi, così come gli ASN che sono attualmente autorizzati a pubblicizzare l'intervallo di indirizzi. Per il AWS GovCloud (US) Regions, autorizza ASN 8987 anziché 16509 e 14618. È necessario impostare la lunghezza massima alle dimensioni del CIDR che si desidera importare. Il prefisso IPv4 più specifico che puoi importare è /24. L'intervallo di indirizzi IPv6 più specifico che puoi portare è /48 per i CIDR pubblicizzabili pubblicamente e /56 per i CIDR non pubblicizzabili pubblicamente.

> **Important**
>
> Quando crei un oggetto ROA per Amazon VPC IP Address Manager (IPAM), per i CIDR IPv4 devi impostare la lunghezza massima di un prefisso di indirizzo IP su `/24`. Per i CIDR IPv6, se vengono aggiunti a un pool pubblicizzabile, la lunghezza massima di un prefisso dell'indirizzo IP deve essere `/48`. Ciò garantisce la massima flessibilità per dividere l'indirizzo IP pubblico tra le regioni. AWS IPAM applica la lunghezza massima impostata. Per ulteriori informazioni sugli indirizzi BYOIP su IPAM, consulta il Tutorial: portare i CIDR di indirizzi BYOIP su IPAM nella Guida per l'utente di IPAM di Amazon VPC.

Potrebbe essere necessarie fino a 24 ore prima che il ROA diventi disponibile su Amazon. Per ulteriori informazioni, consulta il tuo RIR:

- Richieste — ROA ARIN
- — Gestire i ROA RIPE
- APNIC – Gestione delle route

Quando esegui la migrazione degli annunci pubblicitari da un carico di lavoro locale a AWS, devi creare un ROA per l'ASN esistente prima di creare il RoA per gli ASN di Amazon. In caso contrario, potresti avere un impatto sul routing e sugli annunci pubblicitari esistenti.

> **Important**
>
> Affinché Amazon possa pubblicizzare e continuare a pubblicizzare il tuo intervallo di indirizzi IP, i ROA per gli ASN di Amazon devono essere conformi alle precedenti linee guida. Se i tuoi RoAS non sono validi o non sono conformi alle linee guida di cui sopra, Amazon si riserva il diritto di smettere di pubblicizzare il tuo intervallo di indirizzi IP.

> **Note**
>
> Questo passaggio non è richiesto per lo spazio di indirizzi IPv6 non pubblicizzabile pubblicamente.

Onboarding del BYOIP

Il processo di onboarding per BYOIP prevede le seguenti attività a seconda delle tue esigenze.

Attività

- Effettuare il provisioning di un intervallo di indirizzi pubblicizzabile pubblicamente in AWS
- Effettuare il provisioning di un intervallo di indirizzi IPv6 non pubblicizzabile pubblicamente
- Pubblicizza l'intervallo di indirizzi tramite AWS
- Annullamento del provisioning dell'intervallo di indirizzi

Effettuare il provisioning di un intervallo di indirizzi pubblicizzabile pubblicamente in AWS

Quando fornisci un intervallo di indirizzi da utilizzare AWS, confermi di controllare l'intervallo di indirizzi e autorizzi Amazon a pubblicizzarlo. Verifichiamo inoltre che tu abbia il controllo dell'intervallo di indirizzi tramite un messaggio di autorizzazione firmato. Questo messaggio è firmato con la coppia di chiavi X.509 autofirmata utilizzata per aggiornare il record RDAP con il certificato X.509. AWS richiede un messaggio di autorizzazione firmato crittograficamente da presentare al RIR. Il RIR autentica la firma basandosi sul certificato aggiunto a RDAP e controlla i dettagli dell'autorizzazione rispetto al ROA.

Eseguire il provisioning dell'intervallo di indirizzi

1. Composizione di un messaggio

   Comporre il messaggio di autorizzazione in testo normale. Il formato del messaggio è il seguente, in cui la data è la data di scadenza del messaggio:

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   Sostituire il numero di account, l'intervallo di indirizzi e la data di scadenza con i valori desiderati per creare un messaggio analogo al seguente:

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   Questo non deve essere confuso con un messaggio ROA, che ha un aspetto simile.

2. Firma di messaggi

   Firmare il messaggio di testo normale utilizzando la chiave privata creata in precedenza. La firma restituita da questo comando è una stringa lunga che sarà necessario utilizzare nel passaggio successivo.

   > **Important**
   >
   > Si consiglia di copiare e incollare questo comando. Ad eccezione del contenuto del messaggio, non modificare o sostituire nessuno dei valori.

   ```
   signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
    rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM
    | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
   ```

3. Provisioning dell'indirizzo

   Utilizzate il AWS CLI provision-byoip-cidrcomando per fornire l'intervallo di indirizzi. L'opzione `--cidr-authorization-context` utilizza le stringhe di messaggio e firma create in precedenza.

   > **Important**
   >
   > È necessario specificare la AWS regione in cui deve essere fornito l'intervallo BYOIP se diverso dalla configurazione in uso.AWS CLI `Default region name`

   ```
   aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
    Message="$text_message",Signature="$signed_message" --region us-east-1
   ```

   Il provisioning di un intervallo di indirizzi è un'operazione asincrona, perciò la chiamata ritorna immediatamente, mentre l'intervallo di indirizzi non è pronto per l'utilizzo finché lo stato non passa da `pending-provision` a `provisioned`.

4. Monitoraggio dell'avanzamento

   Sebbene la maggior parte del provisioning venga completata entro due ore, potrebbe essere necessaria fino a una settimana per completare il processo di provisioning per gli intervalli

pubblicizzabili pubblicamente. Utilizzate il describe-byoip-cidrscomando per monitorare l'avanzamento, come in questo esempio:

```
aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
```

Se si verificano problemi durante il provisioning e lo stato passa a `failed-provision`, eseguire nuovamente il comando `provision-byoip-cidr` dopo che i problemi sono stati risolti.

Effettuare il provisioning di un intervallo di indirizzi IPv6 non pubblicizzabile pubblicamente

Per impostazione predefinita, viene eseguito il provisioning di un intervallo di indirizzi affinché sia pubblicizzabile pubblicamente su Internet. Puoi eseguire il provisioning di un intervallo di indirizzi IPv6 che non sarà pubblicizzabile pubblicamente. Per le route che non sono pubblicamente pubblicizzabili, il processo di provisioning viene generalmente completato in pochi minuti. Quando associ un blocco CIDR IPv6 da un intervallo di indirizzi non pubblici a un VPC, puoi accedere al CIDR IPv6 solo tramite opzioni di connettività ibride che supportano IPv6, ad esempio AWS Direct Connect, AWS Site-to-Site VPN, oppure Gateway di transito Amazon VPC.

Non è richiesto un ROA per effettuare il provisioning di un intervallo di indirizzi non pubblici.

> **Important**
>
> - Puoi specificare solo se un intervallo di indirizzi sarà pubblicizzabile pubblicamente durante il provisioning. Non puoi modificare lo stato pubblicizzabile in un secondo momento.
> - Amazon VPC non supporta i CIDR con indirizzo locale univoco (ULA). Tutti VPC devono avere CIDR IPv6 univoci. Due VPC non possono avere lo stesso intervallo CIDR IPv6.

Per fornire un intervallo di indirizzi IPv6 che non sarà pubblicizzabile pubblicamente, usa il comando seguente. provision-byoip-cidr

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

Pubblicizza l'intervallo di indirizzi tramite AWS

Dopo aver eseguito il provisioning, l'intervallo di indirizzi è pronto per essere pubblicizzato. Deve essere pubblicizzato l'intervallo di indirizzi esatto oggetto del provisioning. Non può essere pubblicizzata solo una parte dell'intervallo di indirizzi oggetto del provisioning.

Se hai eseguito il provisioning di un intervallo di indirizzi IPv6 che non verrà pubblicizzato pubblicamente, non è necessario completare questa fase.

Ti consigliamo di smettere di pubblicizzare l'intervallo di indirizzi o qualsiasi parte dell'intervallo di altre località prima di pubblicizzarlo. AWS Se continui a pubblicizzare il tuo intervallo di indirizzi IP o parte di esso da altre località, non possiamo supportarlo in modo affidabile o risolvere i problemi. In particolare, non possiamo garantire che il traffico verso l'intervallo di indirizzi o una parte dell'intervallo entri nella nostra rete.

Per ridurre al minimo i tempi di inattività, puoi configurare AWS le tue risorse in modo da utilizzare un indirizzo del tuo pool di indirizzi prima che venga pubblicizzato, quindi contemporaneamente smettere di pubblicizzarlo dalla posizione corrente e iniziare a pubblicizzarlo. AWS Per ulteriori informazioni sull'allocazione di un indirizzo IP elastico da un pool di indirizzi, consulta Allocare un indirizzo IP elastico.

Limitazioni

- È possibile eseguire il comando advertise-byoip-cidr al massimo una volta ogni 10 secondi, anche se è necessario specificare ogni volta i diversi intervalli di indirizzi.
- È possibile eseguire il comando withdraw-byoip-cidr al massimo una volta ogni 10 secondi, anche se è necessario specificare i diversi intervalli di indirizzi ogni volta.

Per pubblicizzare l'intervallo di indirizzi, utilizzate il seguente advertise-byoip-cidrcomando.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Per interrompere la pubblicità dell'intervallo di indirizzi, usa il seguente withdraw-byoip-cidrcomando.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Annullamento del provisioning dell'intervallo di indirizzi

Per smettere di utilizzare il tuo intervallo di indirizzi con AWS, rilascia innanzitutto tutti gli indirizzi IP elastici e dissocia i blocchi CIDR IPv6 che sono ancora allocati dal pool di indirizzi. Quindi interrompi la pubblicità dell'intervallo di indirizzi e, infine, annulla il provisioning dell'intervallo di indirizzi.

Non puoi annullare il provisioning di una parte dell'intervallo di indirizzi. Se desideri utilizzare un intervallo di indirizzi più specifico con AWS, elimina il provisioning dell'intero intervallo di indirizzi e fornisci un intervallo di indirizzi più specifico.

(IPv4) Per rilasciare ciascun indirizzo IP elastico, utilizza il seguente comando release-address.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Per dissociare un blocco CIDR IPv6, utilizzate il seguente comando. disassociate-vpc-cidr-block

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
 --region us-east-1
```

Per interrompere la pubblicità dell'intervallo di indirizzi, utilizzate il seguente comando. withdraw-byoip-cidr

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Per eliminare il provisioning dell'intervallo di indirizzi, utilizzate il deprovision-byoip-cidrcomando seguente.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

L'annullamento del provisioning di un intervallo di indirizzi può richiedere fino a un giorno.

Utilizzo dell'intervallo di indirizzi

Puoi visualizzare e utilizzare gli intervalli di indirizzi IPv4 e IPv6 di cui hai effettuato il provisioning nell'account.

Intervalli di indirizzi IPv4

Puoi creare un indirizzo IP elastico dal tuo pool di indirizzi IPv4 e utilizzarlo con AWS le tue risorse, come istanze EC2, gateway NAT e Network Load Balancer.

Per visualizzare le informazioni sui pool di indirizzi IPv4 di cui hai effettuato il provisioning nel tuo account, usa il seguente comando 4-pools. describe-public-ipv

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Per creare un indirizzo IP elastico dal pool di indirizzi IPv4, utilizza il comando allocate-address. Puoi utilizzare l'opzione `--public-ipv4-pool` per specificare l'ID del pool di indirizzi restituito da `describe-byoip-cidrs`. Oppure, puoi utilizzare l'opzione `--address` per specificare un indirizzo dall'intervallo di indirizzi di cui è stato effettuato il provisioning.

Intervalli di indirizzi IPv6

Per visualizzare informazioni sui pool di indirizzi IPv6 di cui hai effettuato il provisioning nell'account, utilizza il comando describe-ipv6-pools riportato di seguito.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Per creare un VPC e specificare un blocco CIDR IPv6 dal pool di indirizzi IPv6, utilizza il seguente comando create-vpc. Per consentire ad Amazon di scegliere il blocco CIDR IPv6 dal pool di indirizzi IPv6, ometti l'opzione `--ipv6-cidr-block`.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-
pool pool-id --region us-east-1
```

Per associare un blocco CIDR IPv6 dal tuo pool di indirizzi IPv6 a un VPC, usa il seguente comando. associate-vpc-cidr-block Per consentire ad Amazon di scegliere il blocco CIDR IPv6 dal pool di indirizzi IPv6, ometti l'opzione `--ipv6-cidr-block`.

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-
cidr --ipv6-pool pool-id --region us-east-1
```

Per visualizzare i VPC e le informazioni relative al pool di indirizzi IPv6 associato, utilizza il comando describe-vpcs. Per visualizzare informazioni sui blocchi CIDR IPv6 associati da uno specifico pool di indirizzi IPv6, utilizzare il seguente comando 6-pool-cidrs. get-associated-ipv

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Se annulli l'associazione del blocco CIDR IPv6 dal VPC, viene rilasciato nuovamente nel pool di indirizzi IPv6.

Convalida del BYOIP

1. Convalida della coppia di chiavi x.509 autofirmata

   Verifica che il certificato sia stato caricato e sia valido tramite il comando whois.

   Per ARIN, usa `whois -h whois.arin.net r + 2001:0DB8:6172::/48` per cercare il record RDAP dell'intervallo di indirizzi. Controlla la sezione `Public Comments` per verificare `NetRange` (intervallo di rete) nell'output del comando. Il certificato deve essere aggiunto nella sezione `Public Comments` dell'intervallo di indirizzi.

   Puoi esaminare i `Public Comments` contenenti il certificato usando il comando seguente:

   ```
   whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
   ```

   Questo restituisce un output con il contenuto della chiave, che deve essere simile al seguente:

   ```
   Public Comments:
   -----BEGIN CERTIFICATE-----
   MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
   LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
   hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
   wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
   NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
   rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
   VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
   W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
   R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
   prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
   mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
   Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
   xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
   3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
   AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
   QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
   08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
   ```

```
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Per RIPE, usa `whois -r -h whois.ripe.net` *`2001:0DB8:7269::/48`* per cercare il record RDAP dell'intervallo di indirizzi. Controlla la sezione `descr` per esaminare l'oggetto `inetnum` (intervallo di rete) nell'output del comando. Il certificato deve essere aggiunto come nuovo campo `descr` dell'intervallo di indirizzi.

Puoi esaminare i `descr` contenenti il certificato usando il comando seguente:

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Questo restituisce un output con il contenuto della chiave, che deve essere simile al seguente:

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Per APNIC, usa `whois -h whois.apnic.net` *`2001:0DB8:6170::/48`* per cercare il record RDAP dell'intervallo di indirizzi BYOIP. Controlla la sezione `remarks` per esaminare l'oggetto `inetnum` (intervallo di rete) nell'output del comando. Il certificato deve essere aggiunto come nuovo campo `remarks` dell'intervallo di indirizzi.

Puoi esaminare i `remarks` contenenti il certificato usando il comando seguente:

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Questo restituisce un output con il contenuto della chiave, che deve essere simile al seguente:

```
remarks:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. Convalida della creazione di un oggetto ROA

   Convalida la corretta creazione degli oggetti ROA utilizzando l'API dati RIPEstat. Assicurati di testare l'intervallo di indirizzi rispetto agli ASN Amazon 16509 e 14618, oltre agli ASN attualmente autorizzati a pubblicizzare l'intervallo di indirizzi.

Puoi ispezionare gli oggetti ROA da diversi ASN Amazon con il tuo intervallo di indirizzi usando il comando seguente:

```
curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
resource=ASN&prefix=CIDR
```

In questo output di esempio, la risposta ha il risultato di `"status": "valid"` per l'ASN Amazon 16509. Indica che l'oggetto ROA dell'intervallo di indirizzi è stato creato correttamente:


```
{
    "messages": [],
    "see_also": [],
    "version": "0.3",
    "data_call_name": "rpki-validation",
    "data_call_status": "supported",
    "cached": false,
    "data": {
        "validating_roas": [
            {
                "origin": "16509",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "valid"
            },
            {
                "origin": "14618",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            },
            {
                "origin": "64496",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            }
        ],
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
```

```
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```

Lo stato “unknown” indica che l'oggetto ROA dell'intervallo di indirizzi non è stato creato. Lo stato “invalid_asn” indica che l'oggetto ROA dell'intervallo di indirizzi non è stato creato correttamente.

Disponibilità regionale

La funzionalità BYOIP è attualmente disponibile in tutte le regioni AWS commerciali ad eccezione delle regioni cinesi.

Disponibilità delle zone locali

Una zona locale è un'estensione di una regione situata in prossimità geografica degli utenti. AWS Le zone locali sono raggruppate in "gruppi di confini di rete". In AWS, un gruppo di confine di rete è una raccolta di Availability Zones (AZ), Local Zones o Wavelength Zones da AWS cui pubblicizza un indirizzo IP pubblico. Le Local Zone possono avere gruppi di confine di rete diversi rispetto alle AZ di una AWS regione per garantire una latenza o una distanza fisica minima tra la AWS rete e i clienti che accedono alle risorse in queste Zone.

Puoi eseguire il provisioning di intervalli di indirizzi BYOIPv4 e pubblicizzarli nei seguenti gruppi di confini di rete di zone locali utilizzando l'opzione `--network-border-group`:

- us-east-1-dfw-2
- us-west-2-lax-1
- us-west-2-phx-2

Se hai abilitato delle zone locali (consulta Enable a Local Zone), puoi scegliere un gruppo di confine di rete per le zone locali quando effettui il provisioning e pubblicizzi un CIDR BYOIPv4. Scegliete con attenzione il gruppo di confine della rete poiché l'EIP e la AWS risorsa a cui è associata devono risiedere nello stesso gruppo di confini di rete.

> **Note**
>
> Al momento non è possibile effettuare il provisioning o pubblicizzare intervalli di indirizzi BYOIPv6 nelle zone locali.

Ulteriori informazioni

Per ulteriori informazioni, consulta l' AWS Online Tech talk Deep Dive on Bring Your Own IP.

Indirizzi IP elastici

Un indirizzo IP elastico è un indirizzo IPv4 statico progettato per il cloud computing dinamico. Un indirizzo IP elastico viene assegnato al tuo AWS account ed è tuo fino a quando non lo rilasci. Mediante un indirizzo IP elastico, è possibile mascherare il guasto di un'istanza o di un software rimappando rapidamente l'indirizzo per un'altra istanza presente nell'account. In alternativa, è possibile specificare l'indirizzo IP elastico in un record DNS del dominio, in modo che il dominio punti all'istanza specificata. Per ulteriori informazioni, consulta la documentazione del tuo registrar di domini.

Un indirizzo IP elastico è un indirizzo IPv4 pubblico raggiungibile da Internet. Se l'istanza in uso non dispone di un indirizzo IPv4 pubblico, puoi associare un indirizzo IP elastico all'istanza per abilitare la comunicazione con Internet. Ad esempio, ciò consente di connettersi all'istanza dal computer locale.

Indice

Prezzi degli indirizzi IP elastici

AWS costi per tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.

Nozioni di base sull'indirizzo IP elastico

Le caratteristiche di base di un indirizzo IP elastico sono le seguenti:

- Un indirizzo IP elastico è statico e non cambia nel tempo.
- Un indirizzo IP elastico può essere utilizzato solo in una regione specifica e non può essere spostato in una regione diversa.
- Un indirizzo IP elastico proviene dal pool di indirizzi IPv4 di Amazon o da un pool di indirizzi IPv4 personalizzato che hai inserito nel tuo account. AWS
- Per utilizzare un indirizzo IP elastico bisogna prima allocarne uno al proprio account e associarlo con la propria istanza o con un'interfaccia di rete.
- Quando si associa un indirizzo IP elastico a un'istanza, viene associato anche all'interfaccia di rete primaria dell'istanza. Quando si associa un indirizzo IP elastico a un'interfaccia di rete collegata a un'istanza, viene associato anche all'istanza.
- Quando associ un indirizzo IP elastico a un'istanza o alla sua interfaccia di rete principale, se all'istanza è già associato un indirizzo IPv4 pubblico, tale indirizzo IPv4 pubblico viene rilasciato nuovamente nel pool di indirizzi IPv4 pubblici di Amazon e l'indirizzo IP elastico viene invece associato all'istanza. Non puoi riutilizzare l'indirizzo IPv4 pubblico precedentemente associato all'istanza e non puoi convertire quell'indirizzo IPv4 pubblico in un indirizzo IP elastico. Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici.
- È possibile disassociare un indirizzo IP Elastic da una risorsa e associarlo nuovamente con una risorsa differente. Per evitare comportamenti imprevisti, assicurarsi che tutte le connessioni attive alla risorsa denominata nell'associazione esistente siano chiuse prima di apportare la modifica. Dopo aver associato l'indirizzo IP Elastic a una risorsa diversa, è possibile riaprire le connessioni alla risorsa appena associata.
- Un indirizzo IP elastico disassociato rimane allocato al proprio account fino all'esplicito rilascio. Ti vengono addebitati tutti gli indirizzi IP elastici del tuo account, indipendentemente dal fatto che siano associati o meno a un'istanza. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.
- Quando un indirizzo IP elastico viene associato a un'istanza che in precedenza aveva un indirizzo IPv4 pubblico, l'hostname del DNS pubblico dell'istanza cambia per abbinare l'indirizzo IP elastico.
- Risolveremo un hostname del DNS pubblico per l'indirizzo IPv4 pubblico o per l'indirizzo IP elastico dell'istanza al di fuori della rete della stessa e per l'indirizzo IPv4 privato dell'istanza all'interno della rete dell'istanza.

- Quando allochi un indirizzo IP elastico da un pool di indirizzi IP che hai trasferito al tuo AWS account, questo non viene conteggiato ai fini dei limiti di indirizzi IP elastici. Per ulteriori informazioni, consulta Quota degli indirizzi IP elastici.
- Quando si allocano gli indirizzi IP elastici, è possibile associare gli indirizzi IP elastici a un gruppo di confine di rete. Questa è la posizione da cui pubblicizziamo il blocco CIDR. L'impostazione del gruppo di confine di rete limita il blocco CIDR a questo gruppo. Se non si specifica il gruppo di confine di rete, viene impostato il gruppo di confine contenente tutte le zone di disponibilità nella regione (ad esempio `us-west-2`).
- Un indirizzo IP elastico può essere utilizzato solo in un gruppo di confine di rete specifico.

Utilizzo degli indirizzi IP elastici

Le sezioni seguenti descrivono il funzionamento degli indirizzi IP elastici.

Attività

- Allocare un indirizzo IP elastico
- Descrizione degli indirizzi IP elastici
- Applicazione di tag a un indirizzo IP elastico
- Associazione di un indirizzo IP elastico a un'istanza o un'interfaccia di rete
- Annullare l'associazione di un indirizzo IP elastico
- Trasferimento degli indirizzi IP elastici
- Rilascio di un indirizzo IP elastico
- Recupero di un indirizzo IP elastico
- Utilizzo del DNS inverso per applicazioni e-mail

Allocare un indirizzo IP elastico

Puoi allocare un indirizzo IP elastico dal pool di indirizzi IPv4 pubblici di Amazon o da un pool di indirizzi IP personalizzato che hai trasferito al tuo account. AWS Per ulteriori informazioni su come aggiungere il tuo intervallo di indirizzi IP al tuo AWS account, consulta. Utilizzare gli indirizzi IP personali (BYOIP) in Amazon EC2

È possibile allocare un indirizzo IP elastico utilizzando uno dei metodi descritti di seguito.

Console

Per allocare un indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Network & Security (Rete e sicurezza) e poi Elastic IPs (IP elastici).
3. Scegliere Allocate Elastic IP address (Alloca indirizzo IP elastico).
4. (Facoltativo) Quando si assegna un indirizzo IP elastico (EIP), si sceglie il gruppo di confini di rete in cui allocare l'EIP. Un gruppo di confine di rete è una raccolta di Availability Zones (AZ), Local Zones o Wavelength Zones da AWS cui pubblicizza un indirizzo IP pubblico. Le Local Zones e Wavelength Zones possono avere gruppi di confini di rete diversi rispetto alle AZ di una regione per garantire una latenza o una distanza fisica minima tra AWS la rete e i clienti che accedono alle risorse in queste Zone.

   > **Important**
   >
   > È necessario allocare un EIP nello stesso gruppo di confini di rete della AWS risorsa che verrà associata all'EIP. Un EIP in un gruppo di confini di rete può essere pubblicizzato solo nelle zone di quel gruppo di confini di rete e non in altre zone rappresentate da altri gruppi di confini di rete.

   Se hai abilitato le zone locali o le zone Wavelength (per ulteriori informazioni, consulta Abilitazione di una zona locale o Abilitazione delle zone Wavelength), puoi scegliere un gruppo di confini di rete per AZ, zone locali o zone Wavelength. Scegli con attenzione il gruppo di confini di rete poiché l'EIP e la risorsa AWS a cui è associata devono risiedere nello stesso gruppo di confini di rete. Puoi utilizzare la console EC2 per visualizzare il gruppo di confini di rete in cui si trovano le tue Availability Zones, Local Zones o Wavelength Zones. In genere, tutte le zone di disponibilità in una regione appartengono allo stesso gruppo di confini di rete, mentre le zone locali o le zone Wavelength Zone appartengono a gruppi di confini di rete separati.

   Se non hai abilitato le zone locali o le zone Wavelength, quando allochi un EIP, il gruppo di confini di rete che rappresenta tutte le AZ della regione (ad esempio, `us-west-2`) è predefinito e non potrai modificarlo. Ciò significa che l'EIP assegnato a questo gruppo di confini di rete verrà pubblicizzato in tutte le AZ della regione in cui ti trovi.

5. Per Public IPv4 address pool (Pool di indirizzi IPv4 pubblici) scegliere una delle seguenti opzioni:

   - Amazon's pool of IPv4 addresses (Pool di indirizzi IPv4 di Amazon) — Se desideri che un indirizzo IPv4 venga allocato dal pool di indirizzi IP di Amazon.
   - Indirizzo IPv4 pubblico che porti al tuo AWS account: se desideri allocare un indirizzo IPv4 da un pool di indirizzi IP che hai trasferito al tuo account. AWS Questa opzione è disattivata se non disponi di pool di indirizzi IP.
   - Customer owned pool of IPv4 addresses (Pool di indirizzi IPv4 di proprietà del cliente) - Se desideri allocare un indirizzo IPv4 da un pool creato dalla rete on-premise da utilizzare con un AWS Outpost. Questa opzione è disattivata se non disponi di un Outpost. AWS
6. (Facoltativo) Aggiunta o rimozione di un tag.

   [Aggiunta di un tag] Scegli Aggiungi nuovo tag e procedi come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

   [Rimuovi un tag] Scegli Rimuovi a destra della Chiave e del Valore del tag.
7. Selezionare Alloca.

AWS CLI

Per allocare un indirizzo IP elastico

Utilizzare il comando allocate-address della AWS CLI .

PowerShell

Per allocare un indirizzo IP elastico

Usa il New-EC2Address AWS Tools for Windows PowerShell comando.

Descrizione degli indirizzi IP elastici

È possibile descrivere un indirizzo IP elastico utilizzando uno dei seguenti metodi.

Console

Per descrivere gli indirizzi IP elastici

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico da visualizzare e scegliere Actions (Operazioni), View details (Visualizza dettagli).

AWS CLI

Per descrivere gli indirizzi IP elastici

Utilizzate il comando describe-addresses AWS CLI .

PowerShell

Per descrivere gli indirizzi IP elastici

Usa il comando. Get-EC2Address AWS Tools for Windows PowerShell

Applicazione di tag a un indirizzo IP elastico

È possibile assegnare tag personalizzati ai propri indirizzi IP elastici per categorizzarli in vari modi, per esempio a seconda dello scopo, del proprietario o dell'ambiente. Questa procedura aiuta a trovare velocemente uno specifico indirizzo IP elastico grazie ai tag personalizzati che gli sono stati assegnati.

Non è supportato il tracciamento del costo di allocazione tramite i tag dell'indirizzo IP elastico.

È possibile applicare tag a un indirizzo IP elastico utilizzando uno dei metodi descritti di seguito.

Console

Per applicare un tag a un indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico da taggare e scegliere Actions (Operazioni), View details (Visualizza dettagli).

4. Nella sezione Tags scegliere Manage tags (Gestisci tag).
5. Specificare una coppia chiave e valore di tag.
6. (Facoltativo) Scegliere Add Tag (Aggiungi tag) per aggiungere tag aggiuntivi.
7. Seleziona Salva.

AWS CLI

Per applicare un tag a un indirizzo IP elastico

Usate il comando create-tags AWS CLI .

```
aws ec2 create-tags --resources eipalloc-12345678 --tags Key=Owner,Value=TeamA
```

PowerShell

Per applicare un tag a un indirizzo IP elastico

Usa il comando. New-EC2Tag AWS Tools for Windows PowerShell

Il comando `New-EC2Tag` necessita di un parametro `Tag` che specifichi la coppia chiave/valore per poter essere utilizzato con i tag dell'indirizzo IP elastico. I seguenti comandi creano il parametro `Tag`.

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
 PS C:\> $tag.Key = "Owner"
 PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource eipalloc-12345678 -Tag $tag
```

Associazione di un indirizzo IP elastico a un'istanza o un'interfaccia di rete

Se si sta cercando di associare un indirizzo IP elastico a un'istanza in modo da consentire la comunicazione con Internet, occorre accertarsi che l'istanza si trovi in una sottorete pubblica. Per ulteriori informazioni, consulta la sezione Gateway Internet nella Guida per l'utente di Amazon VPC.

È possibile associare un indirizzo IP elastico a un'istanza o un'interfaccia di rete utilizzando uno dei metodi descritti di seguito.

Console

Per associare un indirizzo IP elastico a un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico creato e scegliere Actions (Operazioni), Associate address (Associa indirizzo IP elastico).
4. Per Resource type (Tipo di risorsa), scegliere Instance (Istanza).
5. Ad esempio, scegliere l'istanza con cui associare l'indirizzo IP elastico. È inoltre possibile immettere del testo per cercare un'istanza specifica.
6. (Facoltativo) Per Private IP address (Indirizzo IP privato), specificare un indirizzo IP privato a cui associare l'indirizzo IP elastico.
7. Seleziona Associate (Associa).

Per associare un indirizzo IP elastico a un'interfaccia di rete.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico creato e scegliere Actions (Operazioni), Associate address (Associa indirizzo IP elastico).
4. Per il Resource type (Tipo di risorsa), scegli Network interface (Interfaccia di rete).
5. Per Network interface (Interfaccia di rete), scegliere l'interfaccia di rete con cui associare l'indirizzo IP elastico. È inoltre possibile immettere del testo per cercare un'interfaccia di rete specifica.
6. (Facoltativo) Per Private IP address (Indirizzo IP privato), specificare un indirizzo IP privato a cui associare l'indirizzo IP elastico.
7. Seleziona Associate (Associa).

AWS CLI

Per associare un indirizzo IP elastico

Utilizzate il comando associate-address AWS CLI .

PowerShell

Per associare un indirizzo IP elastico

Usate il comando. Register-EC2Address AWS Tools for Windows PowerShell

Annullare l'associazione di un indirizzo IP elastico

È possibile annullare l'associazione di un indirizzo IP elastico da un'istanza o un'interfaccia di rete in qualsiasi momento. Dopo aver annullato l'associazione dell'indirizzo IP elastico, è possibile riassociarlo a un'altra risorsa.

È possibile annullare l'associazione di un indirizzo IP elastico utilizzando uno dei metodi descritti di seguito.

Console

Per annullare l'associazione e riassociare un indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico per il quale annullare l'associazione, quindi selezionare Actions (Operazioni), Disassociate Elastic IP address (Annulla associazione indirizzo IP elastico).
4. Selezionare Disassociate (Annulla associazione).

AWS CLI

Per annullare l'associazione di un indirizzo IP elastico

Utilizzare il comando disassociate-address AWS CLI .

PowerShell

Per annullare l'associazione di un indirizzo IP elastico

Utilizza il comando Unregister-EC2Address. AWS Tools for Windows PowerShell

Trasferimento degli indirizzi IP elastici

Questa sezione descrive come trasferire indirizzi IP elastici da un Account AWS a un altro. Il trasferimento di indirizzi IP elastici può risultare utile nelle seguenti situazioni:

- Ristrutturazione organizzativa: utilizza i trasferimenti di indirizzi IP elastici per spostare rapidamente i carichi di lavoro da uno all'altro. Account AWS Non è necessario attendere che i nuovi indirizzi IP elastici vengano inseriti nell'elenco consentito nei gruppi di sicurezza e nei NACL.
- Amministrazione centralizzata della sicurezza: utilizza un account di AWS sicurezza centralizzato per tracciare e trasferire indirizzi IP elastici che sono stati controllati per verificarne la conformità alla sicurezza.
- Ripristino di emergenza: utilizza i trasferimenti di indirizzi IP elastici per eseguire nuovamente la mappatura degli IP in modo rapido per i carichi di lavoro su Internet rivolti al pubblico durante gli eventi di emergenza.

Il trasferimento degli indirizzi IP elastici è gratuito.

Attività

- Abilitare il trasferimento di indirizzi IP elastici
- Disabilitazione del trasferimento di indirizzi IP elastici
- Accettazione di un indirizzo IP elastico trasferito

Abilitare il trasferimento di indirizzi IP elastici

Questa sezione descrive come accettare un indirizzo IP elastico trasferito. Prendi nota delle seguenti limitazioni relative all'abilitazione degli indirizzi IP elastici per il trasferimento:

- È possibile trasferire indirizzi IP elastici da qualsiasi Account AWS (account di origine) a qualsiasi altro AWS account nella stessa AWS regione (account di trasferimento).
- Quando si trasferisce un indirizzo IP elastico, viene eseguito un handshake in due passaggi tra gli Account AWS. Quando l'account di origine inizia il trasferimento, gli account di trasferimento hanno sette giorni per accettare il trasferimento dell'indirizzo IP elastico. Durante questi sette giorni, l'account di origine può visualizzare il trasferimento in sospeso (ad esempio nella AWS console o utilizzando il describe-address-transfers AWS CLI comando). Dopo sette giorni, il trasferimento scade e la proprietà dell'indirizzo IP elastico ritorna all'account di origine.

- I trasferimenti accettati sono visibili sull'account di origine (ad esempio nella AWS console o utilizzando il describe-address-transfers AWS CLI comando) per tre giorni dopo l'accettazione dei trasferimenti.
- AWS non notifica agli account di trasferimento le richieste di trasferimento di indirizzi IP elastici in sospeso. Il proprietario dell'account di origine deve notificare al proprietario dell'account di trasferimento che esiste una richiesta di trasferimento di indirizzo IP elastico che deve accettare.
- Tutti i tag che sono associati a un indirizzo IP elastico da trasferire vengono reimpostati al termine del trasferimento.
- Non è possibile trasferire indirizzi IP elastici allocati da pool di indirizzi IPv4 pubblici che vengono trasferiti ai propri pool di indirizzi, comunemente denominati pool di indirizzi Bring Your Own IP (BYOIP). Account AWS
- Se si tenta di trasferire un indirizzo IP elastico a cui è associato un record DNS inverso, è possibile iniziare il processo di trasferimento, ma l'account di trasferimento non sarà in grado di accettare il trasferimento finché il record DNS associato non verrà rimosso.
- Se hai abilitato e configurato AWS Outposts, potresti aver allocato indirizzi IP elastici da un pool di indirizzi IP (CoIP) di proprietà del cliente. Non è possibile trasferire indirizzi IP elastici allocati dai CoIP. Tuttavia, puoi utilizzarlo AWS RAM per condividere un CoIP con un altro account. Per ulteriori informazioni, consulta Indirizzi IP di proprietà del cliente nella Guida per l'utente di AWS Outposts .
- Puoi utilizzare Amazon VPC IPAM per monitorare il trasferimento di indirizzi IP elastici agli account di un'organizzazione da AWS Organizations. Per ulteriori informazioni, consulta Visualizza la cronologia degli indirizzi IP. Tuttavia, se un indirizzo IP elastico viene trasferito su un account Account AWS esterno all'organizzazione la cronologia di controllo IPAM dell'indirizzo IP elastico andrà persa.

Questa sezione deve essere completata dall'account di origine.

Console

Abilitare il trasferimento di indirizzi IP elastici

1. Assicurati di utilizzare l' AWS account di origine.
2. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
3. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).

4. Seleziona uno o più indirizzi IP elastici per abilitare il trasferimento e scegli Actions (Azioni), Enable transfer (Abilita trasferimento).
5. Se stai trasferendo più indirizzi IP elastici, vedrai l'opzione Transfwer type (Tipo di trasferimento). Selezionare una delle seguenti opzioni:
   - Scegli Account singolo se trasferisci gli indirizzi IP elastici su un unico AWS account.
   - Scegli Account multipli se trasferisci gli indirizzi IP elastici su più AWS account.
6. In Transfer account ID (ID degli account di trasferimento), inserisci gli ID degli account AWS a cui desideri trasferire gli indirizzi IP elastici.
7. Conferma il trasferimento inserendo **`enable`** nella casella di testo.
8. Scegli Invia.
9. Per accettare il trasferimento, consulta Accettazione di un indirizzo IP elastico trasferito. Per disabilitare il trasferimento, consulta Disabilitazione del trasferimento di indirizzi IP elastici.

AWS CLI

Abilitazione del trasferimento di indirizzi IP elastici

Utilizza il comando enable-address-transfer.

PowerShell

Abilitazione del trasferimento di indirizzi IP elastici

Utilizza il comando Enable-EC2AddressTransfer.

Disabilitazione del trasferimento di indirizzi IP elastici

Questa sezione descrive come disabilitare un trasferimento di IP elastici dopo averlo abilitato.

Questi passaggi devono essere completati dall'account di origine che ha abilitato il trasferimento.

Console

Disabilitazione del trasferimento di indirizzi IP elastici

1. Assicurati di utilizzare l' AWS account di origine.
2. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

3. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
4. Nell'elenco delle risorse degli IP elastici, assicurati di avere abilitato la proprietà che mostra la colonna Transfer status (Stato del trasferimento).
5. Seleziona uno o più indirizzi IP elastici con Transfer status (Stato del trasferimento) impostato su Pending (In sospeso) e scegli Actions (Azioni), Disable transfer (Disabilita trasferimento).
6. Conferma inserendo **`disable`** nella casella di testo.
7. Scegli Invia.

AWS CLI

Disabilitazione del trasferimento di indirizzi IP elastici

Utilizza il comando disable-address-transfer.

PowerShell

Disabilitazione del trasferimento di indirizzi IP elastici

Utilizza il comando Disable-EC2AddressTransfer.

Accettazione di un indirizzo IP elastico trasferito

Questa sezione descrive come accettare un indirizzo IP elastico trasferito.

Quando si trasferisce un indirizzo IP elastico, viene eseguito un handshake in due passaggi tra gli Account AWS. Quando l'account di origine inizia il trasferimento, gli account di trasferimento hanno sette giorni per accettare il trasferimento dell'indirizzo IP elastico. Durante questi sette giorni, l'account di origine può visualizzare il trasferimento in sospeso (ad esempio nella AWS console o utilizzando il describe-address-transfers AWS CLI comando). Dopo sette giorni, il trasferimento scade e la proprietà dell'indirizzo IP elastico ritorna all'account di origine.

Quando si accettano i trasferimenti, è bene prendere nota delle seguenti eccezioni che potrebbero verificarsi e delle modalità di risoluzione:

- AddressLimitExceeded: Se l'account di trasferimento ha superato la quota di indirizzi IP elastici, l'account di origine può abilitare il trasferimento di indirizzi IP elastici, ma questa eccezione si verifica quando l'account di trasferimento tenta di accettare il trasferimento. Per impostazione predefinita, tutti gli AWS account sono limitati a 5 indirizzi IP elastici per regione. Consulta Quota degli indirizzi IP elastici per le istruzioni su come aumentare il limite.

- InvalidTransfer. AddressCustomPtrSet: Se tu o qualcuno della tua organizzazione avete configurato l'indirizzo IP elastico che state tentando di trasferire per utilizzare la ricerca DNS inversa, l'account di origine può abilitare il trasferimento per l'indirizzo IP elastico, ma questa eccezione si verifica quando l'account di trasferimento tenta di accettare il trasferimento. Per risolvere questo problema, l'account di origine deve rimuovere il record DNS per l'indirizzo IP elastico. Per ulteriori informazioni, consulta Utilizzo del DNS inverso per applicazioni e-mail.
- InvalidTransfer. AddressAssociated: Se un indirizzo IP elastico è associato a un'istanza ENI o EC2, l'account di origine può abilitare il trasferimento per l'indirizzo IP elastico, ma questa eccezione si verifica quando l'account di trasferimento tenta di accettare il trasferimento. Per risolvere questo problema, l'account di origine deve dissociare l'indirizzo IP elastico. Per ulteriori informazioni, consulta Annullare l'associazione di un indirizzo IP elastico.

Per eventuali altre eccezioni, contatta il AWS Support.

Questa procedura deve essere completata dall'account di trasferimento.

Console

Accettazione del trasferimento di un indirizzo IP elastico

1. Assicurati di utilizzare l'account di trasferimento.
2. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
3. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
4. Scegli Actions (Operazioni), Accept transfer (Accetta trasferimento).
5. Quando viene accettato il trasferimento, nessun tag associato all'indirizzo IP elastico da trasferire viene trasferito con l'indirizzo IP elastico. Se desideri definire un tag Name (Nome) per l'indirizzo IP elastico che stai accettando, seleziona Create a tag with a key of 'Name' and a value that you specify (Crea un tag con una chiave "Nome" e un valore da specificare).
6. Inserisci l'indirizzo IP elastico da trasferire.
7. Se stai accettando più indirizzi IP elastici trasferiti, scegli Add address (Aggiungi indirizzo) per inserire un indirizzo IP elastico aggiuntivo.
8. Scegli Invia.

AWS CLI

Accettazione del trasferimento di un indirizzo IP elastico

Utilizza il comando accept-address-transfer.

PowerShell

Accettazione del trasferimento di un indirizzo IP elastico

Utilizza il comando Approve-EC2AddressTransfer.

Rilascio di un indirizzo IP elastico

Se non hai più bisogno di un indirizzo IP elastico, raccomandiamo di rilasciarlo mediante uno dei seguenti metodi. L'indirizzo da rilasciare non deve essere attualmente associato a una AWS risorsa, come un'istanza EC2, un gateway NAT o Network Load Balancer.

> **Note**
>
> Se hai contattato l' AWS assistenza per configurare il DNS inverso per un indirizzo IP elastico (EIP), puoi rimuovere il DNS inverso, ma non puoi rilasciare l'indirizzo IP elastico perché è stato bloccato dall'assistenza. AWS Per sbloccare l'indirizzo IP elastico, contatta AWS Support. Dopo aver sbloccato l'indirizzo IP elastico, puoi rilasciarlo.

Console

per rilasciare un indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico da rilasciare e scegliere Actions (Operazioni), Release Elastic IP address (Rilascia indirizzo IP elastico).
4. Scegliere Release (Rilascia).

AWS CLI

per rilasciare un indirizzo IP elastico

Usa il comando release-address AWS CLI .

PowerShell

per rilasciare un indirizzo IP elastico

Usate il comando. Remove-EC2Address AWS Tools for Windows PowerShell

Recupero di un indirizzo IP elastico

Se hai rilasciato l'indirizzo IP elastico, dovresti riuscire a recuperarlo. Si applicano le regole seguenti:

- Non è possibile recuperare un indirizzo IP elastico se è stato allocato a un altro account AWS ; in caso contrario, si supererà il limite di indirizzi IP elastici.
- Non è possibile recuperare i tag associati all'indirizzo IP elastico.
- È possibile soltanto recuperare un indirizzo IP elastico tramite l'API di Amazon EC2 o lo strumento a riga di comando.

AWS CLI

Per recuperare un indirizzo IP elastico

Utilizzate il AWS CLI comando allocate-address e specificate l'indirizzo IP utilizzando il `--address` parametro come segue.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

PowerShell

Per recuperare un indirizzo IP elastico

Utilizzate il New-EC2Address AWS Tools for Windows PowerShell comando e specificate l'indirizzo IP utilizzando il `-Address` parametro come segue.

```
PS C:\> New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

Utilizzo del DNS inverso per applicazioni e-mail

Se si intende inviare messaggi e-mail a terzi da un'istanza, consigliamo di eseguire il provisioning di uno o più indirizzi IP elastici e assegnare record DNS inversi statici agli indirizzi IP elastici utilizzati per inviare l'e-mail. In questo modo è possibile evitare che la posta elettronica venga contrassegnata come posta indesiderata da alcune organizzazioni antispam. AWS collabora con gli ISP e le organizzazioni anti-spam su Internet per ridurre la possibilità che le e-mail inviate da questi indirizzi vengano contrassegnate come spam.

Considerazioni

- Prima di creare un record DNS inverso, è necessario impostare un record DNS forward corrispondente (record tipo A) che punta all'indirizzo IP elastico.
- Se un record DNS inverso viene associato a un indirizzo IP elastico, l'indirizzo IP elastico è bloccato per l'account e non potrà essere rilasciato dall'account finché non verrà rimosso il record.
- AWS GovCloud (US) Region

  Non è possibile creare un record DNS inverso utilizzando la console o. AWS CLI AWS deve assegnare i record DNS inversi statici per te. Apri Request to remove reverse DNS and email sending limitations (Richiesta di rimuovere i limiti di invio e-mail e DNS inversi) e specifica gli indirizzi IP elastici e i record DNS inversi.

Creazione di un record DNS inverso

Per creare un record DNS inverso, scegli la scheda che corrisponde al tuo metodo preferito.

Console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Seleziona l'indirizzo IP elastico e scegli Actions (Operazioni), quindi Update reverse DNS (Aggiorna DNS inverso).
4. Per Reverse DNS Domain Name (Nome di dominio di DNS inverso), inserire il nome di dominio.
5. Immettere **`update`** per confermare.
6. Scegliere Update (Aggiorna).

AWS CLI

Utilizzate il modify-address-attribute comando in AWS CLI, come illustrato nell'esempio seguente:

```
aws ec2 modify-address-attribute --allocation-id eipalloc-abcdef01234567890  --
domain-name example.com
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
```

```
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net."
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
        }
    ]
}
```

Rimozione di un registro DNS inverso

Per rimuovere un registro DNS inverso, scegli la scheda che corrisponde al tuo metodo preferito.

Console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Seleziona l'indirizzo IP elastico e scegli Actions (Operazioni), quindi Update reverse DNS (Aggiorna DNS inverso).
4. Per Reverse DNS Domain Name (Nome di dominio di DNS inverso), rimuovi il nome di dominio.
5. Immettere **`update`** per confermare.
6. Scegliere Update (Aggiorna).

AWS CLI

Utilizzate il reset-address-attribute comando in AWS CLI, come illustrato nell'esempio seguente:

```
aws ec2 reset-address-attribute --allocation-id eipalloc-abcdef01234567890 --
attribute domain-name
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com."
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
```

```
        }
    ]
}
```

> **Note**
>
> Se ricevi il seguente errore quando esegui il comando, puoi inviare una richiesta per rimuovere le limitazioni all'invio di e-mail a cui AWS Support richiedere assistenza. L'indirizzo con ID di allocazione non può essere rilasciato perché è bloccato sull'account.

Quota degli indirizzi IP elastici

Per impostazione predefinita, tutti AWS gli account hanno una quota di cinque (5) indirizzi IP elastici per regione, poiché gli indirizzi Internet pubblici (IPv4) sono una risorsa pubblica scarsa. Incoraggiamo fortemente l'utilizzo di un indirizzo IP elastico, per la possibilità di rimappare l'indirizzo su un'altra istanza in caso di fallimento dell'istanza. Inoltre, permette l'utilizzo di hostname DNS per tutte le altre comunicazioni internodo.

Per verificare quanti indirizzi IP elastici sono in uso

Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/ e scegliere Elastic IPs (IP elastici) dal pannello di navigazione.

Verifica della quota corrente di indirizzi IP elastici per l'account

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/.
2. Nella barra di navigazione, nella parte superiore della schermata, seleziona una regione.
3. Nel pannello di controllo, selezionare Amazon Elastic Compute Cloud (Amazon EC2).

   Se Amazon Elastic Compute Cloud (Amazon EC2) non è riportato nel pannello di controllo, selezionare Servizi AWS , immettere **`EC2`** nel campo di ricerca e scegliere quindi Amazon Elastic Compute Cloud (Amazon EC2).
4. Nella pagina Quote di servizio Amazon EC2 immettere **`IP`** nel campo di ricerca. Il limite è EC2-VPC Elastic IPs (IP elastici EC2-VPC). Per ulteriori informazioni, selezionare il limite.

Se si ritiene che l'architettura richieda ulteriori indirizzi IP elastici, è possibile chiedere un aumento delle quote direttamente dalla console Service Quotas. Per richiedere un aumento della quota, è

possibile richiedere un aumento a livello di account. Per ulteriori informazioni, consulta Service Quotas di Amazon EC2.

Interfacce di rete elastiche

Un'interfaccia di rete elastica è un componente di rete logico in un VPC che rappresenta una scheda di rete virtuale. Può includere gli attributi seguenti:

- Un indirizzo IPv4 privato primario dall'intervallo di indirizzi IPv4 del VPC
- Un indirizzo IPv6 primario dall'intervallo di indirizzi IPv6 del VPC
- Uno o più indirizzi IPv4 privati secondari dall'intervallo di indirizzi IPv4 del VPC
- Un indirizzo IP elastico (IPv4) per indirizzo IPv4 privato
- Un indirizzo IPv4 pubblico
- Uno o più indirizzi IPv6
- Uno o più gruppi di sicurezza
- Un indirizzo MAC
- Un flag di controllo di origine/destinazione
- Una descrizione

Dovrai collegare un'interfaccia di rete a un'istanza nella stessa zona di disponibilità. L'account potrebbe anche disporre di interfacce di rete gestite dai richiedenti, create e gestite dai AWS servizi per consentire all'utente di utilizzare altre risorse e servizi. Non puoi gestire queste interfacce di rete in autonomia. Per ulteriori informazioni, consulta Interfacce di rete gestite dal richiedente.

Questa AWS risorsa viene definita interfaccia di rete nell' AWS Management Console API Amazon EC2. Pertanto, in questa documentazione utilizziamo "interfaccia di rete" anziché "interfaccia di rete elastica". Il termine "interfaccia di rete" in questa documentazione significa sempre "interfaccia di rete elastica".

Indice

- Best practice per la configurazione delle interfacce di rete
- Scenari per le interfacce di rete
- Interfacce di rete gestite dal richiedente
- Assegna prefissi alle interfacce di rete Amazon EC2

Informazioni di base sull'interfaccia di rete

Puoi creare un'interfaccia di rete elastica, collegarla a un'istanza, scollegarla da un'istanza e collegarla a un'altra istanza. Gli attributi di un'interfaccia di rete dipendono dal fatto che sia collegata a o scollegata da un'istanza e quindi ricollegata a un'altra istanza. Quando trasferisci un'istanza di rete da un'istanza a un'altra, il traffico di rete viene reindirizzato alla nuova istanza.

Interfaccia di rete primaria

Ogni istanza dispone di un'interfaccia di rete predefinita, denominata interfaccia di rete primaria. Non puoi scollegare un'interfaccia di rete primaria da un'istanza. Puoi creare e collegare interfacce di rete aggiuntive. Il numero massimo di interfacce di rete che puoi usare varia a seconda del tipo di istanza. Per ulteriori informazioni, consulta Indirizzi IP per interfaccia di rete per tipo di istanza.

Indirizzi IPv4 pubblici per le interfacce di rete

In un VPC, tutte le sottoreti hanno un attributo modificabile che determina se alle interfacce di rete create in tale sottorete e pertanto alle istanze avviate in quella sottorete viene assegnato un indirizzo IPv4 pubblico. Per ulteriori informazioni, consulta Impostazioni della sottorete nella Guida per l'utente di Amazon VPC. L'indirizzo IPv4 pubblico viene assegnato dal pool di indirizzi IPv4 pubblici di Amazon. Quando avvii un'istanza, l'indirizzo IP viene assegnato all'interfaccia di rete primaria creata.

Quando crei un'interfaccia di rete, essa eredita l'attributo di indirizzamento IPv4 pubblico dalla sottorete. Se modifichi l'attributo di indirizzamento IPv4 pubblico della sottorete in un secondo momento, l'interfaccia di rete conserva l'impostazione valida al momento della sua creazione. Se avvii un'istanza e specifichi un'interfaccia di rete esistente come interfaccia di rete primaria, l'attributo indirizzo IPv4 pubblico viene determinato da questa interfaccia di rete.

Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici.

Indirizzi IP elastici per l'interfaccia di rete

Se disponi di un indirizzo IP elastico, puoi associarlo a uno o più indirizzi IPv4 privati per l'interfaccia di rete. Puoi associare un indirizzo IP elastico a ciascun indirizzo IPv4 privato.

Se si annulla l'associazione di un indirizzo IP elastico da un'interfaccia di rete, è possibile rilasciarlo nuovamente al pool di indirizzi. Questo è l'unico modo per associare un indirizzo IP elastico a un'istanza in una sottorete o VPC diversa, poiché le interfacce di rete sono specifiche per le sottoreti.

Indirizzi IPv6 pubblici per le interfacce di rete

Puoi associare blocchi CIDR IPv6 al VPC e alla sottorete e assegnare uno o più indirizzi IPv6 in base all'intervallo della sottorete a un'interfaccia di rete. Ciascun indirizzo IPv6 può essere assegnato a un'interfaccia di rete.

Tutte le sottoreti hanno un attributo modificabile che determina se alle interfacce di rete create in tale sottorete e pertanto alle istanze avviate in quella sottorete viene automaticamente assegnato un indirizzo IPv6 in base all'intervallo della sottorete. Per ulteriori informazioni, consulta Impostazioni della sottorete nella Guida per l'utente di Amazon VPC. Quando avvii un'istanza, l'indirizzo IPv6 viene assegnato all'interfaccia di rete primaria creata.

Per ulteriori informazioni, consulta Indirizzi IPv6.

Delega prefisso

Un prefisso per la delega del prefisso è un intervallo CIDR IPv4 o IPv6 privato riservato allocato per l'assegnazione automatica o manuale alle interfacce di rete associate a un'istanza. Utilizzando i prefissi delegati, è possibile avviare i servizi più rapidamente assegnando un intervallo di indirizzi IP come un prefisso unico.

Comportamento risoluzione

Puoi impostare il comportamento di interruzione per un'interfaccia di rete collegata a un'istanza. Puoi specificare se l'interfaccia di rete deve essere eliminata automaticamente quando cessi l'istanza a cui è collegata.

Controllo dell'origine/della destinazione

Puoi attivare o disattivare i controlli di origine e destinazione in modo da garantire che l'istanza sia l'origine o la destinazione di qualsiasi traffico che riceve. Il controllo dell'origine/della destinazione è abilitato per impostazione predefinita. È necessario disattivare i controlli di origine/destinazione se l'istanza esegue servizi quali la conversione degli indirizzi di rete, routing o firewall.

Monitoraggio del traffico IP

Puoi abilitare il log del flusso di un VPC sull'interfaccia di rete in modo che vengano acquisite le informazioni sul traffico IP a livello di interfaccia di rete. Dopo aver creato un log di flusso, puoi

visualizzarne e recuperarne i dati in Amazon CloudWatch Logs. Per ulteriori informazioni, consulta Log di flusso VPC nella Guida per l'utente di Amazon VPC.

Assegnazione automatica di indirizzi IPv4 pubblici

È possibile abilitare e disabilitare l'assegnazione automatica di un indirizzo IPv4 pubblico a un'interfaccia di rete. Questa opzione può essere abilitata per qualsiasi interfaccia di rete, ma si applica solo all'interfaccia di rete principale (eth0). Per ulteriori informazioni, consulta Gestire gli indirizzi IP.

Schede di rete

Le istanze con più schede di rete offrono prestazioni di rete superiori, tra cui capacità di larghezza di banda superiore a 100 Gb/s e prestazioni migliorate per la velocità dei pacchetti. Ogni interfaccia di rete è collegata a una scheda di rete. L'interfaccia di rete primaria deve essere assegnata all'indice della scheda di rete 0.

Se si attiva Elastic Fabric Adapter (EFA) (EFA) quando si avvia un'istanza che supporta più schede di rete, sono disponibili tutte le schede di rete. È possibile assegnare fino a un EFA per scheda di rete. Un EFA conta come un'interfaccia di rete.

Le istanze seguenti supportano più schede di rete. Tutti gli altri tipi di istanza supportano una scheda di rete.

Tipo di istanza	Numero di schede di rete
c6in.32xlarge	2
c6in.metal	2
dl1.24xlarge	4
hpc6id.32xlarge	2
hpc7a.12xlarge	2
hpc7a.24xlarge	2
hpc7a.48xlarge	2
hpc7a.96xlarge	2

Tipo di istanza	Numero di schede di rete
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2
p4d.24xlarge	4
p4de.24xlarge	4
p5.48xlarge	32
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8
trn1n.32xlarge	16
u7in-16tb.224xlarge	2
u7in-24tb.224xlarge	2
u7in-32tb.224xlarge	2

Indirizzi IP per interfaccia di rete per tipo di istanza

Ogni tipo di istanza supporta un numero massimo di interfacce di rete, il numero massimo di indirizzi IPv4 privati per interfaccia di rete e il numero massimo di indirizzi IPv6 per interfaccia di rete. Il limite relativo agli indirizzi IPv6 è diverso da quello relativo agli indirizzi IPv4 privati per interfaccia di rete. Non tutti i tipi di istanza supportano l'indirizzamento IPv6.

Interfacce di rete disponibili

La Amazon EC2 Instance Types Guide fornisce informazioni sulle interfacce di rete disponibili per ogni tipo di istanza. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Specifiche di rete: scopo generale
- Specifiche di rete: ottimizzate per il calcolo
- Specifiche di rete: memoria ottimizzata
- Specifiche di rete: archiviazione ottimizzata
- Specifiche di rete: elaborazione accelerata
- Specifiche di rete: elaborazione ad alte prestazioni
- Specifiche di rete: generazione precedente

Per recuperare le informazioni sull'interfaccia di rete utilizzando il AWS CLI

È possibile utilizzare il describe-instance-types AWS CLI comando per visualizzare informazioni su un tipo di istanza, ad esempio le interfacce di rete supportate e gli indirizzi IP per interfaccia. Nell'esempio seguente vengono visualizzate queste informazioni per tutte le istanze C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].{ \
        Type: InstanceType, \
        MaxENI: NetworkInfo.MaximumNetworkInterfaces, \
        IPv4addr: NetworkInfo.Ipv4AddressesPerInterface}" \
    --output table
```

Output previsto

```
-------------------------------------
|       DescribeInstanceTypes       |
+----------+----------+--------------+
| IPv4addr | MaxENI   |     Type     |
+----------+----------+--------------+
|  30      |  8       |  c5.4xlarge  |
|  50      |  15      |  c5.24xlarge |
|  15      |  4       |  c5.xlarge   |
|  30      |  8       |  c5.12xlarge |
```

```
|  10      |  3       |  c5.large     |
|  15      |  4       |  c5.2xlarge   |
|  50      |  15      |  c5.metal     |
|  30      |  8       |  c5.9xlarge   |
|  50      |  15      |  c5.18xlarge  |
+----------+----------+---------------+
```

Per recuperare le informazioni sull'interfaccia di rete utilizzando il AWS Tools for PowerShell

È possibile utilizzare il Get-EC2InstanceType PowerShell comando per visualizzare informazioni su un tipo di istanza, ad esempio le interfacce di rete supportate e gli indirizzi IP per interfaccia. Nell'esempio seguente vengono visualizzate queste informazioni per tutte le istanze C5.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
Select-Object `
    @{Name = 'Ipv4AddressesPerInterface'; Expression =
 {($_.Networkinfo.Ipv4AddressesPerInterface)}},
    @{Name = 'MaximumNetworkInterfaces'; Expression =
 {($_.Networkinfo.MaximumNetworkInterfaces)}},
    InstanceType | `
Format-Table -AutoSize
```

Output previsto

```
Ipv4AddressesPerInterface MaximumNetworkInterfaces InstanceType
------------------------- ------------------------ ------------
                       30                        8 c5.4xlarge
                       15                        4 c5.xlarge
                       30                        8 c5.12xlarge
                       50                       15 c5.24xlarge
                       30                        8 c5.9xlarge
                       50                       15 c5.metal
                       15                        4 c5.2xlarge
                       10                        3 c5.large
                       50                       15 c5.18xlarge
```

Utilizzo delle interfacce di rete

Puoi utilizzare le interfacce di rete mediante la console Amazon EC2 o la riga di comando.

Indice

Creazione di un'interfaccia di rete

Puoi creare un'interfaccia di rete in una sottorete. Una volta creata, non potrai spostare l'interfaccia di rete in un'altra sottorete. Dovrai collegare un'interfaccia di rete a un'istanza nella stessa zona di disponibilità.

Per creare un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona Crea interfaccia di rete.
4. (Facoltativo) In Descrizione, immetti un nome descrittivo.
5. Per Subnet (Sottorete), selezionare una sottorete. Le opzioni disponibili nelle fasi successive cambiano a seconda del tipo di sottorete selezionato (solo IPv4, solo IPv6 o dual-stack [IPv4 e IPv6]).
6. In Private IPv4 address (Indirizzo IPv4 privato), completa una delle seguenti operazioni:
   - Scegli Assegnazione automatica per consentire a Amazon EC2 di selezionare un indirizzo IPv4 dalla sottorete.
   - Scegli Personalizzato e immetti un indirizzo IPv4 selezionato dalla sottorete.
7. (Solo sottoreti con indirizzi IPv6) Per Indirizzo IPv6, completa una delle seguenti operazioni:
   - Scegli Nessuno se non desideri assegnare un indirizzo IPv6 all'interfaccia di rete.
   - Scegli Assegnazione automatica per consentire a Amazon EC2 di selezionare un indirizzo IPv6 dalla sottorete.
   - Scegli Personalizzato e immetti un indirizzo IPv6 selezionato dalla sottorete.

8. (Facoltativo) Se stai creando un'interfaccia di rete in una sottorete dual-stack o solo IPv6, hai la possibilità diAssegna IP IPv6 primario. Questo assegna un indirizzo unicast globale IPv6 (GUA) primario all'interfaccia di rete. L'assegnazione di un indirizzo IPv6 primario consente di evitare l'interruzione del traffico verso istanze o ENI. Scegli Abilita se l'istanza a cui verrà collegato questo ENI si basa sul fatto che il suo indirizzo IPv6 non cambi. AWS assegnerà automaticamente un indirizzo IPv6 associato all'ENI collegato all'istanza come indirizzo IPv6 principale. Dopo aver abilitato un indirizzo GUA IPv6 come IPv6 primario, non è possibile disattivarlo. Quando si abilita un indirizzo GUA IPv6 come IPv6 primario, la prima GUA IPv6 verrà impostata come indirizzo IPv6 primario fino alla chiusura dell'istanza o alla disconnessione dell'interfaccia di rete. Se disponi di più indirizzi IPv6 associati a un ENI collegato all'istanza e abiliti un indirizzo IPv6 primario, il primo indirizzo GUA IPv6 associato all'ENI diventa l'indirizzo IPv6 primario.
9. (Facoltativo) Per creare un Elastic Fabric Adapter (EFA), scegli Elastic Fabric Adapter (EFA), Attiva.
10. (Facoltativo) In Impostazioni avanzate, per Timeout di tracciamento della connessione inattiva, modifica i timeout di connessione inattiva predefiniti. Per ulteriori informazioni su queste opzioni, consulta Timeout di tracciamento delle connessioni inattive.

    - Timeout TCP stabilito: il timeout (in secondi) per le connessioni TCP inattive in uno stato stabilito. Minimo: 60 secondi. Massimo: 432.000 secondi (5 giorni). Valore predefinito: 432.000 secondi. Consigliato: meno di 432.000 secondi.
    - Timeout UDP: il timeout (in secondi) per i flussi UDP inattivi che hanno registrato traffico solo in un'unica direzione o una singola transazione richiesta-risposta. Minimo: 30 secondi. Massimo 60 secondi. Valore predefinito: 30 secondi.
    - Timeout del flusso UDP: il timeout (in secondi) per i flussi UDP inattivi classificati come flussi che hanno registrato più di una transazione richiesta-risposta. Minimo: 60 secondi. Massimo: 180 secondi (3 minuti). Valore predefinito: 180 secondi.
11. In Security groups (Gruppi di sicurezza), selezionare uno o più gruppi di sicurezza.
12. (Facoltativo) Per ogni tag, seleziona Aggiungi nuovo tag e specifica una chiave tag e un valore di tag facoltativo.
13. Seleziona Crea interfaccia di rete.

Per creare un'interfaccia di rete utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- create-network-interface (AWS CLI)
- New-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Visualizzazione dei dettagli relativi a un'interfaccia virtuale

Puoi visualizzare tutte le interfacce di rete incluse nel tuo account.

Per visualizzare la descrizione di un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Per visualizzare la pagina dei dettagli di un'interfaccia di rete, seleziona l'ID dell'interfaccia di rete. In alternativa, per visualizzare le informazioni senza uscire dalla pagina delle interfacce di rete, seleziona la casella di controllo relativa all'interfaccia di rete.

Per visualizzare la descrizione di un'interfaccia di rete utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Per visualizzare la descrizione di un attributo di un'interfaccia di rete utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- describe-network-interface-attribute (AWS CLI)
- Get-EC2NetworkInterfaceAttribute (AWS Tools for Windows PowerShell)

Collegamento di un'interfaccia di rete a un'istanza

Puoi collegare un'interfaccia di rete a qualsiasi istanza nella stessa zona di disponibilità dell'interfaccia di rete, utilizzando la pagina Istanze o Interfacce di rete della console Amazon EC2. In alternativa, puoi specificare interfacce di rete esistenti all'avvio delle istanze.

> **Important**
>
> Per le istanze EC2 in una sottorete solo IPv6, se si collega un'interfaccia di rete secondaria all'istanza, il nome host DNS privato della seconda interfaccia di rete verrà risolto al primo indirizzo IPv6 sulla prima interfaccia di rete dell'istanza. Per ulteriori informazioni sui nomi host DNS privati delle istanze EC2, consultare Tipi di nomi host delle istanze Amazon EC2.

Se l'indirizzo IPv4 pubblico sull'istanza viene rilasciato, l'istanza non ne riceverà uno nuovo se è presente più di un'interfaccia di rete collegata all'istanza. Per ulteriori informazioni sul funzionamento degli indirizzi IPv4 pubblici, consulta Indirizzi IPv4 pubblici.

Instances page

Per collegare un'interfaccia di rete a un'istanza utilizzando la pagina Instances (Istanze)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona la casella di controllo relativa all'istanza.
4. Scegliere Actions (Operazioni), Networking (Reti), Attach network interface (Collega interfaccia di rete).
5. Selezione di un VPC. Se colleghi un'interfaccia di rete secondaria all'istanza, l'interfaccia di rete può risiedere nello stesso VPC dell'istanza o in un altro VPC di tua proprietà (purché l'interfaccia di rete si trovi in una sottorete che si trova nella stessa zona di disponibilità dell'istanza). Ciò consente di creare istanze multi-homed su VPC con configurazioni di rete e sicurezza differenti.
6. Selezionare un'interfaccia di rete. Se l'istanza supporta più schede di rete, è possibile scegliere una scheda di rete.
7. Scegliere Attach (Collega).

Network Interfaces page

Per collegare un'interfaccia di rete a un'istanza utilizzando la pagina Network Interfaces (Interfacce di rete)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).

3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Seleziona Operazioni, Collega volume.
5. Scegli un'istanza. Se l'istanza supporta più schede di rete, è possibile scegliere una scheda di rete.
6. Scegliere Attach (Collega).

Per collegare un'interfaccia di rete a un'istanza utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

> **Note**
>
> Puoi collegare un'interfaccia di rete che si trova in un altro VPC (ma nella stessa zona di disponibilità) a un'istanza utilizzando il attach-network-interface AWS CLI comando. Non è possibile eseguire questa operazione utilizzando. AWS Management Console

- attach-network-interface (AWS CLI)
- Add-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Scollegamento di un'interfaccia di rete da un'istanza

Puoi scollegare un'interfaccia di rete secondaria collegata a un'istanza EC2 in qualsiasi momento utilizzando la pagina Instances (Istanze) o Network Interfaces (Interfacce di rete) della console Amazon EC2.

Se si tenta di scollegare un'interfaccia di rete collegata a una risorsa da un altro servizio, ad esempio un sistema di bilanciamento del carico Elastic Load Balancing, una funzione Lambda, un o WorkSpace un gateway NAT, viene visualizzato un errore che indica che non si dispone dell'autorizzazione per accedere alla risorsa. Per individuare quale servizio ha creato la risorsa collegata a un'interfaccia di rete, controlla la descrizione dell'interfaccia di rete. Se si elimina la risorsa, viene eliminata anche la sua interfaccia di rete.

Instances page

Per scollegare un'interfaccia di rete da un'istanza utilizzando la pagina Instances (Istanze)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona la casella di controllo relativa all'istanza. Controlla la sezione Interfacce di rete della scheda Rete per verificare che l'interfaccia dell'istanza di rete sia collegata a un'istanza come interfaccia di rete secondaria.
4. Scegliere Actions (Operazioni), Networking (Reti), Detach network interface (Scollega interfaccia di rete).
5. Selezionare l'interfaccia di rete e scegliere Detach (Scollega).

Network Interfaces page

Per scollegare un'interfaccia di rete da un'istanza utilizzando la pagina Network Interfaces (Interfacce di rete)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete. Controlla la sezione Dettagli istanza della scheda Dettagli per verificare che l'interfaccia dell'istanza di rete sia collegata a un'istanza come interfaccia di rete secondaria.
4. Seleziona Operazioni, Elimina.
5. Quando viene richiesta la conferma, seleziona Detach (Scollega).
6. Se non è possibile scollegare l'interfaccia di rete dall'istanza, seleziona Forza scollegamento, Attiva, quindi riprova. Si consiglia di forzare lo scollegamento solo come ultima risorsa.
   La forzatura di uno scollegamento può impedire di collegare un'interfaccia di rete diversa sullo stesso indice fino a quando non si riavvia l'istanza. Può anche impedire ai metadati dell'istanza di mostrare che l'interfaccia di rete è stata scollegata fino a quando non si riavvia l'istanza.

Per scollegare un'interfaccia di rete utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- detach-network-interface (AWS CLI)
- Dismount-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Gestire gli indirizzi IP

È possibile gestire i seguenti indirizzi IP per le interfacce di rete:

- indirizzi IP elastici (uno per indirizzo IPv4 privato)
- Indirizzi IPv4
- Indirizzi IPv6
- Indirizzo IPv6 primario

Per gestire gli indirizzi IP elastici di un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Per associare un indirizzo IP elastico, effettuare le seguenti operazioni:
    a. Quindi seleziona Actions (Operazioni), Associate address (Associa indirizzo).
    b. In Indirizzo, seleziona l'indirizzo IP elastico.
    c. Per Indirizzo IPv4 privato, seleziona l'indirizzo IPv4 privato da associare all'indirizzo IP elastico.
    d. (Facoltativo) Seleziona Consenti di riassociare l'indirizzo IP elastico se l'interfaccia di rete è attualmente associata a un'altra istanza o interfaccia di rete.
    e. Seleziona Associate (Associa).
5. Per disassociare un indirizzo IP elastico, effettuare le seguenti operazioni:
    a. Selezionare Actions (Operazioni), scegliere Disassociate address (Disassocia indirizzo).
    b. In Indirizzo IP pubblico, seleziona l'indirizzo IP elastico.
    c. Selezionare Disassociate (Annulla associazione).

Per gestire gli indirizzi IPv4 e IPv6 di un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Selezionare l'interfaccia di rete.
4. Seleziona Operazioni, Gestisci indirizzi IP.
5. Espandere l'interfaccia di rete.
6. Per Indirizzi IPv4, modifica gli indirizzi IP in base alle esigenze. Per assegnare un indirizzo IPv4, scegli Assegna nuovo indirizzo IP, quindi specifica un indirizzo IPv4 dall'intervallo di sottoreti o lascia che ne scelga uno per te. AWS Per annullare l'assegnazione di un indirizzo IPv4, scegliere Unassign (Annulla assegnazione) accanto all'indirizzo.
7. Per assegnare o annullare l'assegnazione di un indirizzo IPv4 pubblico a un'interfaccia di rete, scegli Assegna automaticamente IP pubblico. Questa opzione può essere abilitata o disabilitata per qualsiasi interfaccia di rete, ma si applicherà solo all'interfaccia di rete principale (eth0).
8. Per Indirizzi IPv6, modifica gli indirizzi IP in base alle esigenze. Per assegnare un indirizzo IPv6, scegli Assegna nuovo indirizzo IP, quindi specifica un indirizzo IPv6 dall'intervallo di sottorete o lascia che ne scelga uno per te. AWS Per annullare l'assegnazione di un indirizzo IPv6, scegliere Unassign (Annulla assegnazione) accanto all'indirizzo.
9. (Facoltativo) Se stai modificando un'interfaccia di rete in una sottorete dual-stack o solo IPv6, hai la possibilità diAssegna IP IPv6 primario. L'assegnazione di un indirizzo IPv6 primario consente di evitare l'interruzione del traffico verso istanze o ENI. Scegli Abilita se l'istanza a cui verrà collegato questo ENI si basa sul fatto che il suo indirizzo IPv6 non cambia. AWS assegnerà automaticamente un indirizzo IPv6 associato all'ENI collegato all'istanza come indirizzo IPv6 principale. Dopo aver abilitato un indirizzo GUA IPv6 come IPv6 primario, non è possibile disattivarlo. Quando si abilita un indirizzo GUA IPv6 come IPv6 primario, la prima GUA IPv6 verrà impostata come indirizzo IPv6 primario fino alla chiusura dell'istanza o alla disconnessione dell'interfaccia di rete. Se disponi di più indirizzi IPv6 associati a un ENI collegato all'istanza e abiliti un indirizzo IPv6 primario, il primo indirizzo GUA IPv6 associato all'ENI diventa l'indirizzo IPv6 primario.
10. Selezionare Salva.

Per gestire gli indirizzi IP di un'interfaccia di rete utilizzando il AWS CLI

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- assign-ipv6-addresses
- associate-address

- disassociate-address
- unassign-ipv6-addresses

Per gestire gli indirizzi IP di un'interfaccia di rete utilizzando gli Strumenti per Windows PowerShell

È possibile utilizzare uno dei seguenti comandi.

- Register-EC2Address
- Register-EC2Ipv6 AddressList
- Unregister-EC2Address
- Unregister-EC2Ipv6 AddressList

Modifica degli attributi dell'interfaccia di rete

È possibile modificare i seguenti attributi dell'interfaccia di rete:

- Descrizione
- Gruppi di sicurezza
- Elimina al termine
- Controllo dell'origine/della destinazione

Per modificare la descrizione di un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Scegli Operazioni, Modifica descrizione.
5. In Descrizione, immetti una descrizione per l'interfaccia di rete.
6. Seleziona Salva.

Per modificare i gruppi di sicurezza di un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Seleziona Operazioni, Gestisci gruppi di sicurezza.
5. In Modifica gruppi di sicurezza, seleziona i gruppi di sicurezza da utilizzare, quindi seleziona Salva.

   Il gruppo di protezione e l'interfaccia di rete devono essere creati per lo stesso VPC. Per modificare il gruppo di protezione per le interfacce di proprietà di altri servizi, ad esempio Elastic Load Balancing, eseguire questa operazione tramite tale servizio.

Per modificare il comportamento di interruzione per un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Seleziona Operazioni, Modifica comportamento di risoluzione.
5. Seleziona o deseleziona Elimina in caso di risoluzione, Attiva a seconda del caso, quindi scegli Salva.

Per modificare il controllo dell'origine/della destinazione per un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Seleziona Operazioni, Modifica controllo origine/destinazione.
5. Seleziona o deseleziona Controllo origine/destinazione, Attiva a seconda del caso, quindi scegli Salva.

Per modificare i timeout di tracciamento delle connessioni inattive:

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Scegli Operazioni, Modifica il timeout di connessione.
5. Modifica i timeout di tracciamento delle connessioni inattive. Per ulteriori informazioni su queste opzioni, consulta Timeout di tracciamento delle connessioni inattive.

   - Timeout TCP stabilito: il timeout (in secondi) per le connessioni TCP inattive in uno stato stabilito. Minimo: 60 secondi. Massimo: 432.000 secondi (5 giorni). Valore predefinito: 432.000 secondi. Consigliato: meno di 432.000 secondi.
   - Timeout UDP: il timeout (in secondi) per i flussi UDP inattivi che hanno registrato traffico solo in un'unica direzione o una singola transazione richiesta-risposta. Minimo: 30 secondi. Massimo 60 secondi. Valore predefinito: 30 secondi.
   - Timeout del flusso UDP: il timeout (in secondi) per i flussi UDP inattivi classificati come flussi che hanno registrato più di una transazione richiesta-risposta. Minimo: 60 secondi. Massimo: 180 secondi (3 minuti). Valore predefinito: 180 secondi.
6. Selezionare Salva.

Per modificare gli attributi dell'interfaccia di rete tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- modify-network-interface-attribute (AWS CLI)
- Edit-EC2NetworkInterfaceAttribute (AWS Tools for Windows PowerShell)

Aggiungere o modificare i tag

I tag sono metadati che puoi aggiungere a un'interfaccia di rete. I tag sono elementi privati e sono visibili solo dal tuo account. Ciascun tag è formato da una chiave e da un valore opzionale. Per ulteriori informazioni sui tag, consulta Tagging delle risorse Amazon EC2..

Per aggiungere o modificare i tag per un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.

4. Nella scheda Tag, seleziona Gestisci tag.
5. Per ogni tag da creare, scegli Aggiungi nuovo tag e specifica una chiave e un valore facoltativo. Al termine, scegliere Save (Salva).

Per aggiungere o modificare i tag per un'interfaccia di rete utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Eliminazione di un'interfaccia di rete

L'eliminazione di un'interfaccia di rete rilascia tutti gli attributi associati all'interfaccia e gli indirizzi IP privati o gli indirizzi IP elastici utilizzati da un'altra istanza.

Non è possibile eliminare un'interfaccia di rete in uso. Innanzitutto, è necessario Scollegare l'interfaccia di rete.

Per eliminare un'interfaccia di rete utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo dell'interfaccia di rete, quindi seleziona Operazioni, Elimina.
4. Quando viene richiesta la conferma, seleziona Elimina.

Per eliminare un'interfaccia di rete utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- delete-network-interface (AWS CLI)
- Remove-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Best practice per la configurazione delle interfacce di rete

- Puoi collegare un'interfaccia di rete a un'istanza quando è in esecuzione (collegamento a caldo), quando è arrestata (collegamento standard) o quando l'istanza viene avviata (collegamento a freddo).
- Puoi scollegare le interfacce di rete secondarie quando l'istanza è in esecuzione o arrestata. Non puoi tuttavia distaccare l'interfaccia di rete primaria.
- Puoi spostare un'interfaccia di rete secondaria da un'istanza a un'altra, se le istanze sono nella stessa zona di disponibilità e nello stesso VPC ma in sottoreti differenti.
- Quando avvii un'istanza utilizzando la CLI, l'API o un SDK, è possibile specificare l'interfaccia di rete primaria e interfacce di rete aggiuntive.
- L'avvio di un'istanza Amazon Linux o Windows Server con più interfacce di rete configura automaticamente le interfacce, gli indirizzi IPv4 privati e le tabelle di routing sul sistema operativo dell'istanza.
- Un collegamento di tipo warm o hot di un'interfaccia di rete aggiuntiva potrebbe richiedere l'implementazione manuale di una seconda interfaccia, la configurazione dell'indirizzo IPv4 privato e la modifica della tabella di routing. Le istanze che eseguono Amazon Linux o Windows Server riconoscono automaticamente il collegamento di tipo warm o a caldo ed eseguono automaticamente la configurazione.
- Non è possibile collegare un'altra interfaccia di rete a un'istanza (ad esempio una configurazione di un gruppo di NIC) per aumentare o raddoppiare la larghezza di banda della rete dalla o all'istanza dual-homed.
- Se colleghi due o più interfacce di rete della stessa sottorete a un'istanza, potresti riscontrare errori a livello di rete, ad esempio il routing asimmetrico. Se possibile, utilizza invece un indirizzo IPv4 privato secondario sull'interfaccia di rete primaria.
- Istanze Windows: se si utilizzano più interfacce di rete, è necessario configurare le interfacce di rete per utilizzare il routing statico.

Configurazione dell'interfaccia di rete tramite ec2-net-utils per Amazon Linux 2

> **Note**
>
> Per AL2023, il pacchetto `amazon-ec2-net-utils` genera configurazioni specifiche dell'interfaccia nella directory `/run/systemd/network`. Per ulteriori informazioni, consulta la sezione Servizio di rete nella Guida per l'utente di Amazon Linux 2023.

Le AMI Amazon Linux 2 possono contenere script aggiuntivi installati da AWS, noti come ec2-net-utils. Questi script automatizzano facoltativamente la configurazione delle interfacce di rete. Questi script sono disponibili solo per Amazon Linux 2.

Utilizza il seguente comando per installare il pacchetto su Amazon Linux 2 se non è già installato oppure per aggiornarlo se è installato e risultano disponibili aggiornamenti aggiuntivi:

```
$ yum install ec2-net-utils
```

I seguenti componenti fanno parte di ec2-net-utils:

Regole udev (`/etc/udev/rules.d`)

Identifica le interfacce di rete quando vengono collegate, scollegate o ricollegate a un'istanza in esecuzione e assicura che lo script hotplug venga eseguito (`53-ec2-network-interfaces.rules`). Esegue la mappatura dell'indirizzo MAC a un nome di dispositivo (`75-persistent-net-generator.rules`, che genera `70-persistent-net.rules`).

Script hotplug

Genera un file di configurazione dell'interfaccia idoneo per l'utilizzo con DHCP (`/etc/sysconfig/network-scripts/ifcfg-ethN`). Genera inoltre un file di configurazione del routing (`/etc/sysconfig/network-scripts/route-ethN`).

Script DHCP

Ogni volta che l'interfaccia di rete riceve un nuovo lease DHCP, questo script esegue una query sui metadati dell'istanza per cercare gli indirizzi IP elastici. Per ogni indirizzo IP elastico, aggiunge una regola al database delle policy di routing per garantire che il traffico in uscita da tale indirizzo utilizzi l'interfaccia di rete corretta. All'interfaccia di rete aggiunge inoltre ciascun indirizzo IP privato come indirizzo secondario.

ec2ifup ethN (`/usr/sbin/`)

Estende la funzionalità del comando standard ifup. Dopo che questo script ha riscritto i file di configurazione `ifcfg-ethN` e `route-ethN`, esegue ifup.

ec2ifdown ethN (`/usr/sbin/`)

Estende la funzionalità del comando standard ifdown. Dopo che questo script ha rimosso le regole per l'interfaccia di rete dal database delle policy di routing, esegue ifdown.

ec2ifscan (`/usr/sbin/`)

Verifica la presenza di interfacce di rete non configurate e le configura.

Questo script non è disponibile nella versione iniziale di ec2-net-utils.

Per elencare i file di configurazione generati da ec2-net-utils, utilizzare il seguente comando:

```
$ ls -l /etc/sysconfig/network-scripts/*-eth?
```

Per disabilitare l'automazione, puoi aggiungere `EC2SYNC=no` al file `ifcfg-ethN` corrispondente. Ad esempio, utilizza il seguente comando per disabilitare l'automazione per l'interfaccia eth1:

```
$ sed -i -e 's/^EC2SYNC=yes/EC2SYNC=no/' /etc/sysconfig/network-scripts/ifcfg-eth1
```

Per disabilitare completamente l'automazione, puoi rimuovere il pacchetto utilizzando il seguente comando:

```
$ yum remove ec2-net-utils
```

Scenari per le interfacce di rete

Il collegamento di più interfacce di rete a un'istanza risulta utile quando desideri:

- Creare una rete di gestione.
- Utilizza appliance di rete e sicurezza nel tuo cloud privato virtuale (VPC).
- Creare istanze dual-homed con carichi di lavoro/ ruoli su sottoreti distinte.
- Creare una soluzione economica a elevata disponibilità.

Creare una rete di gestione

Questo scenario descrive come creare una rete di gestione con interfacce di rete in base ai criteri e alle impostazioni seguenti (figura seguente).

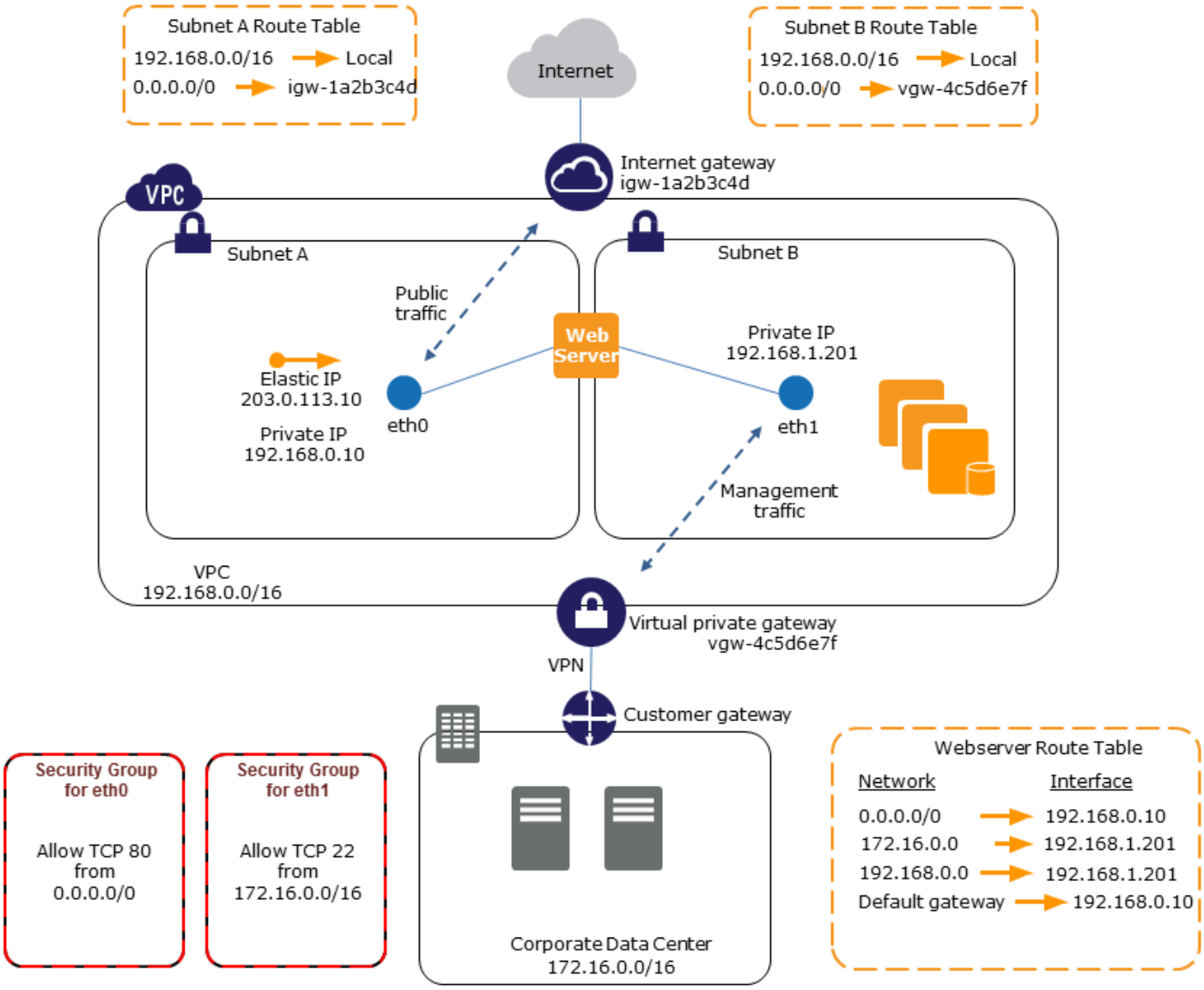
Criteri

- L'interfaccia di rete primaria sull'istanza (eth0) gestisce il traffico pubblico.
- L'interfaccia di rete secondaria sull'istanza (eth1) gestisce il traffico di gestione del back-end. È connessa a una sottorete separata con controlli di accesso più restrittivi e si trova nella stessa zona di disponibilità (AZ) dell'interfaccia di rete principale.

Impostazioni

- L'interfaccia di rete principale, che può essere o meno dietro un sistema di bilanciamento del carico, ha un gruppo di sicurezza associato che consente l'accesso al server da Internet. Ad esempio, abilita le porte TCP 80 e 443 da `0.0.0.0/0` o dal sistema di bilanciamento del carico.
- L'interfaccia di rete secondaria ha un gruppo di sicurezza associato che consente solo l'accesso SSH, avviato da una delle seguenti posizioni:
  - Un intervallo consentito di indirizzi IP, all'interno del VPC privato virtuale o da Internet.
  - Una sottorete privata all'interno della stessa AZ dell'interfaccia di rete principale.
  - Un gateway privato virtuale.

> **Note**
>
> Per garantire le funzionalità di failover, considera di utilizzare un indirizzo IPv4 privato secondario per il traffico in entrata su un'interfaccia di rete. Nel caso di un errore a livello di istanza, è possibile trasferire l'interfaccia e/o l'indirizzo IPv4 privato secondario su un'istanza in standby.



Utilizzo di appliance di rete e sicurezza nel VPC

Alcune appliance di rete e sicurezza, ad esempio i load balancer, i server Network Address Translation (NAT) e i server proxy preferiscono una configurazione basata su più interfacce di rete. Puoi creare e allegare interfacce di rete secondarie alle istanze che eseguono questi tipi di applicazioni e configurare interfacce aggiuntive con i loro indirizzi IP privati e pubblici, gruppi di sicurezza e controllo dell'origine/della destinazione.

Creazione di istanze dual-homed con carichi di lavoro/ ruoli su sottoreti distinte

Puoi inserire un'interfaccia di rete su ciascun server Web che si connette a una rete di livello intermedio in cui si trova un server applicazioni. Anche il server applicazioni può essere di tipo dual-homed in una rete back-end (sottorete) in cui si trova il server di database. Anziché instradare i pacchetti di rete tramite istanze dual-homed, ogni istanza dual-homed riceve ed elabora le richieste sul front-end, stabilisce una connessione con il back-end, quindi invia le richieste ai server sulla rete back-end.

Creazione di istanze dual-homed con carichi di lavoro/ruoli su VPC distinti all'interno dello stesso account

È possibile avviare un'istanza EC2 in un VPC e collegare all'istanza un ENI secondario da un altro VPC (purché nella stessa zona di disponibilità). Ciò consente di creare istanze multi-homed su VPC con configurazioni di rete e sicurezza differenti. Non è possibile creare istanze multi-homed tra VPC e account diversi. AWS

Puoi utilizzare le istanze dual-homed su più VPC nei seguenti casi d'uso:

- Supera le sovrapposizioni CIDR tra due VPC che non possono essere collegati tra loro: puoi sfruttare un CIDR secondario in un VPC e consentire a un'istanza di comunicare tra due intervalli IP non sovrapposti.
- Connetti più VPC all'interno di un unico account: abilita la comunicazione tra singole risorse che normalmente sarebbero separate dai confini del VPC.

Creazione di una soluzione economica a elevata disponibilità

Se l'esecuzione di una delle istanze che utilizzano una funzione specifica non riesce, la relativa interfaccia di rete può essere collegata a un'istanza hot standby preconfigurata per lo stesso ruolo in modo da consentire il rapido ripristino del servizio. Ad esempio, puoi creare un'interfaccia di rete come interfaccia di rete primaria o secondaria per un servizio fondamentale, ad esempio un'istanza di database o un'istanza NAT. Se l'istanza non riesce, tu (o più probabilmente il codice eseguito per tuo conto) puoi collegare l'interfaccia di rete a un'istanza hot standby. Dal momento che l'interfaccia conserva i propri indirizzi IP privati, gli indirizzi IP elastici e l'indirizzo MAC, il traffico di rete comincia a essere indirizzato all'istanza in standby non appena colleghi l'interfaccia di rete all'istanza di sostituzione. Gli utenti rileveranno una breve interruzione della connettività tra il momento in cui l'esecuzione dell'istanza non riesce e il momento in cui l'interfaccia di rete viene collegata all'istanza in standby. Non è tuttavia richiesta alcuna modifica alla tabella di routing VPC o al server DNS.

Interfacce di rete gestite dal richiedente

Un'interfaccia di rete gestita dal richiedente è un'interfaccia di rete che un Servizio AWS crea nel VPC per tuo conto. L'interfaccia di rete è associata a una risorsa per un altro servizio, ad esempio un'istanza database di Amazon RDS, un gateway NAT o un endpoint VPC di interfaccia da AWS PrivateLink.

Considerazioni

- Puoi visualizzare le interfacce di rete gestite dal richiedente presenti nel tuo account. Puoi aggiungere o rimuovere tag, ma non puoi modificare altre proprietà di un'interfaccia di rete gestita dal richiedente.
- Non puoi scollegare un'interfaccia di rete gestita dal richiedente.
- Quando elimini la risorsa associata a un'interfaccia di rete gestita dal richiedente, scollega l'interfaccia di rete Servizio AWS e la elimina. Se il servizio ha scollegato un'interfaccia di rete ma non l'ha eliminata, puoi eliminare l'interfaccia di rete scollegata.

Per visualizzare le interfacce di rete gestite dal richiedente utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Network & Security (Rete e sicurezza), quindi Network Interfaces (Interfacce di rete).
3. Seleziona l'ID dell'interfaccia di rete per aprirne la pagina dei dettagli.
4. Di seguito sono riportati i campi chiave che puoi usare per determinare lo scopo dell'interfaccia di rete:

    - Description (Descrizione): una descrizione fornita dal servizio AWS che ha creato l'interfaccia. Ad esempio, "VPC Endpoint Interface vpce 089f2123488812123".
    - Gestita dal richiedente: indica se l'interfaccia di rete è gestita da. AWS
    - ID richiedente: l'alias o l'ID dell' AWS account del principale o del servizio che ha creato l'interfaccia di rete. Se hai creato l'interfaccia di rete, questo è il tuo Account AWS ID. In caso contrario, è stata creata da un'altra entità principale o da un altro servizio.

Per visualizzare le interfacce di rete gestite dal richiedente utilizzando il AWS CLI

Utilizza il comando describe-network-interfaces come riportato di seguito.

```
aws ec2 describe-network-interfaces --filters Name=requester-managed,Values=true
```

Di seguito è riportato un output di esempio che mostra i campi chiave che puoi usare per determinare lo scopo dell'interfaccia di rete: `Description` e `InterfaceType`.

```
{
     ...
    "Description": "VPC Endpoint Interface vpce-089f2123488812123",
    ...
    "InterfaceType": "vpc_endpoint",
    ...
    "NetworkInterfaceId": "eni-0d11e3ccd2c0e6c57",
    ...
    "RequesterId": "727180483921",
    "RequesterManaged": true,
    ...
}
```

Per visualizzare le interfacce di rete gestite dal richiedente utilizzando gli Strumenti per Windows PowerShell

Utilizzare il Get-EC2NetworkInterfacecmdlet come segue.

```
Get-EC2NetworkInterface -Filter @{ Name="requester-managed"; Values="true" }
```

Di seguito è riportato un output di esempio che mostra i campi chiave che puoi usare per determinare lo scopo dell'interfaccia di rete: `Description` e `InterfaceType`.

```
Description        : VPC Endpoint Interface vpce-089f2123488812123
...
InterfaceType      : vpc_endpoint
...
NetworkInterfaceId : eni-0d11e3ccd2c0e6c57
...
RequesterId        : 727180483921
RequesterManaged   : True
...
```

Assegna prefissi alle interfacce di rete Amazon EC2

È possibile assegnare un intervallo CIDR IPv4 o IPv6 privato, automaticamente o manualmente, alle interfacce di rete. Assegnando i prefissi, è possibile dimensionare e semplificare la gestione delle applicazioni, incluse le applicazioni container e di rete che richiedono più indirizzi IP su un'istanza. Per ulteriori informazioni sugli indirizzi IPv4 e IPv6, consulta Indirizzamento IP per le istanze Amazon EC2.

Sono disponibili le seguenti opzioni di incarico:

- Assegnazione automatica: AWS sceglie il prefisso dal blocco CIDR IPv4 o IPv6 della sottorete VPC e lo assegna all'interfaccia di rete.
- Assegnazione manuale: specifichi il prefisso dal blocco CIDR IPv4 o IPv6 della sottorete VPC e AWS verificate che il prefisso non sia già assegnato ad altre risorse prima di assegnarlo all'interfaccia di rete.

L'assegnazione dei prefissi presenta i seguenti vantaggi:

- Aumento degli indirizzi IP su un'interfaccia di rete: quando si utilizza un prefisso, si assegna un blocco di indirizzi IP anziché singoli indirizzi IP. Questo aumenta il numero di indirizzi IP per un'interfaccia di rete.
- Gestione VPC semplificata per i container: nelle applicazioni container, ogni container richiede un indirizzo IP univoco. L'assegnazione dei prefissi alla tua istanza semplifica la gestione dei tuoi VPC, poiché puoi avviare e terminare i container senza dover chiamare le API Amazon EC2 per i singoli incarichi IP.

Indice

Nozioni di base per l'assegnazione di prefissi

- È possibile assegnare un prefisso a interfacce di rete nuove o esistenti.
- Per utilizzare i prefissi, è necessario assegnare un prefisso all'interfaccia di rete, allegare l'interfaccia di rete all'istanza e configurare il sistema operativo.

- Quando si sceglie l'opzione per specificare un prefisso, il prefisso deve soddisfare i seguenti requisiti:
  - Il prefisso IPv4 che è possibile specificare è `/28`.
  - Il prefisso IPv6 che è possibile specificare è `/80`.
  - Il prefisso si trova nella sottorete CIDR dell'interfaccia di rete e non si sovrappone ad altri prefissi o indirizzi IP assegnati alle risorse esistenti nella sottorete.
- È possibile assegnare un prefisso all'interfaccia di rete primaria o secondaria.
- È possibile assegnare un indirizzo IP elastico a un'interfaccia di rete a cui è stato assegnato un prefisso.
- Puoi inoltre assegnare un indirizzo IP elastico alla parte di indirizzo IP del prefisso assegnato.
- Un nome host DNS privato (interno) di un'istanza viene risolto all'indirizzo IPv4 privato.
- Assegniamo ogni indirizzo IPv4 privato per un'interfaccia di rete, inclusi quelli dei prefissi, utilizzando il seguente formato:
  - Regione `us-east-1`

    ```
    ip-private-ipv4-address.ec2.internal
    ```

  - Tutte le altre Regioni

    ```
    ip-private-ipv4-address.region.compute.internal
    ```

Considerazioni e limiti per i prefissi

Quando si utilizzano i prefissi, prendere in considerazione quanto segue:

- Le interfacce di rete con prefissi sono supportate con istanze basate sul sistema Nitro. AWS
- I prefissi per le interfacce di rete sono limitati agli indirizzi IPv6 e agli indirizzi IPv4 privati.
- Il numero massimo di indirizzi IP che è possibile assegnare a un'interfaccia di rete dipende dal tipo di istanza. Ogni prefisso assegnato a un'interfaccia di rete conta come un unico indirizzo IP. Ad esempio, un'istanza `c5.large` ha un limite di `10` indirizzi IPv4 per interfaccia di rete. Ogni interfaccia di rete per questa istanza ha un indirizzo IPv4 primario. Se un'interfaccia di rete non ha indirizzi IPv4 secondari, è possibile assegnare fino a 9 prefissi all'interfaccia di rete. Per ogni indirizzo IPv4 aggiuntivo assegnato a un'interfaccia di rete, a questa è possibile assegnare un prefisso in meno. Per ulteriori informazioni, consulta Indirizzi IP per interfaccia di rete per tipo di istanza.

- I prefissi sono inclusi nei controlli dell'origine/della destinazione.

Utilizzare i prefissi

È possibile utilizzare i prefissi con le interfacce di rete come segue.

Attività

- Assegnare i prefissi durante la creazione dell'interfaccia di rete
- Assegnare prefissi alle interfacce di rete esistenti
- Configurare il sistema operativo per le interfacce di rete con prefissi
- Visualizzare i prefissi assegnati alle interfacce di rete
- Rimuovere i prefissi dalle interfacce di rete

Assegnare i prefissi durante la creazione dell'interfaccia di rete

Se utilizzi l'opzione di assegnazione automatica, puoi riservare un blocco di indirizzi IP nella sottorete. AWS sceglie i prefissi da questo blocco. Per ulteriori informazioni, consulta la sezione relativa a Prenotazioni della CIDR per la sottorete nella Guida per l'utente di Amazon VPC.

Dopo aver creato l'interfaccia di rete, utilizzate il attach-network-interface AWS CLI comando per collegare l'interfaccia di rete all'istanza. Devi configurare il sistema operativo affinché funzioni con le interfacce di rete con prefissi. Per ulteriori informazioni, consulta Configurare il sistema operativo per le interfacce di rete con prefissi.

Attività

- Assegnare prefissi automatici durante la creazione dell'interfaccia di rete
- Assegnare prefissi specifici durante la creazione dell'interfaccia di rete

Assegnare prefissi automatici durante la creazione dell'interfaccia di rete

Puoi assegnare prefissi automatici durante la creazione dell'interfaccia di rete utilizzando uno dei metodi descritti di seguito.

Console

Per assegnare prefissi automatici durante la creazione dell'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Network Interfaces (Interfacce di rete) e selezionare Create network interface (Crea interfaccia di rete).
3. Specificare una descrizione per l'interfaccia di rete, selezionare la sottorete in cui creare l'interfaccia di rete e configurare gli indirizzi IPv4 e IPv6 privati.
4. Espandere Advanced settings (Impostazioni avanzate) ed eseguire le operazioni descritte di seguito:

   a. Per assegnare automaticamente un prefisso IPv4, per IPv4 prefix delegation (Delega del prefisso IPv4), scegliere Auto-assign (Assegnazione automatica). Poi per Number of IPv4 prefixes (Numero di prefissi IPv4), specificare il numero di prefissi da assegnare.

   b. Per assegnare automaticamente un prefisso IPv6, per IPv6 prefix delegation (Delega del prefisso IPv6), scegliere Auto-assign (Assegnazione automatica). Poi per Number of IPv6 prefixes (Numero di prefissi IPv6), specificare il numero di prefissi da assegnare.

   > **Note**
   >
   > L'opzione IPv6 prefix delegation (Delega del prefisso IPv6) viene visualizzata solo se la sottorete selezionata è abilitata per IPv6.

5. Selezionare i gruppi di sicurezza da associare all'interfaccia di rete e assegnare i tag di risorse se necessario.
6. Seleziona Crea un'interfaccia di rete.

AWS CLI

Per assegnare prefissi IPv4 automatici durante la creazione dell'interfaccia di rete

Utilizzate il create-network-interfacecomando e `--ipv4-prefix-count` impostate il numero di prefissi che desiderate AWS assegnare. Nell'esempio seguente, assegna un prefisso. AWS 1

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv4 automatic example" \
```

```
--ipv4-prefix-count 1
```

Output di esempio

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv4 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:98:65:dd:18:47",
        "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.62",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.62"
            }
        ],
        "Ipv4Prefixes": [
            {
                "Ipv4Prefix": "10.0.0.208/28"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

Per assegnare prefissi IPv6 automatici durante la creazione dell'interfaccia di rete

Utilizzate il create-network-interfacecomando e impostate `--ipv6-prefix-count` il numero di prefissi che desiderate assegnare. AWS Nell'esempio seguente, assegna un prefisso. AWS 1

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv6 automatic example" \
--ipv6-prefix-count 1
```

Output di esempio

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv6 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:bb:e4:31:fe:09",
        "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.73",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv6Prefixes": [
            {
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
```

```
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

Assegnare prefissi specifici durante la creazione dell'interfaccia di rete

Puoi assegnare prefissi specifici durante la creazione dell'interfaccia di rete utilizzando uno dei metodi descritti di seguito.

Console

Per assegnare prefissi specifici durante la creazione dell'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Network Interfaces (Interfacce di rete) e selezionare Create network interface (Crea interfaccia di rete).
3. Specificare una descrizione per l'interfaccia di rete, selezionare la sottorete in cui creare l'interfaccia di rete e configurare gli indirizzi IPv4 e IPv6 privati.
4. Espandere Advanced settings (Impostazioni avanzate) ed eseguire le operazioni descritte di seguito:
   a. Per assegnare un prefisso IPv4 specifico, per IPv4 prefix delegation (Delega del prefisso IPv4), scegliere Custom (Personalizzato). Quindi scegliere Add new prefix (Aggiungi nuovo prefisso) e inserire il prefisso da utilizzare.
   b. Per assegnare un prefisso IPv6 specifico, per IPv6 prefix delegation (Delega prefisso IPv6), scegli Custom (Personalizzato). Quindi scegliere Add new prefix (Aggiungi nuovo prefisso) e inserire il prefisso da utilizzare.

   > **Note**
   > L'opzione IPv6 prefix delegation (Delega del prefisso IPv6) viene visualizzata solo se la sottorete selezionata è abilitata per IPv6.
5. Selezionare i gruppi di sicurezza da associare all'interfaccia di rete e assegnare i tag di risorse se necessario.
6. Seleziona Crea un'interfaccia di rete.

AWS CLI

Per assegnare prefissi IPv4 specifici durante la creazione dell'interfaccia di rete

Utilizzate il create-network-interfacecomando e impostate i `--ipv4-prefixes` prefissi. AWS seleziona gli indirizzi IP da questo intervallo. Nell'esempio seguente, il prefisso CIDR è `10.0.0.208/28`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Output di esempio

```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv4 manual example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.62"
                }
            ],
            "Ipv4Prefixes": [
                {
                    "Ipv4Prefix": "10.0.0.208/28"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
```

```
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "pending",
            "SubnetId": "subnet-047cfed18eEXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    }
```

Per assegnare prefissi IPv6 specifici durante la creazione dell'interfaccia di rete

Usa il create-network-interfacecomando e imposta `--ipv6-prefixes` i prefissi. AWS seleziona gli indirizzi IP da questo intervallo. Nell'esempio seguente, il prefisso CIDR è `2600:1f13:fc2:a700:1768::/80`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

Output di esempio

```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv6 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:bb:e4:31:fe:09",
            "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.73",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
```

```
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv6Prefixes": [
            {
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

Assegnare prefissi alle interfacce di rete esistenti

Dopo aver assegnato i prefissi, utilizzate il attach-network-interface AWS CLI comando per collegare l'interfaccia di rete all'istanza. Devi configurare il sistema operativo affinché funzioni con le interfacce di rete con prefissi. Per ulteriori informazioni, consulta Configurare il sistema operativo per le interfacce di rete con prefissi.

Attività

- Assegnare prefissi automatici a un'interfaccia di rete esistente
- Assegnare prefissi specifici a un'interfaccia di rete esistente

Assegnare prefissi automatici a un'interfaccia di rete esistente

Puoi assegnare prefissi automatici a un'interfaccia di rete esistente utilizzando uno dei metodi descritti di seguito.

Console

Per assegnare prefissi automatici a un'interfaccia di rete esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).

3. Selezionare l'interfaccia di rete a cui assegnare i prefissi e scegliere Actions (Operazioni), Manage prefixes (Gestisci prefissi).
4. Per assegnare automaticamente un prefisso IPv4, per IPv4 prefix delegation (Delega del prefisso IPv4), scegliere Auto-assign (Assegnazione automatica). Poi per Number of IPv4 prefixes (Numero di prefissi IPv4), specificare il numero di prefissi da assegnare.
5. Per assegnare automaticamente un prefisso IPv6, per IPv6 prefix delegation (Delega del prefisso IPv6), scegliere Auto-assign (Assegnazione automatica). Poi per Number of IPv6 prefixes (Numero di prefissi IPv6), specificare il numero di prefissi da assegnare.

> **Note**
>
> L'opzione IPv6 prefix delegation (Delega del prefisso IPv6) viene visualizzata solo se la sottorete selezionata è abilitata per IPv6.

6. Selezionare Salva.

AWS CLI

È possibile utilizzare il comando assign-ipv6-addresses per assegnare i prefissi IPv6 e il comando per assegnare i prefissi IPv4 alle interfacce di rete esistenti. assign-private-ip-addresses

Per assegnare prefissi IPv4 automatici a un'interfaccia di rete esistente

Utilizzate il comando e impostate il numero di prefissi che desiderate assegnare. assign-private-ip-addresses`--ipv4-prefix-count` AWS Nell'esempio seguente, AWS 1 assegna il prefisso IPv4.

```
$ C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefix-count 1
```

Output di esempio

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
            "Ipv4Prefix": "10.0.0.176/28"
```

```
        }
    ]
}
```

Per assegnare prefissi IPv6 automatici a un'interfaccia di rete esistente

Utilizzate il comando assign-ipv6-addresses e impostate il numero di prefissi da `--ipv6-prefix-count` assegnare. AWS Nell'esempio seguente, assegna il prefisso IPv6. AWS 1

```
$ C:\> aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix-count 1
```

Output di esempio

```
{
    "AssignedIpv6Prefixes": [
        "2600:1f13:fc2:a700:18bb::/80"
    ],
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE"
}
```

Assegnare prefissi specifici a un'interfaccia di rete esistente

Puoi assegnare prefissi specifici a un'interfaccia di rete esistente utilizzando uno dei metodi descritti di seguito.

Console

Per assegnare prefissi specifici a un'interfaccia di rete esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Selezionare l'interfaccia di rete a cui assegnare i prefissi e scegliere Actions (Operazioni), Manage prefixes (Gestisci prefissi).
4. Per assegnare un prefisso IPv4 specifico, per IPv4 prefix delegation (Delega del prefisso IPv4), scegliere Custom (Personalizzato). Quindi scegliere Add new prefix (Aggiungi nuovo prefisso) e inserire il prefisso da utilizzare.

5. Per assegnare un prefisso IPv6 specifico, per IPv6 prefix delegation (Delega prefisso IPv6), scegli Custom (Personalizzato). Quindi scegliere Add new prefix (Aggiungi nuovo prefisso) e inserire il prefisso da utilizzare.

> **Note**
>
> L'opzione IPv6 prefix delegation (Delega del prefisso IPv6) viene visualizzata solo se la sottorete selezionata è abilitata per IPv6.

6. Selezionare Salva.

AWS CLI

Assegnare prefissi IPv4 specifici a un'interfaccia di rete esistente

Utilizzate il assign-private-ip-addressescomando e impostate il prefisso`--ipv4-prefixes`. AWS seleziona gli indirizzi IPv4 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è `10.0.0.208/28`.

```
$ C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.208/28
```

Output di esempio

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
            "Ipv4Prefix": "10.0.0.208/28"
        }
    ]
}
```

Assegnare prefissi IPv6 specifici a un'interfaccia di rete esistente

Utilizzate il comando assign-ipv6-addresses e impostatelo sul prefisso. `--ipv6-prefixes` AWS seleziona gli indirizzi IPv6 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è `2600:1f13:fc2:a700:18bb::/80`.

```
$ C:\> aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

Output di esempio

```
{
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE",
    "AssignedIpv6Prefixes": [
        {
            "Ipv6Prefix": "2600:1f13:fc2:a700:18bb::/80"
        }
    ]
}
```

Configurare il sistema operativo per le interfacce di rete con prefissi

Le AMI Amazon Linux potrebbero contenere script aggiuntivi installati da AWS, noti come. `ec2-net-utils` Questi script automatizzano facoltativamente la configurazione delle interfacce di rete. Sono disponibili solo per Amazon Linux.

Se non utilizzi Amazon Linux, è possibile utilizzare un'interfaccia di rete container (CNI) per il plug-in Kubernetes, oppure `dockerd` se gestisci i container con Docker.

Visualizzare i prefissi assegnati alle interfacce di rete

Puoi visualizzare i prefissi assegnati alle interfacce di rete utilizzando uno dei metodi descritti di seguito.

Console

Per visualizzare i prefissi automatici assegnati a un'interfaccia di rete esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Selezionare l'interfaccia di rete per la quale visualizzare i prefissi e scegliere la scheda Details (Dettagli).
4. IPv4 Prefix Delegation (Delega prefisso IPv4) elenca i prefissi IPv4 assegnati e il campo IPv6 Prefix Delegation (Delega prefisso IPv6) elenca i prefissi IPv6 assegnati.

AWS CLI

Puoi usare il describe-network-interfaces AWS CLI comando per visualizzare i prefissi assegnati alle tue interfacce di rete.

```
$ C:\> aws ec2 describe-network-interfaces
```

Output di esempio

```
{
    "NetworkInterfaces": [
        {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv4 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.62"
                }
            ],
            "Ipv4Prefixes": [
                {
                    "Ipv4Prefix": "10.0.0.208/28"
                }
            ],
            "Ipv6Prefixes": [],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "available",
            "SubnetId": "subnet-05eef9fb78EXAMPLE",
```

```
            "TagSet": [],
            "VpcId": "vpc-0e12f52b2146bf252"
        },
        {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv6 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c411c91b5"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:bb:e4:31:fe:09",
            "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.73",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.73"
                }
            ],
            "Ipv4Prefixes": [],
            "Ipv6Prefixes": [
                {
                    "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "available",
            "SubnetId": "subnet-05eef9fb78EXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    ]
}
```

Rimuovere i prefissi dalle interfacce di rete

Puoi rimuovere i prefissi dalle interfacce di rete utilizzando uno dei metodi descritti di seguito.

Console

Per rimuovere i prefissi da un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Selezionare l'interfaccia di rete da cui rimuovere i prefissi e scegliere Actions (Operazioni), Manage prefixes (Gestisci prefissi).
4. Esegui una di queste operazioni:
   - Per rimuovere tutti i prefissi assegnati, per IPv4 prefix delegation (Delega del prefisso IPv4) e IPv6 prefix delegation (Delega del prefisso IPv6), scegliere Do not assign (Non assegnare).
   - Per rimuovere prefissi assegnati specifici, per IPv4 prefix delegation (Delega del prefisso IPv4) o IPv6 prefix delegation (Delega del prefisso IPv6), scegli Custom (Personalizzato) e quindi Unassign (Rimuovi assegnazione) in corrispondenza dei prefissi da rimuovere.

   > **Note**
   >
   > L'opzione IPv6 prefix delegation (Delega del prefisso IPv6) viene visualizzata solo se la sottorete selezionata è abilitata per IPv6.
5. Selezionare Salva.

AWS CLI

È possibile utilizzare il comando unassign-ipv6-addresses per rimuovere i prefissi IPv6 e i comandi per rimuovere i prefissi IPv4 dalle interfacce di rete esistenti. unassign-private-ip-addresses

Per rimuovere i prefissi IPv4 da un'interfaccia di rete

unassign-private-ip-addressesUtilizzate il `--ipv4-prefix` comando e impostatelo sull'indirizzo che desiderate rimuovere.

```
$ C:\> aws ec2 unassign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.176/28
```

Per rimuovere i prefissi IPv6 da un'interfaccia di rete

Utilizzare il comando unassign-ipv6-addresses e impostare `--ipv6-prefix` sull'indirizzo che si desidera rimuovere.

```
$ C:\> aws ec2 unassign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

Larghezza di banda di rete dell'istanza Amazon EC2

Le specifiche della larghezza di banda dell'istanza si applicano sia al traffico in entrata che in uscita dell'istanza. Ad esempio, se un'istanza specifica fino a 10 Gbps di larghezza di banda, significa che ha fino a 10 Gbps di larghezza di banda per il traffico in entrata e fino a 10 Gbps per il traffico in uscita. La larghezza di banda della rete disponibile per un'istanza EC2 dipende da diversi fattori, come descritto di seguito:

Traffico multi-flusso

La larghezza di banda per il traffico a più flussi aggregato disponibile per un'istanza dipende dalla destinazione del traffico.

- All'interno della regione: il traffico può utilizzare l'intera larghezza di banda della rete disponibile per l'istanza.
- In altre regioni, un gateway Internet, Direct Connect o gateway locali (LGW): il traffico può utilizzare fino al 50% della larghezza di banda della rete disponibile per un'istanza di generazione attuale con un minimo di 32 vCPU. La larghezza di banda per un'istanza di generazione corrente con meno di 32 vCPU è limitata a 5 Gbps.

Traffico a flusso singolo

La larghezza di banda di base per il traffico a flusso singolo è limitata a 5 Gbps quando le istanze non si trovano nello stesso gruppo di collocazione cluster. Per ridurre la latenza e aumentare la larghezza di banda a flusso singolo, prova una delle seguenti opzioni:

- Utilizza un gruppo di collocazione cluster per ottenere una larghezza di banda fino a 10 Gbps per le istanze all'interno dello stesso gruppo di collocazione.
- Imposta più percorsi tra due endpoint qualsiasi per ottenere una maggiore larghezza di banda con Multipath TCP (MPTCP).
- Configura ENA Express per le istanze idonee all'interno della stessa sottorete per raggiungere fino a 25 Gbps tra tali istanze.

Larghezza di banda disponibile per l'istanza

La larghezza di banda di rete disponibile per un'istanza dipende dal numero di vCPU di cui dispone. Ad esempio, un'istanza `m5.8xlarge` ha 32 vCPUs e una larghezza di banda di rete a 10 Gb/s e un'istanza `m5.16xlarge` ha una larghezza di banda di 64 vCPUs e larghezza di banda di rete di 20 Gb/s. Le istanze potrebbero tuttavia non raggiungere questa larghezza di banda, ad esempio se superano i limiti di rete a livello di istanza, come il numero di pacchetti al secondo o di connessioni tracciate. La quantità di larghezza di banda disponibile che il traffico può utilizzare dipende dal numero di vCPU e dalla destinazione. Ad esempio, un'istanza `m5.16xlarge` presenta 64 vCPU, quindi il traffico verso un'altra istanza nella regione può utilizzare l'intera larghezza di banda disponibile (20 Gb/s). Tuttavia, il traffico verso un'altra istanza in una regione diversa può utilizzare solo il 50% della larghezza di banda disponibile (10 Gb/s).

In genere, istanze con 16 vCPUs o meno (dimensioni `4xlarge` e inferiori) sono documentate come aventi "fino a" una larghezza di banda specificata; ad esempio, "fino a 10 Gb/s". Queste istanze hanno una larghezza di banda di base. Per soddisfare la domanda aggiuntiva, possono utilizzare un meccanismo di credito I/O di rete per superare la larghezza di banda di base. Le istanze possono utilizzare la larghezza di banda burst per un periodo di tempo limitato, in genere da 5 a 60 minuti, a seconda delle dimensioni dell'istanza.

Un'istanza riceve il numero massimo di crediti I/O di rete all'avvio. Se l'istanza esaurisce i propri crediti I/O di rete, torna alla larghezza di banda di base. Un'istanza in esecuzione guadagna crediti I/O di rete ogni volta che utilizza meno larghezza di banda di rete rispetto alla larghezza di banda di base. Un'istanza arrestata non guadagna crediti I/O di rete. L'ottimizzazione dell'istanza è basata sul massimo sforzo, anche quando l'istanza ha crediti disponibili, poiché la larghezza di banda burst è una risorsa condivisa.

Esistono bucket di credito I/O di rete separati per il traffico in entrata e in uscita.

Prestazioni di rete di base e potenziate

La Amazon EC2 Instance Types Guide descrive le prestazioni di rete per ogni tipo di istanza, oltre alla larghezza di banda di rete di base disponibile per le istanze che possono utilizzare una larghezza di banda burst. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Specifiche di rete: scopo generale
- Specifiche di rete: ottimizzate per il calcolo
- Specifiche di rete: memoria ottimizzata
- Specifiche di rete: archiviazione ottimizzata
- Specifiche di rete: elaborazione accelerata
- Specifiche di rete: elaborazione ad alte prestazioni
- Specifiche di rete: generazione precedente

Per visualizzare le prestazioni della rete utilizzando AWS CLI

È possibile utilizzare il describe-instance-types AWS CLI comando per visualizzare informazioni su un tipo di istanza. Nell'esempio seguente vengono visualizzate le informazioni sulle prestazioni di rete per tutte le istanze C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].[ \
        InstanceType, \
        NetworkInfo.NetworkPerformance, \
        NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps]" \
    --output table
```

Output previsto

```
-----------------------------------------------
|           DescribeInstanceTypes           |
+--------------+--------------------+-------+
|  c5.4xlarge  |  Up to 10 Gigabit  |  5.0  |
|  c5.xlarge   |  Up to 10 Gigabit  |  1.25 |
|  c5.12xlarge |  12 Gigabit        |  12.0 |
|  c5.24xlarge |  25 Gigabit        |  25.0 |
|  c5.metal    |  25 Gigabit        |  25.0 |
```

```
|  c5.9xlarge  |  12 Gigabit        |  12.0 |
|  c5.2xlarge  |  Up to 10 Gigabit  |  2.5  |
|  c5.large    |  Up to 10 Gigabit  |  0.75 |
|  c5.18xlarge |  25 Gigabit        |  25.0 |
+--------------+--------------------+-------+
```

Per visualizzare le prestazioni della rete utilizzando AWS Tools for PowerShell

È possibile utilizzare il Get-EC2InstanceType PowerShell comando per visualizzare informazioni su un tipo di istanza. Nell'esempio seguente vengono visualizzate le informazioni sulle prestazioni di rete per tutte le istanze C5.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
    Select-Object `
    InstanceType,
    @{Name = 'NetworkPerformance'; Expression =
 {($_.Networkinfo.NetworkCards.NetworkPerformance)}},
    @{Name = 'BaselineBandwidthInGbps'; Expression =
 {($_.Networkinfo.NetworkCards.BaselineBandwidthInGbps)}} | `
Format-Table -AutoSize
```

Output previsto

```
InstanceType NetworkPerformance BaselineBandwidthInGbps
------------ ------------------ ----------------------
c5.4xlarge   Up to 10 Gigabit                    5.00
c5.xlarge    Up to 10 Gigabit                    1.25
c5.12xlarge  12 Gigabit                         12.00
c5.9xlarge   12 Gigabit                         12.00
c5.24xlarge  25 Gigabit                         25.00
c5.metal     25 Gigabit                         25.00
c5.2xlarge   Up to 10 Gigabit                    2.50
c5.large     Up to 10 Gigabit                    0.75
c5.18xlarge  25 Gigabit                         25.00
```

Monitorare la larghezza di banda delle istanze

È possibile utilizzare le CloudWatch metriche per monitorare la larghezza di banda della rete dell'istanza e i pacchetti inviati e ricevuti. Puoi utilizzare i parametri delle prestazioni di rete fornite dal driver ENA (Elastic Network Adapter) per monitorare quando il traffico supera le quote di rete definite da Amazon EC2 a livello di istanza.

Puoi configurare se Amazon EC2 invia i dati metrici per l'istanza CloudWatch utilizzando periodi di un minuto o cinque minuti. È possibile che i parametri delle prestazioni di rete mostrino che è stata superata una soglia e che i pacchetti sono stati eliminati, mentre i parametri dell'istanza no. CloudWatch Ciò può accadere quando l'istanza presenta un breve picco nella domanda di risorse di rete (noto come microburst), ma le CloudWatch metriche non sono sufficientemente granulari da riflettere questi picchi di microsecondi.

Ulteriori informazioni

- Parametri dell'istanza
- Parametri sulle prestazioni di rete

Rete avanzata su Amazon EC2

Le reti avanzate utilizzano la specifica SR-IOV (Single Root I/O Virtualization) per fornire funzionalità di rete a prestazioni elevate sui tipi di istanza supportati. SR-IOV è un metodo di virtualizzazione dei dispositivi che fornisce prestazioni I/O più elevate e minore utilizzo della CPU rispetto alle interfacce di rete virtualizzate tradizionali. La rete avanzata offre una maggiore larghezza di banda, prestazioni PPS (packet per second) più elevate e una latenza costantemente inferiore tra le istanze. L'utilizzo di questo servizio avanzato non comporta costi supplementari.

Per ulteriori informazioni sulla velocità di rete supportata per ogni tipo di istanza, consulta Tipi di istanze Amazon EC2.

Indice

Supporto di reti avanzate

Tutti i tipi di istanza della generazione attuale supportano le reti avanzate, ad eccezione delle istanze T2.

È possibile abilitare la rete avanzata utilizzando uno dei seguenti meccanismi:

Elastic Network Adapter (ENA)

Elastic Network Adapter (ENA) supporta velocità di rete fino a 100 Gbps per i tipi di istanza supportati.

Tutte le istanze basate sul sistema AWS Nitro utilizzano ENA per una rete avanzata. Inoltre, i seguenti tipi di istanze Xen supportano ENA: H1, I3, G3, P2, P3`m4.16xlarge`, P3dn e R4.

Per ulteriori informazioni, consulta Abilita una rete avanzata con l'Elastic Network Adapter (ENA) sulle tue istanze EC2.

Interfaccia VF (Virtual Function) Intel 82599

L'interfaccia VF (Virtual Function) Intel 82599 supporta velocità di rete fino a 10 Gbps per i tipi di istanza supportati.

I seguenti tipi di istanza utilizzano l'interfaccia Intel 82599 VF per una rete avanzata: C3, C4, D2, I2, M4 (tranne m4.16xlarge) e R3.

Per ulteriori informazioni, consulta Abilita reti avanzate con l'interfaccia Intel 82599 VF sulle tue istanze EC2.

Abilita una rete avanzata con l'Elastic Network Adapter (ENA) sulle tue istanze EC2

Amazon EC2 fornisce funzionalità di rete avanzate tramite Elastic Network Adapter (ENA). Per utilizzare la rete avanzata, è necessario installare il modulo ENA richiesto e abilitare il supporto ENA.

Indice

- Verifica dell'abilitazione delle reti avanzate
- Abilitazione delle reti avanzate su un'istanza
- Note di rilascio del driver

Requisiti

Per preparare la configurazione delle funzionalità delle reti avanzate tramite ENA, configura l'istanza nel seguente modo:

- Avvia un'istanza basata sul sistema AWS Nitro.
- Verificare che l'istanza disponga di connettività Internet.
- Se sull'istanza sono presenti dati importanti che devono essere conservati, è consigliabile eseguire una copia di backup di tali dati ora mediante la creazione di un'AMI dall'istanza. L'aggiornamento dei kernel e dei relativi moduli, nonché l'abilitazione dell'attributo `enaSupport`, potrebbero rendere non compatibili le istanze o irraggiungibili i sistemi operativi. Se disponi di un backup recente, i tuoi dati saranno mantenuti.
- Istanze Linux: avvia l'istanza utilizzando una versione supportata del kernel Linux e una distribuzione supportata, in modo che la rete avanzata ENA sia abilitata automaticamente per l'istanza. Per ulteriori informazioni, consulta le note di rilascio del driver ENA Linux Kernel.
- Istanze Windows: se l'istanza esegue Windows Server 2008 R2 SP1, assicurati che sia installato l'aggiornamento per il supporto alla firma del codice SHA-2.
- Puoi utilizzarlo AWS CloudShellda oppure installarlo e configurarlo AWS Tools for Windows PowerShellsu qualsiasi computer a tua scelta, preferibilmente sul desktop AWS CLIo sul laptop locale. AWS Management Console Per ulteriori informazioni, consulta Accesso a Amazon EC2 o la Guida per l'utente di AWS CloudShell. Le reti avanzate non possono essere gestite dalla console Amazon EC2.

Prestazioni di reti avanzate

Nella documentazione seguente viene fornito un riepilogo delle prestazioni di rete per i tipi di istanza che supportano le reti avanzate ENA:

- Specifiche di rete per istanze di elaborazione accelerata
- Specifiche di rete per istanze ottimizzate per il calcolo
- Specifiche di rete per istanze generiche

- Specifiche di rete per istanze di elaborazione ad alte prestazioni
- Specifiche di rete per istanze ottimizzate per la memoria
- Specifiche di rete per istanze ottimizzate per l'archiviazione

AMI Linux con il modulo richiesto

Le seguenti AMI includono il modulo ENA richiesto e hanno abilitato il supporto ENA:

- AL2023
- Amazon Linux 2
- AMI Amazon Linux 2018.03 e versioni successive
- Ubuntu 14.04 o versioni successive con kernel `linux-aws`

> **Note**
>
> AWS I tipi di istanza basati su Graviton richiedono Ubuntu 18.04 o versione successiva con kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 o versioni successive
- SUSE Linux Enterprise Server 12 SP2 o versioni successive
- CentOS 7.4.1708 o versioni successive
- FreeBSD 11.1 o versioni successive
- Debian GNU/Linux 9 o versioni successive

Per verificare se la rete avanzata è già abilitata, verifica che il `ena` modulo sia installato sull'istanza e che l'attributo sia impostato. `enaSupport` In tal caso, il comando ethtool -i eth***n*** dovrebbe mostrare che il modulo è in uso nell'interfaccia di rete.

Modulo kernel (ena)

Per verificare se il modulo `ena` è installato, utilizza il comando modinfo come descritto nell'esempio seguente:

```
[ec2-user ~]$ modinfo ena
filename:    /lib/modules/4.14.33-59.37.amzn2.x86_64/kernel/drivers/amazon/net/ena/
ena.ko
version:  1.5.0g
```

```
license:  GPL
description: Elastic Network Adapter (ENA)
author:   Amazon.com, Inc. or its affiliates
srcversion:  692C7C68B8A9001CB3F31D0
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
retpoline:   Y
intree:   Y
name:     ena
...
```

Nell'istanza Amazon Linux, il `ena` modulo è installato.

```
ubuntu:~$ modinfo ena
ERROR: modinfo: could not find module ena
```

Nell'istanza di Ubuntu, il modulo non è installato, quindi devi prima installarlo. Per ulteriori informazioni, consulta Ubuntu.

Verifica dell'abilitazione delle reti avanzate

Puoi verificare se la rete avanzata è abilitata nelle tue istanze o nelle tue AMI.

Attributo di ist

Per controllare se per un'istanza è stato impostato l'attributo `enaSupport` per le reti avanzate, utilizza uno dei seguenti comandi. Se l'attributo è impostato, viene restituito true.

- describe-instances (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query
 "Reservations[].Instances[].EnaSupport"
```

- Get-EC2Instance(Strumenti per Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

Attributo dell'immagine

Per controllare se per un'AMI è stato impostato l'attributo `enaSupport` per le reti avanzate, utilizza uno dei seguenti comandi. Se l'attributo è impostato, viene restituito true.

- describe-images (AWS CLI/AWS CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[].EnaSupport"
```

- Get-EC2Image(Strumenti per Windows PowerShell)

```
(Get-EC2Image -ImageId ami_id).EnaSupport
```

Driver di interfaccia di rete Linux

Utilizza il comando seguente per verificare se il modulo `ena` viene utilizzato su un'interfaccia specifica, sostituendo il nome dell'interfaccia che desideri controllare. Se usi una singola interfaccia (impostazione predefinita), essa sarà `eth0`. Se il sistema operativo supporta nomi di rete prevedibili, questo potrebbe essere un nome simile a `ens5`.

Nell'esempio seguente, il modulo `ena` non viene caricato, perché il driver nell'elenco è `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

In questo caso, il modulo `ena` è caricato con la versione minima consigliata. Questa istanza dispone della funzionalità per reti avanzate adeguatamente configurata.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
```

```
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Abilitazione delle reti avanzate su un'istanza

La procedura da utilizzare dipende dal sistema operativo dell'istanza.

Amazon Linux

Amazon Linux 2 e le ultime versioni di AMI Amazon Linux includono il modulo necessario per migliorare la rete con ENA installato e hanno il supporto ENA abilitato. Pertanto, se si avvia un'istanza con una versione HVM di Amazon Linux su un tipo di istanza supportato, l'istanza dispone già dell'abilitazione delle reti avanzate. Per ulteriori informazioni, consulta Verifica dell'abilitazione delle reti avanzate.

Se l'istanza è stata avviata utilizzando una AMI Amazon Linux più vecchia che non dispone delle reti avanzate già abilitate, utilizzare la seguente procedura per abilitare le reti avanzate.

Per abilitare le reti avanzate su Amazon Linux AMI

1. Connettiti alla tua istanza.
2. Dall'istanza, esegui il seguente comando per aggiornare l'istanza in base al nuovo kernel e ai nuovi moduli kernel, compreso `ena`:

   ```
   [ec2-user ~]$ sudo yum update
   ```
3. Dal computer locale, riavvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: reboot-instances (AWS CLI), Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Ricollegati all'istanza e verifica che il modulo `ena` sia installato con la versione minima consigliata utilizzando il comando modinfo ena disponibile in Verifica dell'abilitazione delle reti avanzate.
5. [Istanza supportata da EBS] Dal computer locale, arresta l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario interromperla nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.

[Istanza supportata da instance store] Non è possibile arrestare l'istanza per modificare l'attributo. Segui invece questa procedura: Per abilitare le reti avanzate su AMI Amazon Linux (istanze supportate da instance store).

6. Dal computer locale, abilita l'attributo relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

   - Edit-EC2InstanceAttribute(Strumenti per Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
     ```

7. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un'AMI supportata da Amazon EBS. L'AMI eredita l'attributo `enaSupport` relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.
8. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario avviare l'istanza nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.
9. Connettiti all'istanza e verifica che il modulo `ena` sia installato e caricato sull'interfaccia di rete in uso tramite il comando ethtool -i eth*n* disponibile in Verifica dell'abilitazione delle reti avanzate.

   Se è impossibile connettersi all'istanza dopo aver abilitato le reti avanzate, consulta Risolvere i problemi relativi all'Elastic Network Adapter su Linux.

Per abilitare le reti avanzate su AMI Amazon Linux (istanze supportate da instance store)

Segui la procedura precedente fino al punto in cui si arresta l'istanza. Crea una nuova AMI come descritto in Creazione di un'AMI Linux supportata da un instance store, assicurandoti di abilitare l'attributo relativo alle reti avanzate durante la registrazione dell'AMI.

- register-image (AWS CLI)

  ```
  aws ec2 register-image --ena-support ...
  ```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

Ubuntu

Le più recenti AMI HVM di Ubuntu includono il modulo necessario per migliorare il networking con ENA installato e hanno il supporto ENA abilitato. Pertanto, se si avvia un'istanza con la più recente versione Ubuntu HVM AMI; su un tipo di istanza supportato, l'istanza dispone già dell'abilitazione delle reti avanzate. Per ulteriori informazioni, consulta Verifica dell'abilitazione delle reti avanzate.

Se l'istanza è stata avviata utilizzando un'AMI di una versione precedente per la quale la funzionalità di reti avanzate non è abilitata, puoi installare il pacchetto kernel `linux-aws` per avere i driver di rete ottimizzati più recenti e aggiornare l'attributo richiesto.

Come installare il pacchetto **`linux-aws`** kernel (Ubuntu 16.04 o versioni successive)

Ubuntu 16.04 e 18.04 vengono forniti con il kernel personalizzato Ubuntu (pacchetto kernel `linux-aws`). Per usare un kernel diverso, contatta AWS Support.

Come installare il pacchetto **`linux-aws`** kernel (Ubuntu Trusty 14.04)

1. Connettiti alla tua istanza.
2. Aggiorna la cache dei pacchetti e i pacchetti.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Se durante il processo di aggiornamento viene richiesto di installare `grub`, utilizza `/dev/xvda` per installare `grub`, quindi scegli di conservare la versione corrente di `/boot/grub/menu.lst`.

3. [Istanza supportata da EBS] Dal computer locale, arresta l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario interromperla nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.

[Istanza supportata da instance store] Non è possibile arrestare l'istanza per modificare l'attributo. Segui invece questa procedura: Per abilitare le reti avanzate su Ubuntu (istanze supportate da instance store).

4. Dal computer locale, abilita l'attributo relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

   - Edit-EC2InstanceAttribute(Strumenti per Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
     ```

5. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un'AMI supportata da Amazon EBS. L'AMI eredita l'attributo `enaSupport` relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.
6. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario avviare l'istanza nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.

Per abilitare le reti avanzate su Ubuntu (istanze supportate da instance store)

Segui la procedura precedente fino al punto in cui si arresta l'istanza. Crea una nuova AMI come descritto in Creazione di un'AMI Linux supportata da un instance store, assicurandoti di abilitare l'attributo relativo alle reti avanzate durante la registrazione dell'AMI.

- register-image (AWS CLI)

  ```
  aws ec2 register-image --ena-support ...
  ```

- Register-EC2Image (AWS Tools for Windows PowerShell)

  ```
  Register-EC2Image -EnaSupport $true ...
  ```

RHEL, SUSE, CentOS

Le più recenti AMI per Red Hat Enterprise Linux, SUSE Linux Enterprise Server e CentOS includono il modulo necessario per migliorare la rete con ENA e hanno il supporto ENA abilitato. Pertanto, se si lancia un'istanza con la più recente versione di AMI su un tipo di istanza supportato, l'istanza dispone già dell'abilitazione delle reti avanzate. Per ulteriori informazioni, consulta Verifica dell'abilitazione delle reti avanzate.

La procedura seguente descrive le fasi generali per abilitare le reti avanzate ENA su una distribuzione Linux diversa da AMI Amazon Linux o Ubuntu. Per ulteriori informazioni, ad esempio sintassi dettagliata dei comandi, posizione dei file o supporto di pacchetti e strumenti, consulta la documentazione per la distribuzione Linux in uso.

Per abilitare le reti avanzate su Linux

1. Connettiti alla tua istanza.
2. Clona il codice sorgente del `ena` modulo sulla tua istanza da at. GitHub https://github.com/amzn/amzn-drivers (SUSE Linux Enterprise Server 12 SP2 e versioni successive includono ENA 2.02 per impostazione predefinita, pertanto non è necessario scaricare e compilare il driver ENA. Per SUSE Linux Enterprise Server 12 SP2 e versioni successive, è necessario presentare una richiesta per aggiungere la versione del driver che si desidera al kernel di serie).

   ```
   git clone https://github.com/amzn/amzn-drivers
   ```

3. Compila e installa il modulo `ena` sull'istanza. Questi passaggi dipendono dalla distribuzione Linux. Per ulteriori informazioni sulla compilazione del modulo su Red Hat Enterprise Linux, consulta Come installare il driver ENS più recente per un supporto di rete avanzato su un'istanza Amazon EC2 che esegue RHEL?
4. Esegui il comando sudo depmod per aggiornare le dipendenze del modulo.
5. Aggiorna `initramfs` sull'istanza in modo che il nuovo modulo venga caricato in fase di avvio. Ad esempio, se la distribuzione supporta dracut, è possibile utilizzare il seguente comando:

   ```
   dracut -f -v
   ```

6. Determina se il sistema utilizza nomi di interfaccia di rete prevedibili per impostazione di default. I sistemi che utilizzano systemd o udev versione 197 o successive possono rinominare i dispositivi Ethernet e pertanto non garantiscono che la singola interfaccia di rete venga rinominata in `eth0`. Questo comportamento potrebbe causare problemi durante la connessione all'istanza. Per

ulteriori informazioni e per informazioni sulle altre opzioni di configurazione disponibili, consulta l'argomento relativo ai nomi di interfaccia di rete prevedibili sul sito Web freedesktop.org.

a. È possibile controllare le versioni di systemd o udev sui sistemi basati su RPM utilizzando il seguente comando:

```
rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
systemd-208-11.el7_0.2.x86_64
```

Nell'esempio precedente relativo a Red Hat Enterprise Linux 7, la versione di systemd è 208, pertanto, i nomi di interfaccia di rete prevedibili devono essere disabilitati.

b. Disabilitare i nomi di interfaccia di rete prevedibili aggiungendo l'opzione `net.ifnames=0` alla riga `GRUB_CMDLINE_LINUX` in `/etc/default/grub`.

```
sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/
grub
```

c. Ricompila il file di configurazione di grub.

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Istanza supportata da EBS] Dal computer locale, arresta l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario interromperla nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.

   [Istanza supportata da instance store] Non è possibile arrestare l'istanza per modificare l'attributo. Segui invece questa procedura: Per abilitare le reti avanzate su Linux (istanze supportate da archivio istanze).

8. Dal computer locale, abilita l'attributo `enaSupport` relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   - modify-instance-attribute (AWS CLI)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
   ```

   - Edit-EC2InstanceAttribute(Strumenti per Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
   ```

9. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un'AMI supportata da Amazon EBS. L'AMI eredita l'attributo `enaSupport` relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.

   Se il sistema operativo dell'istanza contiene un file `/etc/udev/rules.d/70-persistent-net.rules`, è necessario eliminarlo prima di creare l'AMI. Questo file contiene l'indirizzo MAC per la scheda Ethernet dell'istanza originale. Se un'altra istanza viene avviata con questo file, il sistema operativo non sarà in grado di trovare il dispositivo ed `eth0` potrebbe non funzionare causando problemi di avvio. Questo file viene rigenerato al successivo ciclo di avvio e qualsiasi istanza avviata dall'AMI crea la propria versione del file.

10. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario avviare l'istanza nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.

11. (Facoltativo) Connettiti all'istanza e verifica che il modulo sia installato.

    Se è impossibile connettersi all'istanza dopo aver abilitato le reti avanzate, consulta Risolvere i problemi relativi all'Elastic Network Adapter su Linux.

Per abilitare le reti avanzate su Linux (istanze supportate da archivio istanze)

Segui la procedura precedente fino al punto in cui si arresta l'istanza. Crea una nuova AMI come descritto in Creazione di un'AMI Linux supportata da un instance store, assicurandoti di abilitare l'attributo relativo alle reti avanzate durante la registrazione dell'AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu con DKMS

Questo metodo è solo per scopi di test e feedback. Non è pensato per l'utilizzo con distribuzioni di produzione. Per distribuzioni di produzione, consulta Ubuntu.

> **Important**
>
> L'uso di DKMS annulla il contratto di assistenza per l'abbonamento. Non deve essere utilizzato per le distribuzioni di produzione.

Per abilitare le reti avanzate con ENA su Ubuntu (istanze supportate da EBS)

1. Seguire le fasi 1 e 2 in Ubuntu.
2. Installare i pacchetti `build-essential` per compilare il modulo del kernel e il pacchetto `dkms` in modo che il modulo `ena` venga ricompilato a ogni aggiornamento del kernel.

   ```
   ubuntu:~$ sudo apt-get install -y build-essential dkms
   ```

3. Clona il codice sorgente del `ena` modulo sulla tua istanza da GitHub at. https://github.com/amzn/amzn-drivers

   ```
   ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
   ```

4. Spostare il pacchetto `amzn-drivers` nella directory `/usr/src/` in modo che DKMS riesca a individuarlo e compilarlo per ogni aggiornamento del kernel. Aggiungere il numero di versione (il numero di versione corrente è disponibile nelle note di rilascio) del codice sorgente al nome della directory. Nell'esempio seguente viene visualizzata la seguente versione `1.0.0`.

   ```
   ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
   ```

5. Creare il file di configurazione DKMS con i seguenti valori, sostituendo la versione in uso di `ena`.

   Creare il file.

   ```
   ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
   ```

   Modificare il file e aggiungere i valori seguenti.

   ```
   ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
   ```

```
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Aggiungere, compilare e installare il modulo `ena` sull'istanza utilizzando DKMS.

   Aggiungere il modulo a DKMS.

   ```
   ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
   ```

   Compilare il modulo utilizzando il comando dkms.

   ```
   ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
   ```

   Installare il modulo utilizzando dkms.

   ```
   ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
   ```

7. Ricompilare `initramfs` in modo che il modulo corretto venga caricato in fase di avvio.

   ```
   ubuntu:~$ sudo update-initramfs -u -k all
   ```

8. Verificare che il modulo `ena` sia installato utilizzando il comando modinfo ena disponibile in Verifica dell'abilitazione delle reti avanzate.

   ```
   ubuntu:~$ modinfo ena
   filename:    /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
   version:  1.0.0
   license:  GPL
   description: Elastic Network Adapter (ENA)
   author:   Amazon.com, Inc. or its affiliates
   srcversion:  9693C876C54CA64AE48F0CA
   alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
   alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
   alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
   ```

```
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:    3.13.0-74-generic SMP mod_unload modversions
parm:     debug:Debug level (0=none,...,16=all) (int)
parm:     push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
     0 - Automatically choose according to device capability (default)
     1 - Don't push anything to device memory
     3 - Push descriptors and header buffer to device memory (int)
parm:     enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:     enable_missing_tx_detection:Enable missing Tx completions. (default=1)
 (int)
parm:     numa_node_override_array:Numa node override map
 (array of int)
parm:     numa_node_override:Enable/Disable numa node override (0=disable)
 (int)
```

9. Continuare con la fase 3 in Ubuntu.

Abilitazione delle reti avanzate su Windows

Se hai avviato l'istanza per la quale la funzionalità di reti avanzate non è già abilitata, devi scaricare e installare il driver per la scheda di rete richiesto sull'istanza e quindi impostare l'attributo `enaSupport` dell'istanza in modo da attivare le reti avanzate. Puoi abilitare questo attributo solo sui tipi di istanza supportati e solo se il driver ENA è installato. Per ulteriori informazioni, consulta Supporto di reti avanzate.

Per abilitare le reti avanzate

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. [Solo Windows Server 2016 e 2019] Esegui il seguente PowerShell script EC2Launch per configurare l'istanza dopo l'installazione del driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

3. Dall'istanza, installare il driver nel seguente modo:
   a. Scarica il driver più recente per l'istanza.
   b. Estrai l'archivio .zip.
   c. Installa il driver eseguendo lo `install.ps1` PowerShell script.

> **Note**
>
> Se si verifica un errore della policy di esecuzione, impostare la policy su `Unrestricted` (per impostazione predefinita è impostata su `Restricted` o `RemoteSigned`). In una riga di comando`Set-ExecutionPolicy -ExecutionPolicy Unrestricted`, esegui e quindi esegui nuovamente `install.ps1` PowerShell lo script.

4. Dal computer locale, arresta l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: stop-instances (AWS CLI/AWS CloudShell), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario interromperla nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.
5. Abilita il supporto ENA sull'istanza nel seguente modo:

   a. Dal computer locale, controlla l'attributo relativo al supporto ENA per l'istanza EC2 sull'istanza eseguendo uno dei seguenti comandi. Se l'attributo non è abilitato, l'output riporterà "[]" o sarà vuoto. `EnaSupport` è configurato su `false` per impostazione predefinita.

   - describe-instances (AWS CLI/AWS CloudShell)

     ```
     aws ec2 describe-instances --instance-ids instance_id --query
      "Reservations[].Instances[].EnaSupport"
     ```

   - Get-EC2Instance(Strumenti per Windows PowerShell)

     ```
     (Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
     ```

   b. Per abilitare il supporto ENA, esegui uno dei comandi riportati di seguito:

   - modify-instance-attribute (AWS CLI/AWS CloudShell)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

   - Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
     ```

Se si verificano problemi durante il riavvio dell'istanza, è possibile disabilitare il supporto ENA utilizzando uno dei seguenti comandi:

- modify-instance-attribute (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $false
```

c. Verifica che l'attributo sia stato impostato su `true` utilizzando describe-instances o Get-EC2Instance come descritto in precedenza. Ora l'output restituito sarà simile al seguente:

```
[
 true
]
```

6. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI/AWS CloudShell), Start-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario avviarla utilizzando la AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.
7. Nell'istanza, verifica che il driver ENA sia installato e abilitato nel seguente modo:

   a. Fai clic con il pulsante destro del mouse sull'icona di rete e scegli Open Network and Sharing Center (Apri centro connessioni di rete e condivisione).

   b. Seleziona la scheda Ethernet (ad esempio, Ethernet 2).

   c. Seleziona Details (Dettagli). In Network Connection Details (Dettagli connessione di rete), verifica che nel campo Description (Descrizione) sia visualizzato Amazon Elastic Network Adapter.

8. (Facoltativo) Crea un'AMI dall'istanza. L'AMI eredita l'attributo `enaSupport` dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con ENA abilitato per impostazione di default.

Note di rilascio del driver

Driver ENA per Linux

Per informazioni sulle versioni del driver ENA Linux, consulta le note di rilascio del driver del kernel ENA Linux.

Driver ENA per Windows

Le AMI di Windows includono il driver Amazon ENA per abilitare le reti avanzate.

La tabella seguente mostra la versione corrispondente del driver ENA da scaricare per ciascuna versione di Windows Server.

Versione di Windows Server	Versione driver ENA
Windows Server 2022	Versione 2.4.0 e successive
Windows Server 2019	più recente
Windows Server 2016	più recente
Windows Server 2012 R2	2.6.0 e precedenti
Windows Server 2012	2.6.0 e precedenti
Windows Server 2008 R2	versioni 2.2.3 e precedenti

Nella tabella seguente sono riepilogate le modifiche relative a ciascuna versione.

Versione driver	Dettagli	Data di rilascio
2.7.0	Nuove caratteristiche • È stato rimosso il supporto per Windows Server 2012 (Windows 8) e Windows Server 2012 R2 (Windows 8.1). Queste versioni del sistema operativo hanno	1 maggio 2024

Versione driver	Dettagli	Data di rilascio
	raggiunto la fine del supporto da AWS. L'installazione del driver non riuscirà in Windows Server 2012 e versioni precedenti. • È stato aggiunto il supporto per l'offload del calcolo del checksum Tx IPv6 sul dispositivo. • È stato aggiunto un ampio supporto per Low Latency Queuing (LLQ). Questo è abilitato dinamicamente in base alle raccomandazioni del dispositivo. È possibile sovrascrivere questa impostazione con la nuova chiave di registro «WideLLQ». • È stata aggiunta la segnalazione delle cadute di pacchetti dovute al sovraccarico di Rx, che indica uno spazio insufficiente nell'anello Rx per i pacchetti in entrata. • È stato aggiunto il supporto per le notifiche di configura zione non ottimali provenienti dal dispositivo. Vedi l'ID dell'evento `59000` nel visualizzatore eventi di Windows. Correzioni di bug • Evita il ripristino non necessario del dispositivo causato da pacchetti Tx con intestazioni che superano la dimensione massima dell'intestazione Low Latency Queuing (LLQ).	

Versione driver	Dettagli	Data di rilascio

2.6.0	Nuove caratteristiche
	• Aggiunge i seguenti parametri delle prestazioni di rete per i tipi di istanze che supportano ENA Express.
	  • `ena_srd_mode`
	  • `ena_srd_tx_pkts`
	  • `ena_srd_eligible_tx_pkts`
	  • `ena_srd_rx_pkts`
	  • `ena_srd_resource_utilization`
	• Aggiunge il parametro delle prestazioni di rete `conntrack_allowance_available` per i tipi di istanze basati su Nitro.
	• Aggiunge un nuovo motivo di ripristino dell'adattatore dovuto al rilevamento di un danneggiamento dei dati RX.
	• Aggiorna l'infrastruttura di registrazione dei driver.
	
	Correzioni di bug
	• Impedisce il ripristino dell'adattatore nel caso in cui l'esaurimento della CPU causi il fallimento dell'aggi ornamento dei parametri delle prestazioni di rete.
	• Impedisce la falsa rilevazione di un'interruzione dell'heartbeat del dispositivo.
		20 giugno 2023

Versione driver	Dettagli	Data di rilascio
	• Corregge lo script di installazione del driver per supportare l'operazione di downgrade. • Corregge la statistica del conteggio degli errori di ricezione.	
2.5.0	Annuncio È stata ripristinata la versione 2.5.0 del driver ENA per Windows a causa della mancata inizializzazione sul controller di dominio Windows. Windows Client e Windows Server non sono stati interessati.	17 febbraio 2023

Versione driver	Dettagli	Data di rilascio
24,0	Nuove caratteristiche • Aggiunto il supporto per Windows Server 2022. • Rimosso il supporto per Windows Server 2008 R2. • Imposta LLQ (Low Latency Queuing) su sempre attivo per migliorare le prestazioni delle istanze Amazon EC2 di sesta generazione. Correzioni di bug • Corregge la mancata pubblicazione dei parametri delle prestazioni di rete nel sistema PCW di unità di conteggio delle prestazioni di Windows. • Corregge una perdita di memoria durante l'operazione di lettura della chiave di registro. • Impedisce un ciclo di ripristino infinito in caso di errore irrecuperabile durante il processo di ripristino dell'adattatore.	28 aprile 2022

Versione driver	Dettagli	Data di rilascio

2.2.4	Annuncio
	
	È stato eseguito il ripristino dello stato precedente del driver ENA Windows versione 2.2.4 a causa del potenziale peggioramento delle prestazioni nelle istanze EC2 di sesta generazione. È consigliabile eseguire il downgrade del driver, usando uno dei metodi seguenti:
	
	• Installazione della versione precedente
	
	1. Scarica la versione precedente del pacchetto dal collegamento in questa tabella (versione 2.2.3).
	2. Esegui lo script install.ps1 PowerShell di installazione.
	
	Per ulteriori dettagli sulle fasi di pre-installazione e post-installazione, consulta Abilitazione delle reti avanzate su Windows.
	
	Utilizzo di Amazon EC2 Systems Manager per un aggiornamento in blocco
	
	• Esegui un aggiornamento in blocco tramite il documento SSM `AWS-ConfigureAWSPackage` , con i seguenti parametri:
	  • Nome: AwsEnaNetworkDriver
	  • Versione: 2.2.3
		26 ottobre 2021

Versione driver	Dettagli	Data di rilascio
2.2.3	Nuova caratteristica • Aggiunge il supporto per le nuove schede Nitro con reti di istanze fino a 400 Gbps. Correzioni di bug • Corregge la race condition tra la modifica dell'ora di sistema e la query sull'ora di sistema da parte del driver ENA, che causa il rilevamento di falsi positivi della mancata risposta dell'hardware. Il driver Windows ENA versione 2.2.3 è la versione finale che supporta Windows Server 2008 R2. I tipi di istanza attualmente disponibili che utilizzano ENA continuer anno a essere supportati su Windows Server 2008 R2 e i driver sono disponibili per download. Nessun tipo di istanza futuro supporta Windows Server 2008 R2 e non è possibile avviare, importare o migrare immagini di Windows Server 2008 R2 a tipi di istanza futuri.	25 marzo 2021

Versione driver	Dettagli	Data di rilascio
2.2.2	Nuova caratteristica • Aggiunge il supporto per interrogare le metriche delle prestazioni degli adattatori di rete con CloudWatch i contatori delle prestazioni per gli utenti Windows. Correzioni di bug • Risolve i problemi di prestazioni nelle istanze bare metal.	21 dicembre 2020
2.2.1	Nuova caratteristica • Aggiunge un metodo per consentire all'host di eseguire query sulla Elastic Network Adapter per le metriche delle prestazioni di rete.	1 ottobre 2020

Versione driver	Dettagli	Data di rilascio
2.2.0	Nuove caratteristiche • Aggiunge il supporto per i tipi di hardware di nuova generazione. • Migliora il tempo di avvio dell'istanza dopo la ripresa dall'arresto correlato all'ibernazione ed elimina i messaggi di errore ENA falsi positivi. Ottimizzazione delle prestazioni • Ottimizza l'elaborazione del traffico in entrata. • Migliora la gestione della memoria condivisa in ambienti con risorse limitate. Correzioni di bug • Evita crash del sistema dopo la rimozione del dispositivo ENA in rari scenari in cui il driver non riesce a eseguire il reset.	12 agosto 2020
2.1.5	Correzioni di bug • Corregge errori di inizializzazione occasionali della scheda di rete nelle istanze Bare Metal.	23 giugno 2020

Versione driver	Dettagli	Data di rilascio
2.1.4	Correzioni di bug • Impedire problemi di connettività causati da metadati del pacchetto LSO danneggiato in arrivo dallo stack di rete. • Impedire l'arresto anomalo del sistema causato da una race condition rara che comporta l'accesso a memoria pacchetto già rilasciata.	25 novembre 2019
2.1.2	Nuova caratteristica • Aggiunto supporto per report ID fornitore per consentire al sistema operativo di generare UUID basati su MAC. Correzioni di bug • Migliorate le prestazioni di configurazione di rete DHCP durante l'inizializzazione. • Checksum L4 calcolato correttamente sul traffico IPv6 in ingresso quando l'unità di trasmissione massima (MTU) supera 4K. • Miglioramenti generali alla stabilità del driver e correzioni di bug di minore entità.	4 novembre 2019

Versione driver	Dettagli	Data di rilascio
2.1.1	Correzioni di bug • Evita la perdita di pacchetti TCP LSO altamente frammentati provenienti dal sistema operativo. • Gestisce correttamente il protocollo Encapsulating Security Payload (ESP) all'interno dell'IPSec nelle reti IPv6.	16 settembre 2019

Versione driver	Dettagli	Data di rilascio

2.1.0	Il driver ENA Windows v2.1 introduce nuove capacità dei dispositivi ENA, offre ottimizzazione delle prestazioni, aggiunge nuove funzionalità e include molteplici miglioramenti alla stabilità.
	• Nuove caratteristiche
	  • Uso della chiave di registro Windows standardizzata per la configurazione dei frame Jumbo.
	  • Possibilità di impostare l'ID VLAN mediante la GUI delle proprietà del driver ENA.
	  • Flussi di ripristino migliorati
	  • Meccanismo di identificazione degli errori migliorato.
	  • Aggiunta del supporto per i parametri i ripristino regolabili.
	  • Supporto fino a un massimo di 32 code di I/O per le istanze EC2 più recenti con più di 8 vCPU.
	  • ~90% di riduzione del footprint di memoria dei driver.
	• Ottimizzazione delle prestazioni
	  • Latenza ridotta del percorso di trasmissione
	  • Supporto per offload di checksum di ricezione.
	  • Ottimizzazione delle prestazioni per sistemi a carico elevato (uso ottimizzato dei meccanismi di blocco).
	  •
		1 luglio 2019

Versione driver	Dettagli	Data di rilascio

	Ulteriori miglioramenti per ridurre l'uso della CPU e potenziare la capacità di risposta del sistema sotto carico.
	• Correzioni di bug
	  • Correzione degli arresti anomali dovuti ad analisi non valida o intestazioni Tx non contigue.
	  • Correzione degli arresti anomali del driver v1.5 durante lo scollegamento dall'interfaccia di rete elastica su istanze Bare Metal.
	  • Correzione degli errori di calcolo di checksum delle pseudo-intestazioni LSO su IPv6.
	  • Correzione della potenziale perdita di risorse di memoria in fase di errore di inizializzazione.
	  • Disabilitazione dell'offload di checksum TCP/UDP per i frammenti IPv4.
	  • Correzione della configurazione VLAN. La rete VLAN è stata disabilitata per errore laddove avrebbe dovuto essere disabilitata solo la priorità VLAN.
	  • Abilitazione della corretta analisi dei messaggi del driver personalizzato da parte del visualizzatore eventi.
	  • Correzione degli errori di inizializzazione del driver per una gestione non valida del timestamp.
	  • Correzione della race condition tra l'elaborazione dei dati e la disabilitazione dei dispositivi ENA.	

Versione driver	Dettagli	Data di rilascio
1.5.0	• Maggiore stabilità e correzioni relative alle prestazioni. • I buffer di ricezione possono ora essere configurati fino a un valore di 8192 in Proprietà avanzate del NIC ENA. • Buffer di ricezione predefinito di 1k.	4 ottobre 2018
1.2.3	Include le correzioni relative all'affidabilità e unifica il supporto per Windows Server 2008 R2 mediante Windows Server 2016.	13 febbraio 2018
1.0.8	Versione iniziale. Incluso nelle AMI per Windows Server 2008 R2, Windows Server 2012 RTM, Windows Server 2012 R2 e Windows Server 2016.	2016 luglio

Amazon SNS può avvisarti in caso di pubblicazione di nuove versioni dei driver Windows di EC2. Utilizza la procedura seguente per effettuare l'iscrizione a queste notifiche.

Per sottoscrivere alle notifiche EC2

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario selezionare questa regione perché le notifiche SNS per le quali stai effettuando la sottoscrizione si trovano in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Create subscription (Crea sottoscrizione) segui questi passaggi:
   a. In Topic ARN (ARN argomento) copia il seguente nome della risorsa Amazon (ARN):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

   b. In Protocol (Protocollo), scegli `Email`.

c. In Endpoint immetti l'indirizzo e-mail utilizzabile per ricevere le notifiche.

d. Scegli Create Subscription (Crea sottoscrizione).

6. Riceverai a breve un'e-mail di conferma. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

Quando i nuovi driver Windows di EC2 vengono rilasciati, inviamo notifiche ai sottoscrittori. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Per annullare la sottoscrizione alle notifiche dei driver Windows per Amazon EC2

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
3. Selezionare la casella di spunta della sottoscrizione, quindi scegliere Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni). Quando viene richiesta la conferma, selezionare Delete (Elimina).

Migliora le prestazioni di rete con ENA Express sulle tue istanze EC2

ENA Express è alimentato dalla tecnologia AWS Scalable Reliable Datagram (SRD). SRD è un protocollo di trasporto di rete ad alte prestazioni che utilizza l'instradamento dinamico per aumentare la velocità di trasmissione effettiva e ridurre al minimo la latenza di coda. Con ENA Express, puoi comunicare tra due istanze EC2 nella stessa zona di disponibilità.

Vantaggi di ENA Express

- Aumenta la larghezza di banda massima che un singolo flusso può utilizzare da 5 Gbps a 25 Gbps all'interno della zona di disponibilità, fino al limite delle istanze aggregate.
- Riduce la latenza di coda del traffico di rete tra le istanze EC2, specialmente durante i periodi di elevato carico di rete.
- Rileva ed evita i percorsi di rete congestionati.
- Gestisce alcune attività direttamente a livello di rete, come il riordino dei pacchetti sul lato di ricezione e la maggior parte delle ritrasmissioni necessarie. Questo libera il livello dell'applicazione per altre attività.

> **Note**
>
> Se l'applicazione invia o riceve un volume elevato di pacchetti al secondo e deve ottimizzare la latenza per la maggior parte del tempo, specialmente nei periodi in cui la rete non è congestionata, Reti avanzate potrebbe essere la soluzione più adatta alla rete.

Durante i periodi di tempo in cui il traffico di rete è scarso, potresti notare un leggero aumento della latenza dei pacchetti (decine di microsecondi) quando il pacchetto utilizza ENA Express. In questi periodi, le applicazioni che danno priorità a specifiche caratteristiche prestazionali di rete possono trarre vantaggio da ENA Express come segue:

- I processi possono trarre vantaggio dall'aumento della larghezza di banda massima a flusso singolo da 5 Gbps a 25 Gbps all'interno della stessa zona di disponibilità, fino al limite di istanze aggregate. Ad esempio, se un tipo di istanza specifico supporta fino a 12,5 Gbps, anche la larghezza di banda a flusso singolo è limitata a 12,5 Gbps.
- I processi in esecuzione più a lungo termine dovrebbero avere una latenza di coda ridotta durante i periodi di congestione della rete.
- I processi possono trarre vantaggio da una distribuzione più fluida e standard per i tempi di risposta della rete.

Prerequisiti per le istanze Linux

Per garantire che ENA Express possa funzionare in modo efficace, aggiorna le impostazioni dell'istanza come segue.

- Se l'istanza utilizza frame jumbo, esegui il comando seguente per impostare la tua unità di trasmissione massima (MTU) su 8900.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- Aumenta la dimensione dell'anello ricevitore (Rx) nel modo seguente:

```
[ec2-user ~]$ ethtool -G device rx 8192
```

- Per massimizzare la larghezza di banda di ENA Express, configura i limiti della coda TCP come segue:

1. Imposta il limite di coda ridotta TCP su 1 MB o più. Ciò aumenta i dati in coda per la trasmissione su un socket:

```
sudo sh -c 'echo 1048576 > /proc/sys/net/ipv4/tcp_limit_output_bytes'
```

2. Disabilita i limiti della coda di byte sul dispositivo eth se sono abilitati per la tua distribuzione Linux. Ciò aumenta anche i dati in coda per la trasmissione, ma a livello di coda del dispositivo:

```
sudo sh -c 'for txq in /sys/class/net/eth0/queues/tx-*; do echo max > ${txq}/
byte_queue_limits/limit_min; done'
```

> **Note**
>
> Il driver ENA per la distribuzione Amazon Linux disattiva i limiti delle code di byte per impostazione predefinita.

Come funziona ENA Express

ENA Express è alimentato dalla tecnologia AWS Scalable Reliable Datagram (SRD). Distribuisce i pacchetti per ogni flusso di rete su diversi AWS percorsi di rete e regola dinamicamente la distribuzione quando rileva segni di congestione. Gestisce anche il riordino dei pacchetti sul lato di ricezione.

Per garantire che ENA Express sia in grado di gestire il traffico di rete come previsto, le istanze di invio e ricezione e la comunicazione tra di esse devono soddisfare tutti i seguenti requisiti:

- Sono supportati i tipi sia delle istanze di invio sia di quelle di ricezione. Per ulteriori informazioni, consulta la tabella Tipi di istanza supportati per ENA Express.
- Sia le istanze di invio sia quelle di ricezione devono avere ENA Express configurato. Se esistono differenze nella configurazione, si possono verificare situazioni in cui il traffico è impostato automaticamente sulla trasmissione ENA standard. Lo scenario seguente mostra ciò che accade in questo caso.

  Scenario: differenze nella configurazione

Istanza	ENA Express abilitato	UDP utilizza ENA Express
Istanza 1	Sì	Sì
Istanza 2	Sì	No

In questo caso, il traffico TCP tra le due istanze può utilizzare ENA Express, poiché è abilitato su entrambe le istanze. Tuttavia, poiché una delle istanze non utilizza ENA Express per il traffico UDP, la comunicazione tra queste due istanze tramite UDP utilizza la trasmissione ENA standard.

- Le istanze di invio e ricezione devono essere eseguite nella stessa zona di disponibilità.
- Il percorso di rete tra le istanze non deve includere box middleware (software intermediario). ENA Express attualmente non supporta i box middleware (software intermediario).
- (Solo istanze Linux) Per sfruttare tutto il potenziale della larghezza di banda, utilizzate la versione del driver 2.2.9 o successiva.
- (Solo istanze Linux) Per generare parametri, utilizzate la versione del driver 2.8 o successiva.

Se qualche requisito non è soddisfatto, le istanze utilizzano il protocollo TCP/UDP standard ma senza SRD per comunicare.

Per assicurarti che il driver di rete dell'istanza sia configurato per prestazioni ottimali, consulta le best practice consigliate per i driver ENA. Queste best practice si applicano anche a ENA Express. Per ulteriori informazioni, consulta la Guida alle migliori pratiche e all'ottimizzazione delle prestazioni dei driver ENA Linux sul GitHub sito Web.

> **Note**
>
> Per Amazon EC2, una relazione tra un'istanza e un'interfaccia di rete a essa collegata è un collegamento. Le impostazioni di ENA Express si applicano al collegamento. Se l'interfaccia di rete è scollegata dall'istanza, il collegamento non esiste più e le impostazioni di ENA Express ad esso applicate non sono più valide. Lo stesso vale quando un'istanza viene terminata, anche se l'interfaccia di rete rimane.

Tipi di istanza supportati per ENA Express

Le seguenti schede mostrano i tipi di istanze che supportano ENA Express.

General purpose

Tipo di istanza	Architettura
m6a.12xlarge	x86_64
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64
m6i.metal	x86_64
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64

Tipo di istanza	Architettura
m6id.metal	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64

Compute optimized

Tipo di istanza	Architettura
c6a.12xlarge	x86_64
c6a.16xlarge	x86_64
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64

Tipo di istanza	Architettura
c6a.48xlarge	x86_64
c6a.metal	x86_64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64
c6id.metal	x86_64
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64

Tipo di istanza	Architettura
c7gd.metal	arm64
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24xl	x86_64
c7i.metal-48xl	x86_64

Memory optimized

Tipo di istanza	Architettura
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64
r6a.48xlarge	x86_64
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64

Tipo di istanza	Architettura
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64
r6id.32xlarge	x86_64
r6id.metal	x86_64
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64
r7i.12xlarge	x86_64
r7i.16xlarge	x86_64
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64
r7i.metal-24xl	x86_64
r7i.metal-48xl	x86_64

Tipo di istanza	Architettura
r8g.12xlarge	arm64
r8g.16xlarge	arm64
r8g.24xlarge	arm64
r8g.48xlarge	arm64
r8g.metal-24xl	arm64
r8g.metal-48xl	arm64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64

Accelerated computing

Tipo di istanza	Architettura
g6.48xlarge	x86_64

Storage optimized

Tipo di istanza	Architettura
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64
i4i.32xlarge	x86_64
i4i.metal	x86_64
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Elencazione e visualizzazione delle impostazioni di ENA Express

Questa sezione spiega come elencare e visualizzare le informazioni di ENA Express dalla AWS Management Console o dalla AWS CLI. Per ulteriori informazioni, scegli la scheda corrispondente al metodo che utilizzerai.

Console

Questa scheda spiega come trovare informazioni sulle impostazioni correnti di ENA Express e come visualizzare il supporto per i tipi di istanza nella AWS Management Console.

Visualizzazione del supporto dei tipi di istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Instance types (Tipi di istanza).
3. Seleziona un tipo di istanza per visualizzare i dettagli dell'istanza. Puoi scegliere il collegamento Instance type (Tipo di istanza) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco per visualizzare i dettagli nel riquadro dei dettagli in fondo alla pagina.
4. Nella scheda Networking (Reti) o nella rispettiva sezione sulla pagina dei dettagli, ENA Express support (Supporto di ENA Express) mostra un valore vero o falso per indicare se il tipo di istanza supporta questa funzionalità.

Visualizzazione delle impostazioni dall'elenco delle interfacce di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Network interfaces (Interfacce di rete).
3. Seleziona un'interfaccia di rete per visualizzare i dettagli relativi a quell'istanza. Puoi scegliere il collegamento Network interface ID (ID interfaccia di rete) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco per visualizzare i dettagli nel riquadro dei dettagli in fondo alla pagina.
4. Nella sezione Network interface attachment (Collegamento dell'interfaccia di rete) della scheda Details (Dettagli) o della pagina dei dettagli, rivedi le impostazioni per ENA Express ed ENA Express UDP

Visualizzazione delle impostazioni dalle istanze

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegliere Instances (Istanze).
3. Seleziona un'istanza per visualizzarne i dettagli. Puoi scegliere il collegamento Instance ID (ID dell'istanza) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco per visualizzare i dettagli nel riquadro dei dettagli in fondo alla pagina.

4. Nella sezione Network interfaces (Interfacce di rete) della schedaNetworking (Reti), scorri verso destra per rivedere le impostazioni per ENA Express ed ENA Express UDP.

AWS CLI

Questa scheda spiega come trovare informazioni sulle impostazioni correnti di ENA Express e come visualizzare il supporto per i tipi di istanza nella AWS CLI.

Descrizione dei tipi di istanza

Per informazioni sulle impostazioni del tipo di istanza per un tipo di istanza specifico, esegui il describe-instance-typescomando in e sostituisci il tipo di istanza come segue: AWS CLI

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-types m6i.metal
{
"InstanceTypes": [
{
 "InstanceType": "m6i.metal",
 "CurrentGeneration": true,
 ...
 },
 "NetworkInfo": {
  ...
  "EnaSrdSupported": true
 },
 ...
}
]
}
```

Descrivere le istanze

Per informazioni sulla configurazione di ENA Express per istanze specifiche, esegui il describe-instancescomando in AWS CLI, come segue. Questo esempio di comando restituisce un elenco di configurazioni ENA Express per le interfacce di rete collegate a ciascuna delle istanze in esecuzione specificate dal parametro. `--instance-ids`

```
[ec2-user ~]$ aws ec2 describe-instances --instance-
ids i-1234567890abcdef0 i-0598c7d356eba48d7 --query 'Reservations[*].Instances[*].
[InstanceId, NetworkInterfaces[*].Attachment.EnaSrdSpecification]'[
 [
```

```
  [
   "i-1234567890abcdef0",
   [
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ],
 [
  [
   "i-0598c7d356eba48d7",
   [
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ]
]
```

Descrizione delle interfacce di rete

Per informazioni sulle impostazioni ENA Express per un'interfaccia di rete, esegui il describe-network-interfacescomando nel modo seguente AWS CLI :

```
[ec2-user ~]$ aws ec2 describe-network-interfaces
{
"NetworkInterfaces": [
{
 "Association": {
  ....IPs, DNS...
 },
 "Attachment": {
  "AttachTime": "2022-11-17T09:04:28+00:00",
  "AttachmentId": "eni-attach-0ab1c23456d78e9f0",
  "DeleteOnTermination": true,
```

```
  "DeviceIndex": 0,
  "NetworkCardIndex": 0,
  "InstanceId": "i-1234567890abcdef0",
  "InstanceOwnerId": "111122223333",
  "Status": "attached",
  "EnaSrdSpecification": {
   "EnaSrdEnabled": true,
   "EnaSrdUdpSpecification": {
    "EnaSrdUdpEnabled": true
   }
  }
 },
 ...
 "NetworkInterfaceId": "eni-1234567890abcdef0",
 "OwnerId": "111122223333",
 ...
}
]
}
```

PowerShell

Questa scheda spiega come trovare informazioni sulle impostazioni correnti di ENA Express e visualizzare il supporto per i tipi di istanza utilizzati PowerShell.

Descrizione dei tipi di istanza

Per informazioni sulle impostazioni del tipo di istanza per un tipo di istanza specifico, esegui Get-EC2InstanceType Cmdletcon gli Strumenti per PowerShell e sostituisci il tipo di istanza come segue:

```
PS C:\> Get-EC2InstanceType -InstanceType m6i.metal | `
Select-Object `
    InstanceType,
    CurrentGeneration,
    @{Name = 'EnaSrdSupported'; Expression = { $_.NetworkInfo.EnaSrdSupported } } |
 `
Format-List

InstanceType      : m6i.metal
CurrentGeneration : True
EnaSrdSupported   : True
```

Se ENA Express è abilitato, viene restituito un valore di `True`.

Descrizione delle interfacce di rete

Per informazioni sulle impostazioni ENA Express per un'interfaccia di rete, esegui Get-EC2NetworkInterface Cmdletcon gli strumenti per PowerShell quanto segue:

```
PS C:\> Get-EC2NetworkInterface -NetworkInterfaceId eni-0d1234e5f6a78901b | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
 { $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }

Association         :
NetworkInterfaceId  : eni-0d1234e5f6a78901b
OwnerId             : 111122223333
AttachTime          : 6/11/2022 1:13:11 AM
AttachmentId        : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
NetworkCardIndex    : 0
InstanceId          : i-0d1234e5f6a78901b
InstanceOwnerId     : 111122223333
Status              : attached
EnaSrdEnabled       : True
EnaSrdUdpEnabled    : False
```

Configurazione delle impostazioni di ENA Express

È possibile configurare ENA Express per i tipi di istanze EC2 supportati senza dover installare alcun software aggiuntivo.

Questa sezione spiega come configurare ENA Express da AWS Management Console o da AWS CLI. Per ulteriori informazioni, scegli la scheda corrispondente al metodo che utilizzerai.

Console

Questa scheda spiega come gestire le impostazioni di ENA Express per le interfacce di rete collegate a un'istanza.

Gestione di ENA Express dall'elenco delle interfacce di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Network interfaces (Interfacce di rete).
3. Seleziona un'interfaccia di rete collegata a un'istanza. Puoi scegliere il collegamento Network interface ID (ID interfaccia di rete) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco.
4. Scegli Manage ENA Express (Gestisci ENA Express) dal menu Action (Operazione) in alto a destra della pagina. Si apre la finestra di dialogo Manage ENA Express (Gestisci ENA Express), dove vengono visualizzati l'ID dell'interfaccia di rete selezionata e le impostazioni correnti.

   > **Note**
   >
   > Se l'interfaccia di rete selezionata non è collegata a un'istanza, questa operazione non viene visualizzata nel menu.

5. Per utilizzare ENA Express, seleziona la casella di controllo Enable (Abilita).
6. Quando ENA Express è abilitato, puoi configurare le impostazioni UDP. Per utilizzare ENA Express UDP, seleziona la casella di controllo Enable (Abilita).
7. Per salvare le impostazioni, scegli Save (Salva).

Gestione di ENA Express dall'elenco delle istanze

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegliere Instances (Istanze).
3. Seleziona il tipo di istanza che vuoi gestire. Puoi scegliere il collegamento Instance ID (ID dell'istanza) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco.

4. Seleziona la Network interface (Interfaccia di rete) da configurare per l'istanza.
5. Scegli Manage ENA Express (Gestisci ENA Express) dal menu Action (Operazione) in alto a destra della pagina.
6. Per configurare ENA Express per un'interfaccia di rete collegata all'istanza, selezionala dall'elenco Network interface (Interfaccia di rete).
7. Per utilizzare ENA Express per il collegamento dell'interfaccia di rete selezionato, seleziona la casella di controllo Enable (Abilita).
8. Quando ENA Express è abilitato, puoi configurare le impostazioni UDP. Per utilizzare ENA Express UDP, seleziona la casella di controllo Enable (Abilita).
9. Per salvare le impostazioni, scegli Save (Salva).

Configurazione di ENA Express durante il collegamento di un'interfaccia di rete a un'istanza EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Network interfaces (Interfacce di rete).
3. Seleziona un'interfaccia di rete non collegata a un'istanza, dove Status (Stato) è Available (Disponibile). Puoi scegliere il collegamento Network interface ID (ID interfaccia di rete) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco.
4. Seleziona l'Instance (Istanza) a cui collegarti.
5. Per utilizzare ENA Express dopo il collegamento dell'interfaccia di rete all'istanza, seleziona la casella di controllo Enable (Abilita).
6. Quando ENA Express è abilitato, puoi configurare le impostazioni UDP. Per utilizzare ENA Express UDP, seleziona la casella di controllo Enable (Abilita).
7. Per collegare l'interfaccia di rete all'istanza e salvare le impostazioni di ENA Express, scegli Attach (Collega).

AWS CLI

Questa scheda spiega come configurare le impostazioni di ENA Express nella AWS CLI.

Configurazione di ENA Express durante il collegamento di un'interfaccia di rete

Per configurare ENA Express quando colleghi un'interfaccia di rete a un'istanza, esegui il attach-network-interfacecomando in AWS CLI, come mostrato negli esempi seguenti:

Esempio 1: utilizzo di ENA Express per il traffico TCP ma non per il traffico UDP

In questo esempio, configuriamo `EnaSrdEnabled` come true e consentiamo l'impostazione predefinita di `EnaSrdUdpEnabled` su false.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification 'EnaSrdEnabled=true'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Esempio 2: utilizzo di ENA Express sia per il traffico TCP sia per il traffico UDP

In questo esempio, configuriamo sia `EnaSrdEnabled` sia `EnaSrdUdpEnabled` come true.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Aggiornamento delle impostazioni di ENA Express per il collegamento dell'interfaccia di rete

Per aggiornare le impostazioni ENA Express per un'interfaccia di rete collegata a un'istanza, esegui il modify-network-interface-attributecomando in AWS CLI, come mostrato negli esempi seguenti:

Esempio 1: utilizzo di ENA Express per il traffico TCP ma non per il traffico UDP

In questo esempio, configuriamo `EnaSrdEnabled` come true e consentiamo l'impostazione predefinita di `EnaSrdUdpEnabled` su false, se non è stato fatto in precedenza.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --network-interface-
id eni-0123f4567890a1b23 --ena-srd-specification 'EnaSrdEnabled=true'
```

Esempio 2: utilizzo di ENA Express sia per il traffico TCP sia per il traffico UDP

In questo esempio, configuriamo sia `EnaSrdEnabled` sia `EnaSrdUdpEnabled` come true.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Esempio 3: abbandono dell'utilizzo di ENA Express per il traffico UDP

In questo esempio, configuriamo `EnaSrdUdpEnabled` come false.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

Questa scheda spiega come configurare le impostazioni di ENA Express utilizzando PowerShell.

Configurazione di ENA Express durante il collegamento di un'interfaccia di rete

Per configurare le impostazioni ENA Express per un'interfaccia di rete, Add-EC2NetworkInterface Cmdleteseguila con gli strumenti per, PowerShell come mostrato negli esempi seguenti:

Esempio 1: utilizzo di ENA Express per il traffico TCP ma non per il traffico UDP

In questo esempio, configuriamo `EnaSrdEnabled` come true e consentiamo l'impostazione predefinita di `EnaSrdUdpEnabled` su false.

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true

eni-attach-012c3d45e678f9012
```

Esempio 2: utilizzo di ENA Express sia per il traffico TCP sia per il traffico UDP

In questo esempio, configuriamo sia `EnaSrdEnabled` sia `EnaSrdUdpEnabled` come true.

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
```

```
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdUdpSpecification_EnaSrdUdpEnabled $true

eni-attach-012c3d45e678f9012
```

Aggiornamento delle impostazioni di ENA Express per il collegamento dell'interfaccia di rete

Per aggiornare le impostazioni ENA Express per un'interfaccia di rete collegata a un'istanza, esegui il Add-EC2NetworkInterface Cmdletcomando in Strumenti per PowerShell, come mostrato negli esempi seguenti:

Esempio 1: utilizzo di ENA Express per il traffico TCP ma non per il traffico UDP

In questo esempio, configuriamo `EnaSrdEnabled` come true e consentiamo l'impostazione predefinita di `EnaSrdUdpEnabled` su false, se non è stato fatto in precedenza.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Esempio 2: utilizzo di ENA Express sia per il traffico TCP sia per il traffico UDP

In questo esempio, configuriamo sia `EnaSrdEnabled` sia `EnaSrdUdpEnabled` come true.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
```

```
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : True
```

Esempio 3: abbandono dell'utilizzo di ENA Express per il traffico UDP

In questo esempio, configuriamo `EnaSrdUdpEnabled` come false.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Configura ENA Express all'avvio

È possibile utilizzare uno dei seguenti metodi per configurare ENA Express per un'AMI quando si avvia un'istanza dalla AWS Management Console.

- Puoi configurare ENA Express per la tua AMI quando avvii un'istanza con la procedura guidata di avvio dell'istanza. Per i dettagli sulla configurazione, consulta Configurazione avanzata di rete nelle Impostazioni di rete per la procedura guidata di avvio dell'istanza.
- Puoi configurare ENA Express per l'AMI quando usi un modello di avvio. Per ulteriori informazioni sulla configurazione del modello di avvio, consulta Configurazione di rete avanzata nelle Impostazioni di rete per i modelli di avvio.

Monitoraggio delle prestazioni di ENA Express

Dopo avere abilitato ENA Express per i collegamenti dell'interfaccia di rete sia sull'istanza di invio sia sull'istanza di ricezione, è possibile utilizzare i parametri di ENA Express per garantire che le istanze traggano il massimo vantaggio dai miglioramenti delle prestazioni offerti dalla tecnologia SRD.

Per visualizzare un elenco di parametri filtrati per ENA Express, esegui il comando ethtool per la tua interfaccia di rete (mostrata qui come `eth0`):

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
 ena_srd_resource_utilization: 0
```

Verifica delle impostazioni di ENA Express per un'istanza

Per verificare le impostazioni correnti di ENA Express per il collegamento dell'interfaccia di rete sulla tua istanza, esegui il comando `ethtool` per elencare i parametri di ENA Express e prendi nota del valore del parametro `ena_srd_mode`. I valori sono i seguenti:

- `0` = ENA Express disattivato, UDP disattivato
- `1` = ENA Express attivato, UDP disattivato
- `2` = ENA Express disattivato, UDP attivato

> **Note**
>
> Ciò accade solo quando ENA Express è stato abilitato in origine e UDP è stato configurato per il suo utilizzo. Il valore precedente viene mantenuto per il traffico UDP.

- `3` = ENA Express attivato, UDP attivato

Dopo avere abilitato ENA Express per il collegamento dell'interfaccia di rete su un'istanza, l'istanza di invio avvia la comunicazione con l'istanza di ricezione e SRD rileva se ENA Express è in funzione sia sull'istanza di invio sia sull'istanza di ricezione. Se ENA Express è in funzione, la comunicazione può utilizzare la trasmissione SRD. Se ENA Express non è in funzione, la comunicazione torna alla

trasmissione ENA standard. Per verificare se la trasmissione dei pacchetti utilizza SRD, è possibile confrontare il numero di pacchetti idonei (parametro `ena_srd_eligible_tx_pkts`) con il numero di pacchetti SRD trasmessi (parametro `ena_srd_tx_pkts`) durante un determinato periodo di tempo.

È possibile monitorare l'utilizzo delle risorse SDR utilizzando il parametro `ena_srd_resource_utilization`. Se la tua istanza sta per esaurire le risorse SRD, saprai che è il momento di aumentare orizzontalmente l'istanza.

Per ulteriori informazioni sui parametri di ENA Express, consulta la pagina Parametri di ENA Express.

Ottimizza le prestazioni per le impostazioni ENA Express

Per verificare la configurazione dell'istanza Linux per prestazioni ottimali di ENA Express, puoi eseguire il seguente script disponibile nel GitHub repository Amazon:

https://github.com/amzn/amzn-ec2-ena-utilities/blob/main/ena-express/ .sh check-ena-express-settings

Lo script esegue una serie di test e suggerisce le modifiche di configurazione consigliate e richieste.

Abilita reti avanzate con l'interfaccia Intel 82599 VF sulle tue istanze EC2

Amazon EC2 fornisce funzioni di rete avanzate tramite l'interfaccia VF 82599 Intel, che utilizza il driver Intel `ixgbevf`.

Indice

Requisiti

Per preparare la configurazione delle funzionalità delle reti avanzate tramite l'interfaccia VF Intel 82599, configura l'istanza nel seguente modo:

- Scegli tra i seguenti tipi di istanze supportati: C3, C4, D2, I2, M4 (esclusi `m4.16xlarge`) ed R3.
- Verificare che l'istanza disponga di connettività Internet.
- Se sull'istanza sono presenti dati importanti che devono essere conservati, è consigliabile eseguire una copia di backup di tali dati ora mediante la creazione di un'AMI dall'istanza. L'aggiornamento dei kernel e dei relativi moduli, nonché l'abilitazione dell'attributo `sriovNetSupport`, potrebbero rendere non compatibili le istanze o irraggiungibili i sistemi operativi. Se disponi di un backup recente, i tuoi dati saranno mantenuti.
- Istanze Linux: avvia l'istanza da un'AMI HVM utilizzando la versione del kernel Linux 2.6.32 o successiva. Per le AMI HVM di Amazon Linux i moduli necessari per le reti avanzate sono installati e gli attributi obbligatori sono impostati. Pertanto, se viene avviata un'istanza supportata da Amazon EBS e che include il supporto delle reti avanzate tramite un'AMI HVM di Amazon Linux corrente, le reti avanzate sono già abilitate per l'istanza.

  > **Warning**
  >
  > Le reti avanzate sono supportate solo per le istanze HVM. L'abilitazione delle reti avanzate con un'istanza PV potrebbe rendere irraggiungibile l'istanza. L'impostazione di questo attributo senza un modulo appropriato o una versione di modulo corretta può rendere irraggiungibile l'istanza.

- Istanze Windows: avvia l'istanza da un'AMI HVM a 64 bit. Non è possibile abilitare la rete avanzata su Windows Server 2008. Le reti avanzate sono già abilitate per le AMI per Windows Server 2012 R2 e Windows Server 2016 e versioni successive. Windows Server 2012 R2 include il driver Intel 1.0.15.3. Consigliamo di aggiornare questo driver alla versione più recente utilizzando la utility Pnputil.exe.
- Puoi utilizzarlo AWS CloudShellda oppure installarlo e configurarlo AWS Tools for Windows PowerShellsu qualsiasi computer a tua scelta, preferibilmente sul desktop o sul laptop locale. AWS Management ConsoleAWS CLI Per ulteriori informazioni, consulta Accesso a Amazon EC2 o la Guida per l'utente di AWS CloudShell. Le reti avanzate non possono essere gestite dalla console Amazon EC2.

Verificate che il driver sia installato

Verifica che il driver sia installato sull'istanza.

Driver di interfaccia di rete Linux

Utilizza il comando seguente per verificare se il modulo viene utilizzato su un'interfaccia specifica, sostituendo il nome dell'interfaccia che desideri controllare. Se usi una singola interfaccia (impostazione predefinita), essa sarà `eth0`. Se il sistema operativo supporta nomi di rete prevedibili, questo potrebbe essere un nome simile a `ens5`.

Nell'esempio seguente, il modulo `ixgbevf` non viene caricato, perché il driver nell'elenco è `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

In questo esempio, viene caricato il modulo `ixgbevf`. Questa istanza dispone della funzionalità per reti avanzate adeguatamente configurata.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Adattatore di rete Windows

Per verificare se il driver è installato, connettiti all'istanza e apri Device Manager (Gestione dispositivi). In Network adapters (Schede di rete) deve essere presente la voce "Intel(R) 82599 Virtual Function" (Funzione virtuale Intel(R) 82599).

Verifica dell'abilitazione delle reti avanzate

Verificare che l'`sriovNetSupport`attributo sia impostato.

Attributo di istanza (sriovNetSupport)

Per controllare se per un'istanza è stato impostato l'attributo `sriovNetSupport` per le reti avanzate, utilizza uno dei seguenti comandi. Se l'attributo è impostato, il valore è`simple`.

- describe-instance-attribute (AWS CLI) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute
 sriovNetSupport
```

- Get-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute sriovNetSupport
```

Attributo dell'immagine (sriovNetSupport)

Per verificare se un'AMI dispone già del set di `sriovNetSupport` attributi di rete avanzato, utilizzare uno dei seguenti comandi. Se l'attributo è impostato, il valore è`simple`.

- describe-images (AWS CLI)

```
aws ec2 describe-images --image-id ami_id --query "Images[].SriovNetSupport"
```

- Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami-id).SriovNetSupport
```

Abilitazione delle reti avanzate su un'istanza

La procedura da utilizzare dipende dal sistema operativo dell'istanza.

> **Warning**
>
> Non sono disponibili procedure per disabilitare l'attributo delle reti avanzate dopo averlo abilitato.

Amazon Linux

Per le AMI HVM di Amazon Linux più recenti, il modulo `ixgbevf` necessario per le reti avanzate è installato e l'attributo `sriovNetSupport` è impostato. Pertanto, se avvii un tipo di istanza tramite un'AMI HVM di Amazon Linux corrente, le reti avanzate sono già abilitate per l'istanza. Per ulteriori informazioni, consulta Verifica dell'abilitazione delle reti avanzate.

Se l'istanza è stata avviata utilizzando una AMI Amazon Linux più vecchia che non dispone delle reti avanzate già abilitate, utilizzare la seguente procedura per abilitare le reti avanzate.

Per abilitare le reti avanzate

1. Connettiti alla tua istanza.
2. Dall'istanza, esegui il seguente comando per aggiornare l'istanza in base al nuovo kernel e ai nuovi moduli kernel, compreso `ixgbevf`:

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. Dal computer locale, riavvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: reboot-instances (AWS CLI), Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Ricollegati all'istanza e verifica che il modulo `ixgbevf` sia installato con la versione minima consigliata utilizzando il comando modinfo ixgbevf disponibile in Verifica dell'abilitazione delle reti avanzate.
5. [Istanza supportata da EBS] Dal computer locale, arresta l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario interromperla nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.

   [Istanza supportata da instance store] Non è possibile arrestare l'istanza per modificare l'attributo. Passa invece alla procedura successiva.
6. Dal computer locale, abilita l'attributo relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   AWS CLI

   modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
 simple
```

PowerShell

Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

7. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un'AMI supportata da Amazon EBS. L'AMI eredita l'attributo relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.
8. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario avviare l'istanza nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.
9. Connettiti all'istanza e verifica che il modulo `ixgbevf` sia installato e caricato sull'interfaccia di rete in uso tramite il comando ethtool -i eth***n*** disponibile in Verifica dell'abilitazione delle reti avanzate.

Per abilitare le reti avanzate (istanze supportate da instance store)

Segui la procedura precedente fino al punto in cui si arresta l'istanza. Crea una nuova AMI come descritto in Creazione di un'AMI Linux supportata da un instance store, assicurandoti di abilitare l'attributo relativo alle reti avanzate durante la registrazione dell'AMI.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Prima di iniziare, controlla se le reti avanzate sono già abilitate nell'istanza.

L'AMI HVM Quick Start Ubuntu (Avvio rapido Ubuntu) include i driver necessari per le reti avanzate. Se hai una versione di `ixgbevf` precedente alla 2.16.4, puoi installare il pacchetto kernel `linux-aws` per avere i driver di rete ottimizzati più recenti.

La seguente procedura descrive le fasi generali necessarie per compilare il modulo `ixgbevf` su un'istanza Ubuntu.

Come installare il pacchetto **`linux-aws`** kernel

1. Connettiti alla tua istanza.
2. Aggiorna la cache dei pacchetti e i pacchetti.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Se durante il processo di aggiornamento viene richiesto di installare `grub`, utilizza `/dev/xvda` per installare `grub`, quindi scegli di conservare la versione corrente di `/boot/grub/menu.lst`.

Altre distribuzioni Linux

Prima di iniziare, controlla se le reti avanzate sono già abilitate nell'istanza. L'AMI HVM Quick Start (Avvio rapido) più recente include i driver necessari per le reti avanzate. Non devi pertanto eseguire procedure aggiuntive.

La procedura seguente descrive le fasi generali da eseguire se devi abilitare le reti avanzate con l'interfaccia VF Intel 82599 su una distribuzione Linux diversa da Amazon Linux o Ubuntu. Per ulteriori informazioni, ad esempio sintassi dettagliata dei comandi, posizione dei file o supporto di pacchetti e strumenti, consulta la documentazione specifica per la distribuzione Linux in uso.

Per abilitare le reti avanzate su Linux

1. Connettiti alla tua istanza.

2. Scarica l'origine del modulo `ixgbevf` sull'istanza da Sourceforge all'indirizzo https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/.

   Le versioni di `ixgbevf` precedenti alla 2.16.4, compresa la versione 2.14.2, non vengono compilate correttamente su alcune distribuzioni Linux, comprese determinate versioni di Ubuntu.

3. Compila e installa il modulo `ixgbevf` sull'istanza.

   > **Warning**
   >
   > Se si esegue la compilazione del modulo `ixgbevf` per il kernel corrente e quindi si aggiorna il kernel senza ricompilare il driver per il nuovo kernel, al successivo riavvio il sistema potrebbe ripristinare il modulo `ixgbevf` specifico della distribuzione. Questo potrebbe rendere irraggiungibile il sistema se la versione specifica della distribuzione è incompatibile con la rete migliorata.

4. Esegui il comando sudo depmod per aggiornare le dipendenze del modulo.
5. Aggiorna `initramfs` sull'istanza in modo che il nuovo modulo venga caricato in fase di avvio.
6. Determina se il sistema utilizza nomi di interfaccia di rete prevedibili per impostazione di default. I sistemi che utilizzano systemd o udev versione 197 o successive possono rinominare i dispositivi Ethernet e pertanto non garantiscono che la singola interfaccia di rete venga rinominata in `eth0`. Questo comportamento potrebbe causare problemi durante la connessione all'istanza. Per ulteriori informazioni e per informazioni sulle altre opzioni di configurazione disponibili, consulta l'argomento relativo ai nomi di interfaccia di rete prevedibili sul sito Web freedesktop.org.

   a. È possibile controllare le versioni di systemd o udev sui sistemi basati su RPM utilizzando il seguente comando:

   ```
   [ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
   systemd-208-11.el7_0.2.x86_64
   ```

   Nell'esempio precedente relativo a Red Hat Enterprise Linux 7, la versione di systemd è 208, pertanto, i nomi di interfaccia di rete prevedibili devono essere disabilitati.

   b. Disabilitare i nomi di interfaccia di rete prevedibili aggiungendo l'opzione `net.ifnames=0` alla riga `GRUB_CMDLINE_LINUX` in `/etc/default/grub`.

   ```
   [ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /
   etc/default/grub
   ```

c. Ricompila il file di configurazione di grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Istanza supportata da EBS] Dal computer locale, arresta l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: stop-instances (AWS CLI/AWS CloudShell), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario interromperla nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.

   [Istanza supportata da instance store] Non è possibile arrestare l'istanza per modificare l'attributo. Passa invece alla procedura successiva.

8. Dal computer locale, abilita l'attributo relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

9. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un'AMI supportata da Amazon EBS. L'AMI eredita l'attributo relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.

   Se il sistema operativo dell'istanza contiene un file `/etc/udev/rules.d/70-persistent-net.rules`, è necessario eliminarlo prima di creare l'AMI. Questo file contiene l'indirizzo MAC per la scheda Ethernet dell'istanza originale. Se un'altra istanza viene avviata con questo file, il sistema operativo non sarà in grado di trovare il dispositivo ed `eth0` potrebbe non funzionare causando problemi di avvio. Questo file viene rigenerato al successivo ciclo di avvio e qualsiasi istanza avviata dall'AMI crea la propria versione del file.

10. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario avviare l'istanza nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.
11. (Facoltativo) Connettiti all'istanza e verifica che il modulo sia installato.

Per abilitare le reti avanzate (istanze supportate da archivio istanze)

Segui la procedura precedente fino al punto in cui si arresta l'istanza. Crea una nuova AMI come descritto in Creazione di un'AMI Linux supportata da un instance store, assicurandoti di abilitare l'attributo relativo alle reti avanzate durante la registrazione dell'AMI.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Se hai avviato l'istanza per la quale la funzionalità di reti avanzate non è già abilitata, devi scaricare e installare il driver per la scheda di rete richiesto sull'istanza e quindi impostare l'attributo `sriovNetSupport` dell'istanza in modo da attivare le reti avanzate. Puoi abilitare questo attributo solo sui tipi di istanza supportati. Per ulteriori informazioni, consulta Supporto di reti avanzate.

> **Important**
>
> Per visualizzare gli ultimi aggiornamenti dei driver nelle AMI Windows, consulta la cronologia delle versioni di Windows AMI nel AWS Windows AMI Reference.

Per abilitare le reti avanzate

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. [Windows Server 2016 e versioni successive] Esegui il seguente PowerShell script di avvio EC2 per configurare l'istanza dopo l'installazione del driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

> **Important**
>
> La password amministratore verrà reimpostata quando abiliti lo script EC2 Launch dell'istanza di inizializzazione. Puoi modificare il file di configurazione per disattivare la reimpostazione della password amministratore specificandolo nelle impostazioni delle attività di inizializzazione.

3. Dall'istanza, scaricare il driver della scheda di rete Intel per il sistema operativo in uso:

   - Windows Server 2022

     Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.
   - Windows Server 2019 incluso per Server versione 1809 e successive*

     Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.
   - Windows Server 2016 incluso per Server versione 1803 e precedenti*

     Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.
   - Windows Server 2012 R2

     Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.
   - Windows Server 2012

     Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.
   - Windows Server 2008 R2

     Visita la pagina di download e scarica `PROWinx64Legacy.exe`.

*Le versioni Server 1803 e precedenti e 1809 e successive non sono specificatamente trattate nelle pagine Driver e Software Intel.

4. Installa il driver della scheda di rete Intel per il sistema operativo in uso.

   - Windows Server 2008 R2

     1. Nella cartella Downloads, individua il file `PROWinx64Legacy.exe` e rinominalo `PROWinx64Legacy.zip`.
     2. Estrai i contenuti del file `PROWinx64Legacy.zip`.
     3. Apri la riga di comando, passa alla cartella contenente i file estratti e utilizza l'utility `pnputil` per aggiungere e installare il file INF nell'archivio dei driver.

        ```
        C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
        ```

   - Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 e Windows Server 2012

     1. Nella cartella Downloads, estrarre i contenuti del file `Wired_driver_`*`version`*`_x64.zip`.
     2. Nella cartella dei file estratti, individua il file `Wired_driver_`*`version`*`_x64.exe` e rinominalo `Wired_driver_`*`version`*`_x64.zip`.
     3. Estrai i contenuti del file `Wired_driver_`*`version`*`_x64.zip`.
     4. Apri la riga di comando, passa alla cartella contenente i file estratti ed esegui uno dei seguenti comandi per utilizzare l'utility `pnputil` per aggiungere e installare il file INF nell'archivio dei driver.

        - Windows Server 2022

          ```
          C:\> pnputil -i -a PROXGB\Winx64\WS2022\vxs.inf
          ```

        - Windows Server 2019

          ```
          C:\> pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
          ```

        - Windows Server 2016

          ```
          C:\> pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
          ```

        - Windows Server 2012 R2

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

- Windows Server 2012

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

5. Dal computer locale, abilita l'attributo relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

6. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un'AMI supportata da Amazon EBS. L'AMI eredita l'attributo relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.
7. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se l'istanza è gestita da AWS OpsWorks, è necessario avviare l'istanza nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.

Risolvere i problemi di connettività

Se si perde la connettività durante l'abilitazione delle reti avanzate, il modulo `ixgbevf` potrebbe non essere compatibile con il kernel. Prova a installare la versione del modulo `ixgbevf` inclusa nella distribuzione di Linux per l'istanza in uso.

Se si abilitano le reti avanzate per un'istanza PV o AMI, l'istanza può risultare irraggiungibile.

Per ulteriori informazioni, consulta Come posso attivare e configurare una rete avanzata sulle mie istanze EC2?

Monitoraggio delle prestazioni di rete per l'istanza EC2

Il driver ENA (Elastic Network Adapter) pubblica i parametri delle prestazioni di rete dalle istanze in cui sono attivati. È possibile utilizzare questi parametri per risolvere i problemi relativi alle prestazioni delle istanze, scegliere la dimensione dell'istanza appropriata per un carico di lavoro, pianificare le attività di scalabilità in modo proattivo e confrontare le applicazioni per determinare se massimizzano le prestazioni disponibili in un'istanza.

Amazon EC2 definisce i valori massimi di rete a livello di istanza per garantire un'esperienza di rete di alta qualità, comprese prestazioni di rete costanti per tutte le dimensioni delle istanze. AWS fornisce i valori massimi per quanto segue per ogni istanza:

- Capacità di larghezza di banda: ogni istanza EC2 ha una larghezza di banda massima per il traffico aggregato in entrata e in uscita, in base al tipo e alle dimensioni dell'istanza. Alcune istanze utilizzano un meccanismo di credito I/O di rete per allocare la larghezza di banda di rete alle istanze in base all'utilizzo medio della larghezza di banda. Amazon EC2 offre inoltre la larghezza di banda massima per il traffico verso AWS Direct Connect e Internet. Per ulteriori informazioni, consulta Larghezza di banda di rete dell'istanza Amazon EC2.
- Prestazioni P acket-per-second (PPS): ogni istanza EC2 ha prestazioni PPS massime, in base al tipo e alle dimensioni dell'istanza.
- Connessioni tracciate: il gruppo di sicurezza tiene traccia di ogni connessione stabilita per garantire che i pacchetti restituiti vengano consegnati come previsto. Per ciascuna istanza esiste un numero massimo di connessioni che possono essere monitorate. Per ulteriori informazioni, consulta la sezione Monitoraggio della connessione al gruppo di sicurezza.
- Accesso al servizio locale del collegamento: Amazon EC2 fornisce un numero massimo di PPS per interfaccia di rete per il traffico verso servizi quali il servizio DNS, il servizio di metadati dell'istanza e il servizio Amazon Time Sync.

Quando il traffico di rete di un'istanza supera il limite massimo, AWS modella il traffico che supera il massimo mettendo in coda e quindi eliminando i pacchetti di rete. Utilizzando i parametri delle prestazioni di rete è possibile monitorare quando il traffico supera un valore massimo. Questi parametri indicano in tempo reale l'impatto sul traffico di rete e i possibili problemi relativi alle prestazioni della rete.

Indice

Requisiti

Istanze Linux

- Installare il driver ENA versione 2.2.10 o successiva. Per verificare la versione installata, utilizzare il comando ethtool. Nell'esempio seguente, la versione soddisfa il requisito minimo.

  ```
  [ec2-user ~]$ ethtool -i eth0 | grep version
  version: 2.2.10
  ```

  Per aggiornare il driver ENA, consulta Reti avanzate.
- Per importare questi parametri su Amazon CloudWatch, installa l' CloudWatch agente. Per ulteriori informazioni, consulta Collect network performance metrics nella Amazon CloudWatch User Guide.
- Per supportare la `conntrack_allowance_available` metrica, installa il driver ENA versione 2.8.1.

Istanze Windows

- Installare il driver ENA versione 2.2.2 o successiva. Per verificare la versione installata, utilizzare Gestione periferiche come segue.
  1. Aprire Gestione periferiche eseguendo `devmgmt.msc`.
  2. Espandere Network Adapters (Schede di rete).
  3. Scegliere Amazon Elastic Network Adapter (Adattatore di rete elastico di Amazon), quindi Properties (Proprietà).
  4. Nella scheda Driver individuare Driver Version (Versione driver).

  Per aggiornare il driver ENA, consulta Reti avanzate.

- Per importare questi parametri su Amazon CloudWatch, installa l' CloudWatch agente. Per ulteriori informazioni, consulta Collect advanced network metrics nella Amazon CloudWatch User Guide.

Parametri per il driver ENA

Il driver ENA fornisce i seguenti parametri all'istanza in tempo reale. Questi forniscono il numero complessivo di pacchetti accodati o rilasciati su ciascuna interfaccia di rete dall'ultimo ripristino del driver.

Parametro	Descrizione	Supportato su
`bw_in_allowance_exceeded`	Il numero di pacchetti accordati o rilasciati perché la larghezza di banda aggregata in ingresso ha superato il valore massimo per l'istanza.	Tutti i tipi di istanza
`bw_out_allowance_exceeded`	Il numero di pacchetti accodati o rilasciati perché la larghezza di banda aggregata in uscita ha superato il valore massimo per l'istanza.	Tutti i tipi di istanza
`conntrack_allowance_exceeded`	Il numero di pacchetti accodati o rilasciati perché il rilevamento delle connessioni ha superato il valore massimo per l'istanza e non è stato possibile stabilire nuove connessioni. Ciò può comportare la perdita di pacchetti per il traffico da o verso l'istanza.	Tutti i tipi di istanza
`conntrack_allowance_available`	Il numero di connessioni tracciate che possono essere stabilite dall'istanza prima di raggiungere il limite Connessioni tracciate di quel tipo di istanza.	Solo istanze basate sul sistema AWS Nitro

Parametro	Descrizione	Supportato su
`linklocal_allowance_exceeded`	Il numero di pacchetti accodati o rilasciati perché il PPS del traffico verso i servizi proxy locali ha superato il valore massimo per l'interfaccia di rete. Ciò influisce sul traffico verso il servizio DNS, il servizio di metadati dell'istanza e il servizio Amazon Time Sync.	Tutti i tipi di istanza
`pps_allowance_exceeded`	Il numero di pacchetti accodati o rilasciati perché il PPS bidirezionale ha superato il valore massimo per l'istanza.	Tutti i tipi di istanza

Visualizzare i parametri delle prestazioni di rete per l'istanza

La procedura da utilizzare dipende dal sistema operativo dell'istanza.

Istanze Linux

È possibile pubblicare parametri negli strumenti preferiti per visualizzare i dati dei parametri. Ad esempio, puoi pubblicare le metriche su Amazon CloudWatch utilizzando l' CloudWatch agente. L'agente consente di selezionare singoli parametri e di controllare la pubblicazione.

Inoltre, è possibile utilizzare ethtool per recuperare i parametri per ogni interfaccia di rete, ad esempio eth0, come indicato di seguito.

```
[ec2-user ~]$ ethtool -S eth0
     bw_in_allowance_exceeded: 0
     bw_out_allowance_exceeded: 0
     pps_allowance_exceeded: 0
     conntrack_allowance_exceeded: 0
     linklocal_allowance_exceeded: 0
     conntrack_allowance_available: 136812
```

Istanze Windows

È possibile visualizzare i parametri utilizzando qualsiasi consumer di contatori delle prestazioni di Windows. I dati possono essere analizzati in base al manifesto. EnaPerfCounters Si tratta di un file XML che definisce il fornitore del contatore delle prestazioni e i relativi set di contatori.

Per installare il manifesto

Se l'istanza è stata avviata utilizzando una AMI contenente il driver ENA 2.2.2 o versione successiva, o si è utilizzato lo script di installazione nel pacchetto driver per il driver ENA 2.2.2, il manifest è già installato. Per installare manualmente il manifest, attenersi alla seguente procedura:

1. Rimuovere il manifest esistente utilizzando il seguente comando:

   ```
   unlodctr /m:EnaPerfCounters.man
   ```

2. Copiare il file manifest `EnaPerfCounters.man` dal pacchetto di installazione del driver a `%SystemRoot%\System32\drivers`.
3. Installare il nuovo manifest utilizzando il seguente comando:

   ```
   lodctr /m:EnaPerfCounters.man
   ```

Per visualizzare le metriche utilizzando Performance Monitor

1. Aprire Performance Monitor.
2. Premere Ctrl+N per aggiungere nuovi contatori.
3. Scegliere ENA Packets Shaping (Modellazione pacchetti ENA) dall'elenco.
4. Selezionare le istanze da monitorare e scegliere Add (Aggiungi).
5. Seleziona OK.

Parametri di ENA Express

ENA Express è alimentato dalla tecnologia AWS Scalable Reliable Datagram (SRD). SRD è un protocollo di trasporto di rete ad alte prestazioni che utilizza l'instradamento dinamico per aumentare la velocità di trasmissione effettiva e ridurre al minimo la latenza di coda. Puoi utilizzare i parametri di ENA Express per assicurarti che le tue istanze traggano il massimo vantaggio dai miglioramenti delle prestazioni offerti dalla tecnologia SRD, ad esempio:

- Valuta le tue risorse per assicurarti che abbiano una capacità sufficiente per stabilire più connessioni SRD.
- Identifica dove risiedono i potenziali problemi che impediscono ai pacchetti in uscita idonei di utilizzare SRD.
- Calcola la percentuale di traffico in uscita che utilizza SRD per l'istanza.
- Calcola la percentuale di traffico in entrata che utilizza SRD per l'istanza.

> **Note**
>
> Per produrre parametri, utilizza la versione 2.8 o successiva del driver.

I seguenti parametri di ENA Express sono disponibili utilizzando il comando ethtool per le istanze basate su Linux.

- `ena_srd_mode`: descrive quali funzionalità ENA Express sono abilitate. I valori sono i seguenti:
  - `0` = ENA Express disattivato, UDP disattivato
  - `1` = ENA Express attivato, UDP disattivato
  - `2` = ENA Express disattivato, UDP attivato

    > **Note**
    >
    > Ciò accade solo quando ENA Express è stato abilitato in origine e UDP è stato configurato per il suo utilizzo. Il valore precedente viene mantenuto per il traffico UDP.

  - `3` = ENA Express attivato, UDP attivato
- `ena_srd_eligible_tx_pkts`: il numero di pacchetti di rete inviati in un determinato periodo di tempo che soddisfano i requisiti SRD di idoneità, come indicato di seguito:
  - Sono supportati i tipi sia delle istanze di invio sia di quelle di ricezione. Per ulteriori informazioni, consulta la tabella Tipi di istanza supportati per ENA Express.
  - Sia le istanze di invio sia quelle di ricezione devono avere ENA Express configurato.
  - Le istanze di invio e ricezione devono essere eseguite nella stessa zona di disponibilità.
  - Il percorso di rete tra le istanze non deve includere box middleware (software intermediario). ENA Express attualmente non supporta i box middleware (software intermediario).

> **Note**
>
> Il parametro di idoneità ENA Express copre i requisiti di origine e destinazione e la rete tra i due endpoint. I pacchetti idonei possono comunque essere squalificati dopo che sono già stati contati. Ad esempio, se un pacchetto idoneo supera il limite massimo di unità di trasmissione (MTU), torna alla trasmissione ENA standard, sebbene il pacchetto sia comunque indicato come idoneo nel contatore.

- `ena_srd_tx_pkts`: il numero di pacchetti SRD trasmessi in un determinato periodo di tempo.
- `ena_srd_rx_pkts`: il numero di pacchetti SRD ricevuti in un determinato periodo di tempo.
- `ena_srd_resource_utilization`: la percentuale di utilizzo massimo della memoria consentita per le connessioni SRD simultanee adoperate dall'istanza.

Per visualizzare un elenco di parametri filtrati per ENA Express, esegui il comando ethtool per la tua interfaccia di rete (mostrata qui come `eth0`):

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
 ena_srd_resource_utilization: 0
```

Traffico in uscita (pacchetti in uscita)

Per assicurarti che il traffico in uscita utilizzi SRD come previsto, confronta il numero di pacchetti SRD idonei (`ena_srd_eligible_tx_pkts`) con il numero di pacchetti SRD inviati (`ena_srd_tx_pkts`) in un determinato periodo di tempo.

Differenze significative tra il numero di pacchetti idonei e il numero di pacchetti SRD inviati sono spesso causate da problemi di utilizzo delle risorse. Quando la scheda di rete collegata all'istanza ha esaurito il massimo delle risorse o se i pacchetti superano il limite MTU, i pacchetti idonei non sono in grado di trasmettere tramite SRD e devono ricorrere alla trasmissione ENA standard. I pacchetti possono ricadere in questa lacuna anche durante le migrazioni in tempo reale o gli aggiornamenti live dei server. È necessaria un'ulteriore risoluzione dei problemi per determinare la causa principale.

> **Note**
>
> È possibile ignorare le piccole differenze occasionali tra il numero di pacchetti idonei e il numero di pacchetti SRD. Tali differenze possono verificarsi, ad esempio, quando l'istanza stabilisce una connessione a un'altra istanza per il traffico SRD.

Per scoprire quale percentuale del traffico totale in uscita in un determinato periodo di tempo utilizza SRD, confronta il numero di pacchetti SRD inviati (`ena_srd_tx_pkts`) con il numero totale di pacchetti inviati per l'istanza (`NetworkPacketOut`) durante tale periodo.

Traffico in ingresso (pacchetti in entrata)

Per scoprire quale percentuale del traffico in entrata utilizza SRD, confronta il numero di pacchetti SRD ricevuti (`ena_srd_rx_pkts`) in un determinato periodo di tempo con il numero totale di pacchetti ricevuti per l'istanza (`NetworkPacketIn`) durante tale periodo.

Utilizzo delle risorse

L'utilizzo delle risorse si basa sul numero di connessioni SRD simultanee che una singola istanza può sostenere in un dato momento. Il parametro di utilizzo delle risorse (`ena_srd_resource_utilization`) tiene traccia dell'utilizzo corrente per l'istanza. A mano a mano che l'utilizzo si avvicina al 100%, puoi aspettarti di riscontrare problemi di prestazioni. ENA Express passa dalla trasmissione SRD alla trasmissione ENA standard e la possibilità di perdita di pacchetti aumenta. L'elevato utilizzo delle risorse indica che è giunto il momento di dimensionare l'istanza per migliorare le prestazioni della rete.

> **Note**
>
> Quando il traffico di rete di un'istanza supera il limite massimo, AWS modella il traffico che supera tale limite mettendo in coda e quindi eliminando i pacchetti di rete.

Persistenza

I parametri di uscita e ingresso si accumulano quando ENA Express è abilitato per l'istanza. I parametri smettono di accumularsi se ENA Express è disattivato, ma persistono fintantoché l'istanza è in esecuzione. I parametri vengono ripristinati se l'istanza si riavvia o viene terminata oppure se l'interfaccia di rete viene scollegata dall'istanza.

Parametri delle prestazioni di rete con il driver DPDK per ENA

Il driver ENA versione 2.2.0 e successive supporta il reporting dei parametri di rete. DPDK 20.11 include il driver ENA 2.2.0 ed è la prima versione di DPDK a supportare questa funzionalità.

È possibile utilizzare un'applicazione di esempio per visualizzare le statistiche DPDK. Per avviare una versione interattiva dell'applicazione di esempio, esegui il comando seguente.

```
./app/dpdk-testpmd -- -i
```

All'interno di questa sessione interattiva, è possibile immettere un comando per recuperare le statistiche estese per una porta. Il seguente comando di esempio recupera le statistiche per la porta 0.

```
show port xstats 0
```

Di seguito è riportato un esempio di sessione interattiva con l'applicazione di esempio DPDK.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected

        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
```

```
        Done
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
        testpmd> show port xstats 0
        ###### NIC extended statistics for port 0
        rx_good_packets: 0
        tx_good_packets: 0
        rx_good_bytes: 0
        tx_good_bytes: 0
        rx_missed_errors: 0
        rx_errors: 0
        tx_errors: 0
        rx_mbuf_allocation_errors: 0
        rx_q0_packets: 0
        rx_q0_bytes: 0
        rx_q0_errors: 0
        tx_q0_packets: 0
        tx_q0_bytes: 0
        wd_expired: 0
        dev_start: 1
        dev_stop: 0
        tx_drops: 0
        bw_in_allowance_exceeded: 0
        bw_out_allowance_exceeded: 0
        pps_allowance_exceeded: 0
        conntrack_allowance_exceeded: 0
        linklocal_allowance_exceeded: 0
        rx_q0_cnt: 0
        rx_q0_bytes: 0
        rx_q0_refill_partial: 0
        rx_q0_bad_csum: 0
        rx_q0_mbuf_alloc_fail: 0
        rx_q0_bad_desc_num: 0
        rx_q0_bad_req_id: 0
        tx_q0_cnt: 0
        tx_q0_bytes: 0
        tx_q0_prepare_ctx_err: 0
        tx_q0_linearize: 0
        tx_q0_linearize_failed: 0
        tx_q0_tx_poll: 0
        tx_q0_doorbells: 0
        tx_q0_bad_req_id: 0
        tx_q0_available_desc: 1023
```

```
        testpmd>
```

Per ulteriori informazioni sull'applicazione di esempio e sul suo utilizzo per recuperare statistiche estese, consulta Testpmd Application User Guide nella documentazione di DPDK.

Parametri sulle istanze che eseguono FreeBSD

A partire dalla versione 2.3.0, il driver ENA FreeBSD supporta la raccolta di parametri sulle prestazioni di rete su istanze che eseguono FreeBSD. Per abilitare la raccolta dei parametri di FreeBSD, inserire il seguente comando e impostare *l'intervallo* su un valore compreso tra 1 e 3600. Questo specifica la frequenza con cui, in pochi secondi, raccogliere i parametri di FreeBSD.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Ad esempio, il seguente comando imposta il driver affinché raccolga i parametri di FreeBSD sull'interfaccia di rete 1 ogni 10 secondi:

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Per disattivare la raccolta dei parametri di FreeBSD, puoi eseguire il comando precedente e specificare `0` come *interval* (intervallo).

Dopo aver abilitato la raccolta delle metriche di FreeBSD, puoi recuperare l'ultimo set di metriche raccolte eseguendo il seguente comando.

```
sysctl dev.ena.network_interface.eni_metrics
```

Risolvere i problemi relativi all'Elastic Network Adapter su Linux

L'Elastic Network Adapter (ENA) è progettato per migliorare lo stato del sistema operativo e ridurre le possibilità di interruzione a lungo termine a causa di un comportamento inatteso dell'hardware e/o di guasti. La struttura dell'ENA rende i guasti dei dispositivi o dei driver il più chiari possibile al sistema. Questo argomento fornisce le informazioni relative alla risoluzione dei problemi dell'ENA.

Se è impossibile connettersi all'istanza, iniziare dalla sezione Risolvere i problemi di connettività.

Se riscontri un peggioramento delle prestazioni dopo la migrazione a un tipo di istanza di sesta generazione, consulta l'articolo Cosa devo fare prima di migrare la mia istanza EC2 a un'istanza di sesta generazione per assicurarmi di ottenere le massime prestazioni di rete?

Se è possibile connettersi all'istanza, è possibile raccogliere informazioni diagnostiche utilizzando i meccanismi di rilevamento e riparazione dei guasti descritti nelle sezioni successive di questo argomento.

Indice

Risolvere i problemi di connettività

Se si perde la connettività durante l'abilitazione della rete avanzata, il modulo `ena` potrebbe essere incompatibile con il kernel dell'istanza attualmente in esecuzione. Questo può accadere se si installa il modulo per una specifica versione del kernel (senza dkms o con un file dkms.conf non configurato correttamente), quindi il kernel di istanza viene aggiornato. Se il kernel di istanza caricato al momento dell'avvio non ha il modulo `ena` correttamente installato, l'istanza non riconoscerà l'adattatore di rete e l'istanza diventerà irraggiungibile.

Se si attivano le reti avanzate per un'istanza PV o AMI, l'istanza può risultare irraggiungibile.

Se l'istanza diventa irraggiungibile dopo aver abilitato le reti avanzate con l'ENA, è possibile disattivare l'attributo `enaSupport` per l'istanza e quest'ultima tornerà all'adattatore di rete originale.

Disattivare le reti avanzate con l'ENA (istanze supportate da EBS)

1. Dal tuo computer locale, arresta l'istanza utilizzando la console Amazon EC2 o uno dei seguenti comandi: stop-instances (), ()AWS CLI. Stop-EC2InstanceAWS Tools for Windows PowerShell Se la tua istanza è gestita da AWS OpsWorks, dovresti interromperla nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.

   > **Tip**
   >
   > Se si utilizza un'istanza supportata da instance store, non è possibile arrestare l'istanza. Invece, vai a Per disabilitare la rete avanzata con ENA (instance store-baked instances).

2. Dal computer locale, disattivare l'attributo delle reti avanzate utilizzando il comando seguente.

   - modify-instance-attribute (AWS CLI)

   ```
   $ C:\> aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
   ```

3. Dal tuo computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei seguenti comandi: start-instances (), ()AWS CLI. Start-EC2InstanceAWS Tools for Windows PowerShell Se la tua istanza è gestita da AWS OpsWorks, dovresti avviare l'istanza nella AWS OpsWorks console in modo che lo stato dell'istanza rimanga sincronizzato.
4. (Facoltativo) Connettersi all'istanza e provare a reinstallare il modulo `ena` con la versione del kernel attuale seguendo i passaggi in Abilita una rete avanzata con l'Elastic Network Adapter (ENA) sulle tue istanze EC2.

Disattivare le reti avanzate con l'ENA (istanze supportate da instance store)

Se l'istanza è supportata da instance store, creare una nuova AMI come descritto in Creazione di un'AMI Linux supportata da un instance store. Assicurarsi di disattivare l'attributo delle reti avanzate `enaSupport` durante la registrazione dell'AMI.

- register-image (AWS CLI)

```
$ C:\> aws ec2 register-image --no-ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
C:\> Register-EC2Image -EnaSupport $false ...
```

Meccanismo keep-alive

Il dispositivo ENA segnala gli eventi keep-alive con una frequenza fissa (di solito una volta al secondo). Il driver dell'ENA è dotato di un meccanismo watchdog che controlla la presenza di questi messaggi keep-alive. Se sono presenti uno o più messaggi, il watchdog viene riarrestato, altrimenti il driver ritiene che il dispositivo abbia subito un guasto e procede come segue:

- Scarica le sue statistiche attuali su syslog

- Reimposta il dispositivo ENA
- Reimposta lo stato del driver ENA

La procedura di ripristino sopra descritta può provocare una perdita di traffico per un breve periodo di tempo (le connessioni TCP devono poter essere ripristinate), ma non dovrebbe influire in altro modo sull'utente.

Il dispositivo ENA può anche richiedere indirettamente una procedura di ripristino del dispositivo, non inviando una notifica keep-alive, per esempio se il dispositivo ENA raggiunge uno stato sconosciuto dopo aver caricato una configurazione irrecuperabile.

Di seguito è riportato un esempio della procedura di ripristino:

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
 process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
 end of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
 driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
 [Wed Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
```

```
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
 process is complete
```

Timeout lettura registro

La struttura dell'ENA suggerisce un utilizzo limitato delle operazioni di lettura degli I/O mappati in memoria (MMIO). I registri MMIO sono accessibili dal driver del dispositivo ENA solo durante la procedura di inizializzazione.

Se i log del driver (disponibili nell'output dmesg) indicano errori nelle operazioni di lettura, ciò può essere causato da un driver incompatibile o compilato in modo errato, da un dispositivo hardware occupato o da un guasto hardware.

Le voci di log intermittenti che indicano errori nelle operazioni di lettura non devono essere considerate un problema; in questo caso il driver le riproverà. Tuttavia, una sequenza di voci di log contenenti errori di lettura indica un problema al driver o all'hardware.

Di seguito è riportato un esempio di voce di log del driver che indica un errore nell'operazione di lettura dovuto a un timeout:

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistiche

Se si verificano prestazioni di rete insufficienti o problemi di latenza, è necessario recuperare le statistiche del dispositivo ed esaminarle. Si possono ottenere tali statistiche utilizzando ethtool, come mostrato di seguito.

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
```

```
  tx_timeout: 0
  suspend: 0
  resume: 0
  wd_expired: 0
  interface_up: 1
  interface_down: 0
  admin_q_pause: 0
  bw_in_allowance_exceeded: 0
  bw_out_allowance_exceeded: 0
  pps_allowance_exceeded: 0
  conntrack_allowance_available: 450878
  conntrack_allowance_exceeded: 0
  linklocal_allowance_exceeded: 0
  queue_0_tx_cnt: 4329
  queue_0_tx_bytes: 1075749
  queue_0_tx_queue_stop: 0
  ...
```

I seguenti parametri di output del comando sono descritti di seguito:

`tx_timeout`: *N*

Numero di volte in cui il watchdog Netdev è stato attivato.

`suspend`: *N*

Numero di volte in cui il driver ha eseguito un'operazione di sospensione.

`resume`: *N*

Numero di volte in cui il driver ha eseguito un'operazione di ripresa.

`wd_expired`: *N*

Numero di volte in cui il driver non ha ricevuto l'evento keep-alive nei tre secondi precedenti.

`interface_up`: *N*

Numero di volte in cui l'interfaccia ENA è stata attivata.

`interface_down`: *N*

Numero di volte in cui l'interfaccia ENA è stata disattivata.

`admin_q_pause`: *N*

Numero di volte in cui la coda di amministrazione non è stata trovata in uno stato di esecuzione.

`bw_in_allowance_exceeded`: *N*

Il numero di pacchetti accordati o rilasciati perché la larghezza di banda aggregata in ingresso ha superato il valore massimo per l'istanza.

`bw_out_allowance_exceeded`: *N*

Il numero di pacchetti accodati o rilasciati perché la larghezza di banda aggregata in uscita ha superato il valore massimo per l'istanza.

`pps_allowance_exceeded`: *N*

Il numero di pacchetti accodati o rilasciati perché il PPS bidirezionale ha superato il valore massimo per l'istanza.

`conntrack_allowance_available`: *N*

Il numero di connessioni tracciate che possono essere stabilite dall'istanza prima di raggiungere il limite Connessioni tracciate di quel tipo di istanza. Disponibile solo per le istanze basate su Nitro. Non supportato con le istanze FreeBSD o gli ambienti DPDK.

`conntrack_allowance_exceeded`: *N*

Il numero di pacchetti accodati o rilasciati perché il rilevamento delle connessioni ha superato il valore massimo per l'istanza e non è stato possibile stabilire nuove connessioni. Ciò può comportare la perdita di pacchetti per il traffico da o verso l'istanza.

`linklocal_allowance_exceeded`: *N*

Il numero di pacchetti accodati o rilasciati perché il PPS del traffico verso i servizi proxy locali ha superato il valore massimo per l'interfaccia di rete. Ciò influisce sul traffico verso il servizio DNS, il servizio di metadati dell'istanza e il servizio Amazon Time Sync.

`queue_`*N*`_tx_cnt`: *N*

Numero di pacchetti trasmessi per questa coda.

`queue_`*N*`_tx_bytes`: *N*

Numero di byte trasmessi per questa coda.

`queue_`*N*`_tx_queue_stop`: *N*

Numero di volte in cui la coda *N* era piena e si è arrestata.

`queue_`*N*`_tx_queue_wakeup`: *N*

Numero di volte in cui la coda *N* ha ripreso dopo essersi arrestata.

`queue_N_tx_dma_mapping_err`: *N*

Conteggio errori di accesso diretto alla memoria. Se questo valore non è pari a 0, significa che le risorse di sistema sono scarse.

`queue_N_tx_linearize`: *N*

Numero di volte in cui è stata tentata la linearizzazione SKB per questa coda.

`queue_N_tx_linearize_failed`: *N*

Numero di volte in cui la linearizzazione SKB non è andata a buon fine per questa coda.

`queue_N_tx_napi_comp`: *N*

Numero di volte in cui il gestore `napi` ha chiamato `napi_complete` per questa coda.

`queue_N_tx_tx_poll`: *N*

Numero di volte in cui il gestore `napi` è stato programmato per questa coda.

`queue_N_tx_doorbells`: *N*

Numero di campanelli di trasmissione per questa coda.

`queue_N_tx_prepare_ctx_err`: *N*

Numero di volte in cui `ena_com_prepare_tx` non è andato a buon fine per questa coda.

`queue_N_tx_bad_req_id`: *N*

`req_id` non valido per questa coda. Il `req_id` valido è zero, meno la `queue_size`, meno 1.

`queue_N_tx_llq_buffer_copy`: *N*

Numero di pacchetti la cui dimensione delle intestazioni è maggiore della voce llq per questa coda.

`queue_N_tx_missed_tx`: *N*

Numero di pacchetti trasmessi lasciati incompleti per questa coda.

`queue_N_tx_unmask_interrupt`: *N*

Numero di volte in cui l'interrupt tx è stato smascherato per questa coda.

`queue_N_rx_cnt`: *N*

Numero di pacchetti ricevuti per questa coda.

`queue_N_rx_bytes`: *N*

Numero di byte ricevuti per questa coda.

`queue_N_rx_rx_copybreak_pkt`: *N*

Numero di volte in cui la coda rx ha ricevuto un pacchetto inferiore alla dimensione del pacchetto rx_copybreak per questa coda.

`queue_N_rx_csum_good`: *N*

Numero di volte in cui la coda rx ha ricevuto un pacchetto in cui il checksum è stato controllato ed era corretto per questa coda.

`queue_N_rx_refil_partial`: *N*

Numero di volte in cui il driver non è riuscito a riempire la parte vuota della coda rx con i buffer per questa coda. Se questo valore non è pari a 0, significa che le risorse di memoria sono scarse.

`queue_N_rx_bad_csum`: *N*

Numero di volte che la coda `rx` ha avuto un checksum negativo per questa coda (solo se è supportato l'offload del checksum).

`queue_N_rx_page_alloc_fail`: *N*

Numero di volte in cui l'assegnazione della pagina non è andata a buon fine per questa coda. Se questo valore non è pari a 0, significa che le risorse di memoria sono scarse.

`queue_N_rx_skb_alloc_fail`: *N*

Numero di volte in cui l'assegnazione dell'SKB non è andata a buon fine per questa coda. Se questo valore non è pari a 0, significa che le risorse di sistema sono scarse.

`queue_N_rx_dma_mapping_err`: *N*

Conteggio errori di accesso diretto alla memoria. Se questo valore non è pari a 0, significa che le risorse di sistema sono scarse.

`queue_N_rx_bad_desc_num`: *N*

Troppi buffer per pacchetto. Se questo valore non è pari a 0, significa che si utilizzano buffer molto piccoli.

`queue_N_rx_bad_req_id`: *N*

Il req_id per questa coda non è valido. Il req_id valido è compreso tra [0, queue_size - 1].

`queue_N_rx_empty_rx_ring: N`

Numero di volte in cui la coda rx è stata vuota per questa coda.

`queue_N_rx_csum_unchecked: N`

Numero di volte in cui la coda rx ha ricevuto un pacchetto il cui checksum non è stato controllato per questa coda.

`queue_N_rx_xdp_aborted: N`

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_ABORT.

`queue_N_rx_xdp_drop: N`

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_DROP.

`queue_N_rx_xdp_pass: N`

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_PASS.

`queue_N_rx_xdp_tx: N`

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_TX.

`queue_N_rx_xdp_invalid: N`

Numero di volte in cui il codice restituito da XDP per il pacchetto non era valido.

`queue_N_rx_xdp_redirect: N`

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_REDIRECT.

`queue_N_xdp_tx_cnt: N`

Numero di pacchetti trasmessi per questa coda.

`queue_N_xdp_tx_bytes: N`

Numero di byte trasmessi per questa coda.

`queue_N_xdp_tx_queue_stop: N`

Numero di volte in cui questa coda era piena e si è arrestata.

`queue_N_xdp_tx_queue_wakeup: N`

Numero di volte in cui questa coda ha ripreso dopo essersi arrestata.

`queue_N_xdp_tx_dma_mapping_err`: *N*

Conteggio errori di accesso diretto alla memoria. Se questo valore non è pari a 0, significa che le risorse di sistema sono scarse.

`queue_N_xdp_tx_linearize`: *N*

Numero di volte in cui è stata tentata la linearizzazione del buffer XDP per questa coda.

`queue_N_xdp_tx_linearize_failed`: *N*

Numero di volte in cui la linearizzazione del buffer XDP non è andata a buon fine per questa coda.

`queue_N_xdp_tx_napi_comp`: *N*

Numero di volte in cui il gestore napi ha chiamato napi_complete per questa coda.

`queue_N_xdp_tx_tx_poll`: *N*

Numero di volte in cui il gestore napi è stato programmato per questa coda.

`queue_N_xdp_tx_doorbells`: *N*

Numero di campanelli di trasmissione per questa coda.

`queue_N_xdp_tx_prepare_ctx_err`: *N*

Numero di volte in cui ena_com_prepare_tx non è andato a buon fine per questa coda. Questo valore deve essere sempre zero; altrimenti, consultare i log del driver.

`queue_N_xdp_tx_bad_req_id`: *N*

Il req_id per questa coda non è valido. Il req_id valido è compreso tra [0, queue_size - 1].

`queue_N_xdp_tx_llq_buffer_copy`: *N*

Numero di pacchetti che hanno copiato le intestazioni utilizzando la copia del buffer llq per questa coda.

`queue_N_xdp_tx_missed_tx`: *N*

Numero di volte in cui una voce di coda tx ha perso un timeout di completamento per questa coda.

`queue_N_xdp_tx_unmask_interrupt`: *N*

Numero di volte in cui l'interrupt tx è stato smascherato per questa coda.

`ena_admin_q_aborted_cmd`: *N*

Il numero di comandi di amministrazione che sono stati interrotti. Questo solitamente accade durante la procedura di auto-ripristino.

`ena_admin_q_submitted_cmd`: *N*

Numero di campanelli di coda di amministrazione.

`ena_admin_q_completed_cmd`: *N*

Numero di completamenti di coda di amministrazione.

`ena_admin_q_out_of_space`: *N*

Numero di volte in cui il driver ha tentato di inviare un nuovo comando di amministrazione, ma la coda era piena.

`ena_admin_q_no_completion`: *N*

Numero di volte in cui il driver non ha ricevuto un completamento di amministrazione per un comando.

Log di errore driver in Syslog

Il driver ENA scrive messaggi di log a syslog durante l'avvio del sistema. In caso di problemi, è possibile esaminare questi log per cercare errori. Di seguito è riportato un esempio di informazioni registrate dal driver ENA in syslog durante l'avvio del sistema, insieme ad alcune annotazioni per la selezione dei messaggi.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.416939] [ENA_COM:
 ena_com_validate_version] ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.420915] [ENA_COM:
 ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.256831] ena 0000:00:03.0: Device
 watchdog is Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.672947] ena 0000:00:03.0: creating 8 io
 queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.680885] [ENA_COM:
 ena_com_init_interrupt_moderation] Feature 20 isn't supported  // Interrupt moderation
 is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.691609] [ENA_COM:
 ena_com_get_feature_ex] Feature 10 isn't supported // RSS HASH function configuration
 is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.694583] [ENA_COM:
 ena_com_get_feature_ex] Feature 18 isn't supported //RSS HASH input source
 configuration is not supported by the device
```

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.697433] [ENA_COM:
 ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.701064] ena 0000:00:03.0 (unnamed
 net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.704917] ena 0000:00:03.0: Elastic
 Network Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  480.805037] EXT4-fs (xvda1): re-mounted.
 Opts: (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  481.025842] NET: Registered protocol family
 10
```

Quali errori posso ignorare?

I seguenti avvisi, che possono apparire nei log di errore del sistema, possono essere ignorati per Elastic Network Adapter:

Set host attribute isn't supported (L'impostazione dell'attributo dell'host non è supportata)

Gli attributi dell'host non sono supportati da questo dispositivo.

failed to alloc buffer for rx queue (allocazione del buffer per la coda rx non riuscita)

Si tratta di un errore recuperabile, che indica che potrebbe essersi verificato un problema di pressione di memoria quando l'errore è stato generato.

La caratteristica *X* non è supportata

La caratteristica a cui si fa riferimento non è supportata da Elastic Network Adapter. I valori possibili di *X* includono:

- **10**: la configurazione della funzione Hash RSS non è supportata per questo dispositivo.
- **12**: la configurazione della tabella di Riferimento indiretto RSS non è supportata per questo dispositivo.
- **18**: la configurazione dell'Input Hash RSS non è supportata per questo dispositivo.
- **20**: la moderazione dell'interruzione non è supportata per questo dispositivo.
- **27**: il driver Elastic Network Adapter non supporta il polling delle funzionalità Ethernet da snmpd.

Failed to config AENQ (Impossibile configurare AENQ)

L'Elastic Network Adapter non supporta la configurazione AENQ.

Trying to set unsupported AENQ events (Tentativo di impostare eventi AENQ non supportati)

Questo errore indica un tentativo di impostare un gruppo di eventi AENQ non supportato dall'Elastic Network Adapter.

Notifiche di configurazione non ottimale

Il dispositivo ENA rileva le impostazioni di configurazione non ottimali nel driver che è possibile modificare. Il dispositivo notifica il driver ENA e registra un avviso sulla console. Nell'esempio seguente viene illustrato il formato del messaggio di avviso.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for
 additional details and mitigation options.
```

L'elenco seguente mostra i dettagli del codice di notifica e le operazioni consigliate per gli esiti di configurazione non ottimali.

- Codice **1**: non è consigliato utilizzare ENA Express con la configurazione LLQ estesa

  ENA Express ENI è configurato con LLQ esteso. Questa configurazione non è ottimale e potrebbe influire sulle prestazioni di ENA Express. Si consiglia di disabilitare le impostazioni LLQ estese quando si utilizzano ENI ENA Express, come indicato di seguito.

  ```
  sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
  ```

  Per ulteriori informazioni sulla configurazione ottimale di ENA Express, consulta la pagina Migliora le prestazioni di rete con ENA Express sulle tue istanze EC2.
- Codice **2**: ENI ENA Express con una profondità di coda Tx non ottimale non è consigliato

  ENI ENA Express è configurato con una profondità di coda Tx non ottimale. Questa configurazione potrebbe influire sulle prestazioni di ENA Express. Si consiglia di estendere tutte le code Tx al valore massimo per l'interfaccia di rete quando si utilizzano ENI ENA Express, come indicato di seguito.

  È possibile eseguire i seguenti ethtool comandi per regolare la dimensione LLQ. Per ulteriori informazioni su come controllare, interrogare e abilitare Wide-LLQ, consulta l'argomento Large Low-Latency Queue (Large LLQ) del driver del kernel Linux per la documentazione ENA nel repository Amazon Drivers. GitHub

```
ethtool -g interface
```

Imposta le code Tx alla profondità massima:

```
ethtool -G interface tx depth
```

Per ulteriori informazioni sulla configurazione ottimale di ENA Express, consulta la pagina Migliora le prestazioni di rete con ENA Express sulle tue istanze EC2.

- Codice**3**: ENA con dimensioni LLQ regolari e traffico di pacchetti Tx supera la dimensione massima supportata dall'header

  Per impostazione predefinita, ENA LLQ supporta intestazioni di pacchetti Tx di dimensioni fino a 96 byte. Se la dimensione dell'intestazione del pacchetto è maggiore di 96 byte, il pacchetto viene eliminato. Per mitigare questo problema, si consiglia di abilitare Wide-LLQ, che aumenta la dimensione dell'intestazione del pacchetto Tx supportata fino a un massimo di 224 byte.

  Tuttavia, quando si abilita Wide-LLQ, la dimensione massima dell'anello Tx viene ridotta da 1000 a 512 voci. Wide-LLQ è abilitato di default per tutti i tipi di istanze Nitro v4 e versioni successive.

  - I tipi di istanze Nitro v4 hanno una dimensione massima predefinita dell'anello Wide-LLQ Tx di 512 voci, che non può essere modificata.
  - I tipi di istanze Nitro v5 hanno una dimensione predefinita dell'anello Wide-LLQ Tx di 512 voci, che è possibile aumentare fino a 1000 voci.

  È possibile eseguire i seguenti ethtool comandi per regolare la dimensione LLQ. Per ulteriori informazioni su come controllare, interrogare e abilitare Wide-LLQ, consulta l'argomento Large Low-Latency Queue (Large LLQ) del driver del kernel Linux per la documentazione ENA nel repository Amazon Drivers. GitHub

  Trova la profondità massima per le tue code Tx:

  ```
  ethtool -g interface
  ```

  Imposta le code Tx alla profondità massima:

  ```
  ethtool -G interface tx depth
  ```

Risolvere i problemi relativi al driver Windows Elastic Network Adapter

L'Elastic Network Adapter (ENA) è progettato per migliorare lo stato del sistema operativo e ridurre le possibilità di interruzione a causa di un comportamento inatteso dell'hardware e/o di guasti che può alterare il funzionamento dell'istanza Windows. La struttura dell'ENA rende i guasti dei dispositivi o dei driver il più chiari possibile al sistema operativo.

Installa il driver Elastic Network Adapter (ENA)

Se l'istanza non è basata su una delle più recenti Amazon Machine Image (AMI) di Windows fornite da Amazon, utilizza la seguente procedura per installare il driver ENA corrente sull'istanza. Devi eseguire questo aggiornamento quando è opportuno riavviare l'istanza. Se lo script di installazione non riavvia automaticamente l'istanza, riavvia l'istanza come fase finale.

Se si utilizza un volume di archivio dell'istanza per memorizzare i dati mentre l'istanza è in esecuzione, tali dati vengono cancellati quando si arresta l'istanza. Prima di arrestare la tua istanza, verifica di aver copiato tutti i dati necessari dai volumi di archivio dell'istanza nell'archiviazione persistente, ad esempio Amazon EBS o Amazon S3.

Prerequisiti

Per installare o aggiornare il driver ENA, l'istanza Windows deve soddisfare i seguenti prerequisiti:

- È installata PowerShell la versione 3.0 o successiva

Fase 1: esegui il backup dei dati

Crea un'AMI di backup, nel caso in cui non riesci a eseguire il rollback delle modifiche tramite Gestione dispositivi. Per creare un'AMI di backup con AWS Management Console, procedi nel seguente modo:

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza che richiede l'aggiornamento del driver e scegli Arresta istanza dal menu di stato dell'istanza.
4. Dopo l'arresto dell'istanza, selezionala di nuovo. Per creare il backup, scegli Immagine e modelli dal menu Azioni, quindi scegli Crea immagine.
5. Per riavviare l'istanza, scegli Avvia istanza dal menu Stato dell'istanza.

Fase 2: installazione o aggiornamento del driver ENA

È possibile installare o aggiornare il driver ENA con AWS Systems Manager Distributor o con i PowerShell cmdlet. Per ulteriori istruzioni, selezionare la scheda corrispondente al metodo che vuoi utilizzare.

Systems Manager Distributor

Puoi utilizzare la funzione Systems Manager Distributor per distribuire i pacchetti ai nodi gestiti da Systems Manager. Con Systems Manager Distributor puoi installare il pacchetto di driver ENA una sola volta o con aggiornamenti programmati. Per ulteriori informazioni su come installare il pacchetto driver ENA (`AwsEnaNetworkDriver`) con Systems Manager Distributor, consulta Installare o aggiornare i pacchetti nella Guida per l'AWS Systems Manager utente.

PowerShell

Questa sezione illustra come scaricare e installare i pacchetti di driver ENA sull'istanza con i cmdlet. PowerShell

Opzione 1: scarica ed estrai l'ultima versione

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Usa il cmdlet invoke-webrequest per scaricare il pacchetto driver più recente:

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

> **Note**
>
> Se ricevi un errore durante il download del file e utilizzi Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il seguente comando e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

In alternativa, puoi scaricare il pacchetto driver più recente da una finestra del browser dell'istanza.

3. Usa il cmdlet expand-archive per estrarre l'archivio zip che hai scaricato nella tua istanza:

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Opzione 2: scarica ed estrai una versione specifica

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Scarica il pacchetto driver ENA per la versione specifica che desideri dal link della versione nella tabella Driver ENA per Windows.
3. Estrai l'archivio .zip nella tua istanza.

Installa il driver ENA con PowerShell

Le fasi di installazione sono le stesse indipendentemente dal fatto che tu abbia scaricato il driver più recente o una versione specifica. Per installare il driver ENA, segui questi passaggi.

1. Per installare il driver, esegui `install.ps1` PowerShell lo script dalla `AwsEnaNetworkDriver` directory dell'istanza. Se ricevi un errore, assicurati di utilizzare la PowerShell versione 3.0 o una versione successiva.
2. Se il programma di installazione non riavvia automaticamente l'istanza, esegui il cmdlet. Restart-Computer PowerShell

```
PS C:\> Restart-Computer
```

Fase 3 (opzionale): verifica la versione del driver ENA dopo l'installazione

Per assicurarti che il pacchetto driver ENA sia stato installato correttamente sulla tua istanza, puoi verificare la nuova versione come segue:

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.

3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Amazon Elastic Network Adapter e quindi Proprietà. In questo modo si apre la finestra di dialogo delle proprietà di Amazon Elastic Network Adapter.

> **Note**
>
> Gli adattatori ENA utilizzano tutti lo stesso driver. Se disponi di più adattatori ENA, puoi selezionarne uno qualsiasi per aggiornare il driver per tutti gli adattatori ENA.

6. Per verificare la versione corrente installata, apri la scheda Driver e controlla la versione del driver. Se la versione corrente non corrisponde alla versione di interesse, consulta Risolvere i problemi relativi al driver Windows Elastic Network Adapter.

Roll back di un driver ENA

Se qualcosa va storto durante l'installazione, potrebbe essere necessario tornare alla versione precedente del driver. Segui questi passaggi per ripristinare la versione precedente del driver ENA installata sull'istanza.

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Amazon Elastic Network Adapter e quindi Proprietà. In questo modo si apre la finestra di dialogo delle proprietà di Amazon Elastic Network Adapter.

> **Note**
>
> Gli adattatori ENA utilizzano tutti lo stesso driver. Se disponi di più adattatori ENA, puoi selezionarne uno qualsiasi per aggiornare il driver per tutti gli adattatori ENA.

6. Per ripristinare il driver, apri la scheda Driver e scegli Roll back dei driver. In questo modo si apre la finestra di dialogo di rollback dei Pacchetti driver.

> **Note**
>
> Se la scheda Driver non mostra l'azione Rollback dei driver o se l'azione non è disponibile, significa che l'Archivio dei driver dell'istanza non contiene il pacchetto driver installato in precedenza. Per risolvere questo problemaScenari per la risoluzione dei problemi, consulta ed espandi la sezione Installazione della versione non prevista del driver ENA. Per ulteriori informazioni sul processo di selezione dei pacchetti driver del dispositivo, consulta Modalità con cui Windows seleziona un pacchetto driver per un dispositivo nel sito web della documentazione Microsoft.

Raccogliere informazioni diagnostiche sull'istanza

I passaggi per aprire gli strumenti del sistema operativo Windows (OS) variano a seconda della versione del sistema operativo installata nell'istanza. Nelle seguenti sezioni, utilizziamo la finestra di dialogo Esegui per aprire gli strumenti, che funziona allo stesso modo in tutte le versioni del sistema operativo. Tuttavia, è possibile accedere a questi strumenti utilizzando qualsiasi metodo si preferisca.

Accesso alla finestra di dialogo Esegui

- Utilizzando la combinazione di tasti logo Windows: `Windows` + `R`
- Utilizzando la barra di ricerca:
  - Inserire `run` nella barra di ricerca.
  - Selezionare l'applicazione Esegui dai risultati di ricerca.

Alcuni passaggi richiedono che il menu contestuale acceda alle proprietà o alle azioni sensibili al contesto. Esistono diversi modi per eseguire questa operazione, a seconda della versione del sistema operativo e dell'hardware.

Accesso al menu contestuale

- Utilizzando il mouse: fare clic con il pulsante destro del mouse su un elemento per visualizzare il menu contestuale.
- Utilizzando la tastiera:
  - A seconda della versione del sistema operativo, utilizzare `Shift` + `F10`, oppure `Ctrl` + `Shift` + `F10`.

- Se la tastiera presenta il tasto contestuale (tre linee orizzontali in una casella), seleziona l'elemento desiderato e premi il tasto contestuale.

Se è possibile connettersi all'istanza, utilizzare le seguenti tecniche per raccogliere informazioni diagnostiche per la risoluzione dei problemi.

Controllo dello stato del dispositivo ENA

Per controllare lo stato del driver ENA per Windows utilizzando Gestione dispositivi in Windows, attenersi alla seguente procedura:

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Amazon Elastic Network Adapter e quindi Proprietà. In questo modo si apre la finestra di dialogo Proprietà di Amazon Elastic Network Adapter.
6. Verificare che il messaggio nella scheda Generale mostri "Questo dispositivo funziona correttamente".

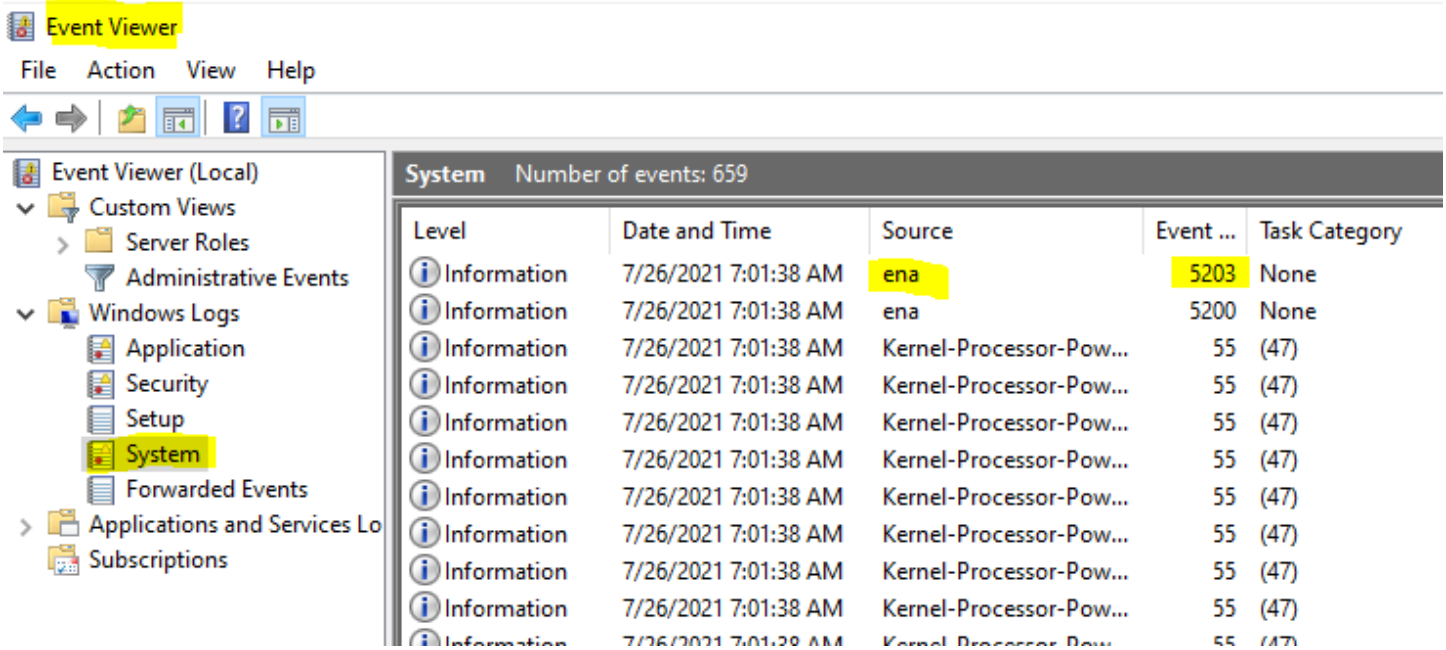
Indagare sui messaggi di evento del driver

Per esaminare i registri degli eventi del driver ENA per Windows utilizzando il Visualizzatore eventi di Windows, attenersi alla seguente procedura:

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Visualizzatore eventi in Windows, inserire `eventvwr.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra del Visualizzatore eventi di Windows.
4. Espandere il menu Eventi di Windows, quindi scegliere Sistema.
5. In Operazioni, nel pannello in alto a destra, scegliere Filtra log corrente. Viene visualizzata la finestra di dialogo di filtro.
6. Nel campo Origine eventi, inserire `ena`. Ciò limita i risultati agli eventi generati dal driver ENA per Windows.
7. Scegli OK. Ciò mostra i risultati del log degli eventi filtrati nelle sezioni di dettaglio della finestra.

8. Per espandere i dettagli, selezionare un messaggio di evento dall'elenco.

L'esempio seguente mostra un evento driver ENA nell'elenco degli eventi di sistema del Visualizzatore eventi di Windows:



Sintesi del messaggio di evento

La tabella seguente mostra i messaggi di evento generati dal driver ENA per Windows.

Input

ID evento	Descrizione dell'evento del driver ENA	Type
5001	Le risorse del hardware sono esaurite	Errore
5002	L'adattatore ha rilevato un errore hardware	Errore
5005	Il timeout impostato sull'adattatore per un'operazione NDIS non completata in modo tempestivo è scaduto.	Errore

ID evento	Descrizione dell'evento del driver ENA	Type
5032	Impossibile ripristinare il dispositivo	Errore
5200	L'adattatore è stato inizializ zato	Messaggio informativo
5201	L'adattatore è stato arrestato	Messaggio informativo
5202	L'adattatore è stato sospeso	Messaggio informativo
5203	L'adattatore è stato riavviato	Messaggio informativo
5204	L'adattatore è stato spento	Messaggio informativo
5205	L'adattatore è stato ripristinato	Errore
5206	L'adattatore è stato rimosso inaspettatamente	Errore
5208	La routine di inizializzazione dell'adattatore non è riuscita	Errore
5210	L'adattatore ha riscontrato e risolto con successo un problema interno	Errore

Visualizzazione dei parametri relativi alle prestazioni

Il driver ENA per Windows pubblica i parametri delle prestazioni di rete dalle istanze in cui sono attivati. È possibile visualizzare e abilitare le metriche sull'istanza utilizzando l'applicazione nativa Performance Monitor (Monitor di sistema). Per ulteriori informazioni sui parametri prodotti dal driver ENA per Windows, consultare Monitoraggio delle prestazioni di rete per l'istanza EC2.

Nei casi in cui le metriche ENA sono abilitate e CloudWatch l'agente Amazon è installato, CloudWatch raccoglie le metriche associate ai contatori in Windows Performance Monitor, nonché alcune metriche avanzate per ENA. Queste parametri vengono raccolti in aggiunta ai parametri

abilitati per impostazione predefinita nelle istanze EC2. Per ulteriori informazioni sulle metriche, consulta Metriche raccolte dall' CloudWatch agente nella Amazon CloudWatch User Guide.

> **Note**
>
> I parametri delle prestazioni sono disponibili per le versioni 2.4.0 e successive dei driver ENA (anche per la versione 2.2.3). È stato eseguito il ripristino dello stato precedente del driver ENA versione 2.2.4 a causa del potenziale peggioramento delle prestazioni nelle istanze EC2 di sesta generazione. Si consiglia di eseguire l'aggiornamento alla versione corrente del driver per assicurarsi di disporre degli aggiornamenti più recenti.

Alcuni dei modi in cui è possibile utilizzare i parametri delle prestazioni includono:

- Risoluzione dei problemi di prestazioni delle istanze.
- Scegliere la dimensione dell'istanza corretta per un dato carico di lavoro.
- Pianificare in modo proattivo le attività di dimensionamento.
- Applicazioni di benchmark per determinare se le prestazioni sono massimizzate sono disponibili su un'istanza.

Frequenza di aggiornamento

Per impostazione predefinita, il driver aggiorna i parametri utilizzando un intervallo di 1 secondo. Tuttavia, l'applicazione che raccoglie i parametri potrebbe utilizzare un intervallo diverso per il polling. È possibile modificare l'intervallo di aggiornamento in Gestione dispositivi, utilizzando le proprietà avanzate per il driver.

Per modificare l'intervallo di aggiornamento dei parametri per il driver ENA per Windows, attenersi alla seguente procedura:

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Amazon Elastic Network Adapter e quindi Proprietà. In questo modo si apre la finestra di dialogo Proprietà di Amazon Elastic Network Adapter.

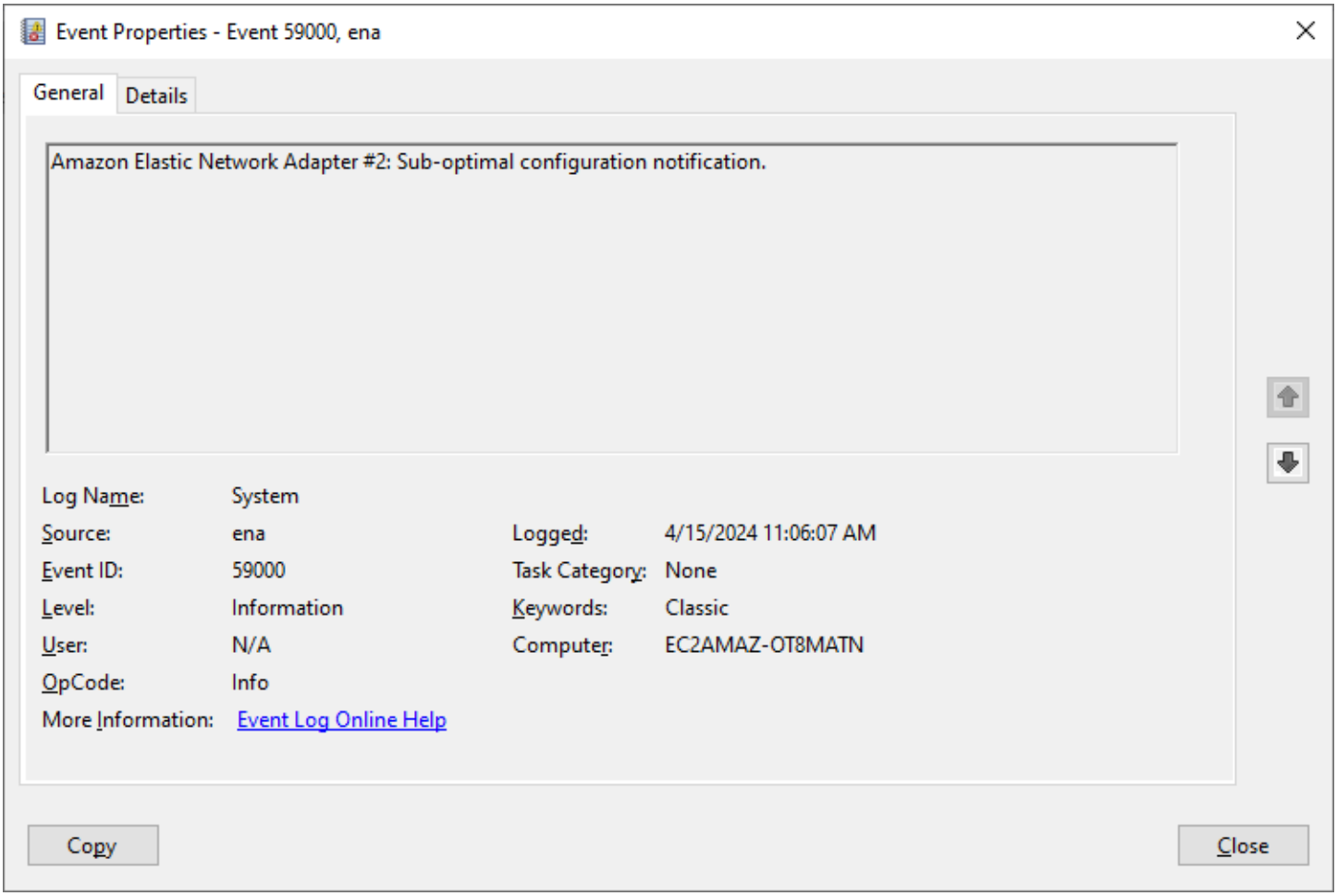
6. Apertura della scheda Avanzate nella finestra popup.
7. Dalla Proprietà, scegliere Intervallo di aggiornamento dei parametri per modificare il valore.
8. Al termine, scegliere OK.

Esamina le notifiche di configurazione non ottimali

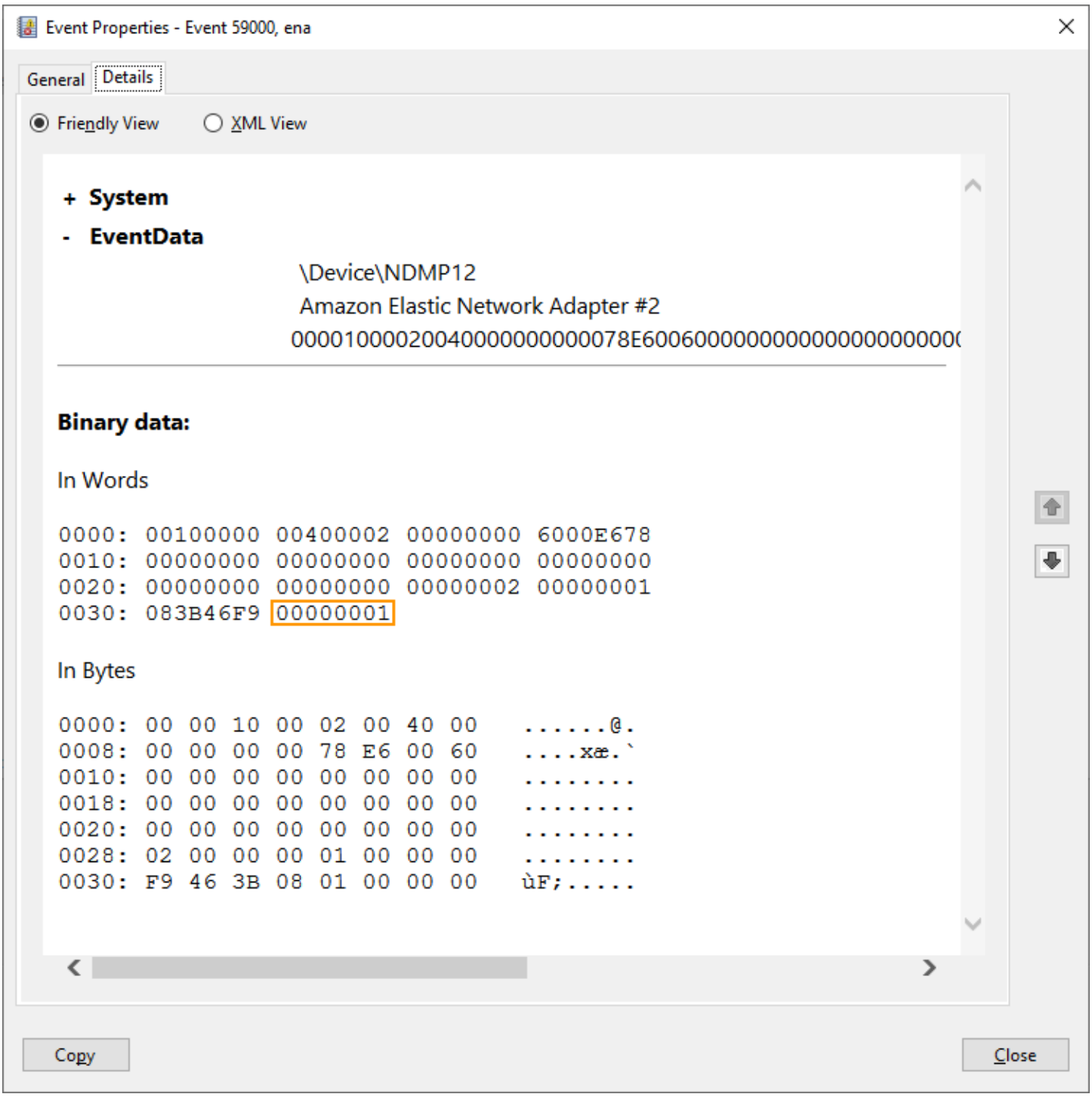
Il dispositivo ENA rileva le impostazioni di configurazione non ottimali nel driver che è possibile modificare. Il dispositivo avvisa il driver ENA e registra una notifica di evento. Per esaminare gli eventi non ottimali in Windows Event Viewer

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Visualizzatore eventi in Windows, inserire `eventvwr.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra del Visualizzatore eventi di Windows.
4. Espandere il menu Eventi di Windows, quindi scegliere Sistema.
5. In Operazioni, nel pannello in alto a destra, scegliere Filtra log corrente. Viene visualizzata la finestra di dialogo di filtro.
6. Nel campo Origine eventi, inserire `ena`. Ciò limita i risultati agli eventi generati dal driver ENA per Windows.
7. Scegli OK. Ciò mostra i risultati del log degli eventi filtrati nelle sezioni di dettaglio della finestra.

Gli eventi con ID `5900`0 notificano all'utente risultati di configurazione non ottimali. Fate clic con il pulsante destro del mouse su un evento e scegliete Proprietà evento per aprire una vista dettagliata oppure selezionate Riquadro di anteprima dal menu Visualizza per visualizzare gli stessi dettagli.



Apri la scheda Dettagli per visualizzare il codice dell'evento. Nella sezione Binary Data: In words, l'ultima parola è il codice.



L'elenco seguente mostra i dettagli del codice di notifica e le operazioni consigliate per gli esiti di configurazione non ottimali.

- Codice **1**: non è consigliato utilizzare ENA Express con la configurazione LLQ estesa

ENA Express ENI è configurato con LLQ esteso. Questa configurazione non è ottimale e potrebbe influire sulle prestazioni di ENA Express. Si consiglia di disabilitare le impostazioni LLQ estese quando si utilizzano ENI ENA Express, come indicato di seguito.

1. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
2. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
3. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
4. Aprire le proprietà del dispositivo per`Amazon Elastic Network Adapter`.
5. Da lì, apri la scheda Avanzate per apportare le modifiche.
6. Seleziona la proprietà LLQ Header Size Policy e impostane il valore su. `Normal (128 Bytes)`
7. Scegliere OK per salvare le modifiche.

- Codice **2**: ENI ENA Express con una profondità di coda Tx non ottimale non è consigliato

  ENI ENA Express è configurato con una profondità di coda Tx non ottimale. Questa configurazione potrebbe influire sulle prestazioni di ENA Express. Si consiglia di estendere tutte le code Tx al valore massimo per l'interfaccia di rete quando si utilizzano ENI ENA Express, come indicato di seguito.

  Segui questi passaggi per allargare le code Tx alla profondità massima:

  1. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
  2. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
  3. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
  4. Aprire le proprietà del dispositivo per. `Amazon Elastic Network Adapter`
  5. Da lì, apri la scheda Avanzate per apportare le modifiche.
  6. Selezionate la proprietà Transmit Buffers e impostate il suo valore sul valore massimo supportato.
  7. Scegliere OK per salvare le modifiche.

Ripristino dell'adattatore ENA

Il processo di ripristino viene avviato quando il driver ENA per Windows rileva un errore su una scheda di rete e contrassegna l'adattatore come non integro. Il driver non può ripristinarsi da solo,

quindi dipende dal sistema operativo controllare lo stato di integrità dell'adattatore e invocare il gestore di ripristino per il driver ENA per Windows. Il processo di ripristino potrebbe comportare un breve periodo di tempo in cui si verifica una perdita di traffico. Tuttavia, le connessioni TCP dovrebbero essere in grado di essere ripristinate.

L'adattatore ENA potrebbe anche richiedere indirettamente una procedura di ripristino del dispositivo, in caso di mancato invio di una notifica keep-alive. Ad esempio, se l'adattatore ENA raggiunge uno stato non riconosciuto dopo aver caricato una configurazione non ripristinabile, potrebbe interrompere l'invio di notifiche keep-alive.

Cause comuni del ripristino dell'adattatore ENA

- Messaggi keep-alive mancanti

  L'adattatore ENA segnala gli eventi keep-alive con una frequenza fissa (di solito una volta al secondo). Il driver ENA per Windows è dotato di un meccanismo watchdog che controlla periodicamente la presenza di questi messaggi keep-alive. Se uno o più nuovi messaggi vengono rilevati dall'ultima volta in cui sono stati controllati, registra un risultato positivo. In caso contrario, il driver conclude che il dispositivo ha riscontrato un utilizzo fuori limite e avvia una sequenza di ripristino.
- Pacchetti bloccati nelle code di trasmissione

  L'adattatore ENA verifica che i pacchetti scorrano attraverso le code di trasmissione come previsto. Il driver ENA per Windows rileva se i pacchetti si bloccano e avvia una sequenza di ripristino, nel caso in cui questo si verifichi.
- Timeout di lettura per registri Memory Mapped I/O (MMIO)

  Per limitare le operazioni di lettura degli I/O mappati in memoria (MMIO), il driver ENA per Windows accede ai registri MMIO solo durante i processi di inizializzazione e ripristino. Se il driver rileva un timeout, richiede una delle seguenti azioni, a seconda del processo in esecuzione:
  - Se viene rilevato un timeout durante l'inizializzazione, il flusso viene interrotto, il che comporta la visualizzazione di un punto esclamativo giallo accanto all'adattatore ENA in Gestione dispositivi di Windows.
  - Se viene rilevato un timeout durante il ripristino, il flusso viene interrotto. Il sistema operativo avvia quindi una rimozione inaspettata dell'adattatore ENA e lo ripristina arrestando e avviando l'adattatore che è stato rimosso. Per ulteriori informazioni sulla rimozione inaspettata di una scheda di interfaccia di rete (NIC), consultare Gestione della rimozione inaspettata di una NIC nella documentazione Sviluppatore hardware di Microsoft Windows.

Scenari per la risoluzione dei problemi

Gli scenari seguenti possono essere utili per risolvere i problemi che possono verificarsi con il driver ENA per Windows. Si consiglia di iniziare con l'aggiornamento del driver ENA, se non si dispone della versione più recente. Per trovare il driver più recente per la versione del sistema operativo Windows, consultare Driver ENA per Windows.

Versione del driver ENA installata non prevista

Descrizione

Dopo aver eseguito i passaggi per installare una versione specifica del driver ENA, Windows Device Manager mostra che Windows ha installato una versione diversa del driver ENA.

Causa

Quando si esegue l'installazione di un pacchetto driver, Windows classifica tutti i pacchetti driver validi per il dispositivo specificato nel Archivio driver locale prima di iniziare. Quindi seleziona il pacchetto con il valore più basso come migliore abbinamento. Può essere diverso dal pacchetto che intendevi installare. Per ulteriori informazioni sul processo di selezione dei pacchetti driver del dispositivo, consulta Modalità con cui Windows seleziona un pacchetto driver per un dispositivo nel sito web della documentazione Microsoft.

Soluzione

Per assicurarti che Windows installi la versione del pacchetto driver scelta, puoi rimuovere i pacchetti driver di livello inferiore dall'Archivio driver con lo strumento da riga di comando PNPUtil.

Segui questi passaggi per aggiornare il driver ENA:

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Aprire la finestra delle proprietà Gestione dispositivi, come descritto nella sezione Controllo dello stato del dispositivo ENA. In questo modo si apre la scheda Generale della finestra Proprietà di Amazon Elastic Network Adapter.
3. Apertura della scheda Driver.
4. Scegliere Update Driver (Aggiorna driver). Si apre la finestra di dialogo Aggiornamento del software del driver — Amazon Elastic Network Adapter.

    a. Nella pagina Modalità di ricerca software driver?, scegli Cerca driver nel computer.

b. Nella pagina Cerca il software dei driver sul computer, scegli Fammi scegliere da un elenco di driver di periferica sul mio computer, situato sotto la barra di ricerca.

c. Nella pagina Seleziona il driver del dispositivo che desideri installare per questo hardware, scegli Disco... .

d. Nella finestra Installa da disco, scegli Cerca... , accanto alla posizione di file dall'elenco discesa

e. Accedere alla posizione in cui è stato scaricato il pacchetto driver ENA di destinazione. Scegli il file `ena.inf` e seleziona Apri.

f. Per avviare l'installazione, scegli OK, quindi scegli Avanti.

5. Se il programma di installazione non riavvia automaticamente l'istanza, esegui il cmdlet. Restart-Computer PowerShell

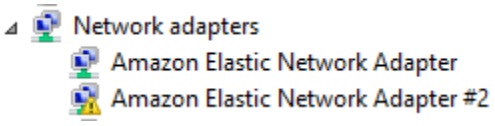
```
PS C:\> Restart-Computer
```

Avviso dispositivo per driver ENA

Descrizione

L'icona dell'adattatore ENA in Gestione dispositivi nella sezione Schede di rete visualizza un segnale di avviso (un triangolo giallo con un punto esclamativo all'interno).

L'esempio seguente mostra un adattatore ENA con l'icona di avviso in Gestione dispositivi di Windows:



Causa

Questo avviso del dispositivo è comunemente causato da problemi di ambiente, che potrebbero richiedere ulteriori ricerche e spesso richiedono un procedimento per esclusione per determinare la causa sottostante. Per un elenco completo degli errori del dispositivo, consultare Messaggi di errore di Gestione dispositivi nella documentazione Sviluppatore hardware di Microsoft Windows.

Soluzione

La soluzione per questo avviso del dispositivo dipende dalla causa principale. Il procedimento per esclusione qui descritto include alcuni passaggi fondamentali per aiutare a identificare e risolvere i

problemi più comuni che potrebbero avere una soluzione semplice. Un'ulteriore analisi della causa principale è necessaria quando questi passaggi non risolvono il problema.

Seguire questi passaggi per identificare e risolvere i problemi più comuni:

1. Avviare e arrestare il dispositivo

   Aprire la finestra delle proprietà Gestione dispositivi, come descritto nella sezione Controllo dello stato del dispositivo ENA. In questo modo si apre la scheda Generale della finestra Proprietà di Amazon Elastic Network Adapter, dove lo Stato del dispositivo visualizza il codice di errore e un breve messaggio.

   a. Apertura della scheda Driver.
   b. Scegliere Disabilitare il dispositivo e selezionare Sì al messaggio di avviso visualizzato.
   c. Scegliere Abilitare dispositivo.

2. Arrestare e avviare l'istanza EC2

   Se l'adattatore mostra ancora l'icona di avviso in Gestione dispositivi, il passo successivo consiste nell'arrestare e avviare l'istanza EC2. Questo passo rilancia l'istanza su un hardware diverso nella maggior parte dei casi.

3. Indagare il possibile problema delle risorse dell'istanza

   Se l'istanza EC2 si è interrotta e avviata e il problema persiste, potrebbe indicare un problema di risorse sull'istanza, ad esempio memoria insufficiente.

Timeout di connessione con ripristino dell'adattatore (codici di errore 5007, 5205)

Descrizione

Il visualizzatore eventi di Windows mostra il timeout dell'adattatore e gli eventi di ripristino verificati in combinazione per gli adattatori ENA. I messaggi sono simili ai seguenti esempi:

- ID evento 5007: Adattatore Amazon Elastic Network: timeout scaduto durante un'operazione.
- ID evento 5205: Adattatore Amazon Elastic Network: il ripristino dell'adattatore è stato avviato.

I ripristini dell'adattatore causano un'interruzione minima del traffico. Anche quando ci sono più ripristini, sarebbe insolito causare gravi interruzioni della rete.

Causa

Questa sequenza di eventi indica che il driver ENA per Windows ha avviato un ripristino per una scheda ENA che non rispondeva. Tuttavia, il meccanismo utilizzato dal driver del dispositivo per rilevare questo problema è soggetto a falsi positivi derivanti dalla starvation della CPU 0.

Soluzione

Se questa combinazione di errori si verifica frequentemente, controllare le allocazioni delle risorse per vedere dove potrebbero essere utile effettuare degli aggiustamenti.

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire il Resource Monitor di Windows, inserire `resmon` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra di Resource Monitor.
4. Apertura della scheda CPU. I grafici di utilizzo per CPU sono mostrati sul lato destro della finestra di Resource Monitor.
5. Controllare i livelli di utilizzo della CPU 0 per vedere se sono troppo alti.

Si consiglia di configurare RSS per escludere la CPU 0 per l'adattatore ENA su tipi di istanza più grandi (più di 16 vCPU). Per i tipi di istanza più piccoli, la configurazione di RSS potrebbe migliorare l'esperienza, ma a causa del minor numero di core disponibili, è necessario eseguire test per garantire che il vincolo dei core della CPU non influisca negativamente sulle prestazioni.

Utilizzare il comando Set-NetAdapterRss per configurare RSS per l'adattatore ENA, come illustrato nell'esempio seguente.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like
 "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

La migrazione a un'infrastruttura di istanza di sesta generazione influisce sulle prestazioni o sull'allegato

Descrizione

Se si esegue la migrazione a un'istanza EC2 di sesta generazione, è possibile che si verifichino prestazioni ridotte o errori degli allegati ENA nel caso in cui la versione del driver ENA per Windows non sia stata aggiornata.

Causa

I tipi di istanze EC2 di sesta generazione richiedono la seguente versione minima del driver ENA Windows, basata sul sistema operativo (SO) dell'istanza.

Versione minima

Versione di Windows Server	Versione driver ENA
Windows Server 2008 R2	2.2.3 o 2.4.0
Windows Server 2012 e versioni successive	Versione 2.2.3 e successive
Workstation Windows	Versione 2.2.3 e successive

Soluzione

Prima di eseguire l'aggiornamento a un'istanza EC2 di sesta generazione, assicurati che l'AMI da cui esegui l'avvio disponga di driver compatibili basati sul sistema operativo dell'istanza, come mostrato nella tabella precedente. Per ulteriori informazioni, consulta l'articolo Cosa devo fare prima di eseguire la migrazione della mia istanza EC2 a un'istanza di sesta generazione per assicurarmi di ottenere le massime prestazioni di rete? nel Knowledge Center di AWS re:Post .

Prestazioni non ottimali per l'interfaccia di rete elastica (ENI)

Descrizione

L'interfaccia ENA non funziona come previsto.

Causa

L'analisi della causa principale per i problemi di prestazioni è un procedimento per esclusione. Ci sono troppe variabili coinvolte per identificare una causa comune.

Soluzione

Il primo passo nell'analisi della causa principale consiste nell'esaminare le informazioni diagnostiche per l'istanza che non funziona come previsto, per determinare se ci sono errori che potrebbero

causare il problema. Per ulteriori informazioni, consulta la sezione Raccogliere informazioni diagnostiche sull'istanza.

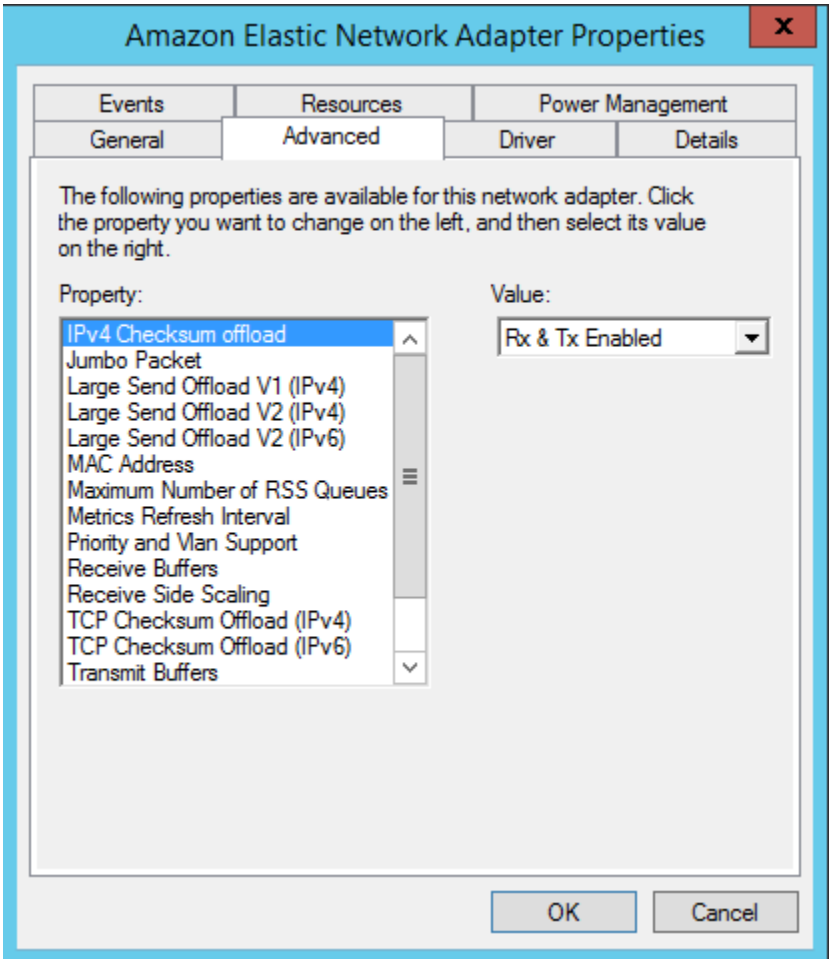
Per ottenere le massime prestazioni di rete sulle istanze con reti avanzate, potrebbe essere necessario modificare la configurazione del sistema operativo predefinita. Alcune ottimizzazioni (come ad esempio l'attivazione dell'offload del checksum e l'abilitazione di RSS) sono configurate sulle AMI ufficiali di Windows per impostazione predefinita. Per altre ottimizzazioni che è possibile applicare all'adattatore ENA, vedere le regolazioni delle prestazioni mostrate in Regolazione delle prestazioni dell'adattatore ENA.

Si consiglia di procedere con cautela e di limitare le regolazioni delle proprietà del dispositivo a quelle elencate in questa sezione o a modifiche specifiche consigliate dal team di supporto. AWS

Per modificare le proprietà dell'adattatore ENA, attenersi alla seguente procedura:

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Amazon Elastic Network Adapter e quindi Proprietà. In questo modo si apre la finestra di dialogo Proprietà di Amazon Elastic Network Adapter.
6. Per apportare le modifiche, apri la scheda Avanzate.
7. Al termine, scegli OK per salvare le modifiche.

L'esempio seguente mostra una proprietà dell'adattatore ENA in Gestione dispositivi di Windows:



Regolazione delle prestazioni dell'adattatore ENA

La tabella seguente include le proprietà che possono essere regolate per migliorare le prestazioni dell'interfaccia ENA.

Input

Proprietà	Descrizione	Valore predefinito	Regolazione
Buffer di ricezione	Controlla il numero di voci nelle code di ricezione del software.	1.024	Questa quota può essere aumentata fino a un massimo di 8192.
Receive Side Scaling (RSS)	Consente la distribuzione efficiente	Abilitato	È possibile distribuire il carico su più

Proprietà	Descrizione	Valore predefinito	Regolazione
	dell'elaborazione della ricezione di rete su più CPU nei sistemi multiprocessore.		processori. Per ulteriori informazioni, consulta Ottimizzazione delle prestazioni di rete sulle istanze Windows.

Proprietà	Descrizione	Valore predefinito	Regolazione
Numero massimo di code RSS	Imposta il numero massimo di code RSS consentite quando RSS è abilitato.	32	Il numero di code RSS viene determinato durante l'inizializzazione del driver e include, tra le altre, le seguenti limitazioni: • Limite di coda RSS impostato da questa proprietà • Limiti di istanza (numero vCPU) • Limiti di generazione hardware (fino a 8 code RSS in ENAv1 e fino a 32 code RSS in ENAv2) È possibile impostare il valore da 1 a 32, a seconda dei limiti di generazione dell'istanza e dell'hardware. Per ulteriori informazioni, consulta Ottimizzazione delle prestazioni di rete sulle istanze Windows.

Proprietà	Descrizione	Valore predefinito	Regolazione
Pacchetti Jumbo	Consente l'utilizzo di frame jumbo ethernet (oltre 1500 byte di payload).	Disabilitato (questo limita il payload a 1500 byte o meno)	Il valore può essere impostato su `9015`, che si traduce in 9001 byte di payload. Questo è il payload massimo per i frame jumbo ethernet. Per informazioni, consulta Considerazioni sull'utilizzo dei frame jumbo ethernet.

Considerazioni sull'utilizzo dei frame jumbo ethernet

I frame jumbo consentono più di 1500 byte di dati aumentando la dimensione di payload per pacchetto, aumentando quindi la percentuale del pacchetto che non suppone un sovraccarico del pacchetto. È quindi necessario un numero minore di pacchetti per inviare la stessa quantità di dati utilizzabili. Tuttavia, il traffico è limitato a un MTU massimo di 1500 nei seguenti casi:

- Traffico al di fuori di una determinata AWS regione per EC2 Classic.
- Traffico esterno a un singolo VPC.
- Traffico su una connessione di peering VPC tra regioni.
- Traffico su connessioni VPN.
- Traffico su un gateway Internet.

> **Note**
>
> I pacchetti superiori a 1500 byte sono frammentati. Se hai flag `Don't Fragment` è impostato nell'intestazione IP, questi pacchetti vengono eliminati.
> I frame jumbo devono essere utilizzati con cautela per il traffico vincolato a Internet o qualsiasi traffico che esca da un VPC. I pacchetti vengono frammentati da sistemi intermedi,

i quali rallentano tale traffico. Per utilizzare i frame jumbo all'interno di un VPC senza influire sul traffico in uscita dal VPC, provare una delle seguenti opzioni:

- Configurare la dimensione MTU per routing.
- Puoi usare più interfacce di rete con dimensioni MTU diverse e instradamenti diversi.

Casi d'uso consigliati per frame jumbo

I frame jumbo possono essere utili per il traffico all'interno e tra i VPC. Si consiglia di utilizzare i frame jumbo per i seguenti casi d'uso:

- Per le istanze collocate in un gruppo di collocazione cluster, i frame jumbo aiutano a raggiungere la massima velocità effettiva della rete possibile. Per ulteriori informazioni, consulta Gruppi di collocamento.
- È possibile utilizzare i frame jumbo per il traffico tra i VPC e le proprie reti locali su AWS Direct Connect. Per ulteriori informazioni sull'utilizzo e la verifica della funzionalità jumbo frame AWS Direct Connect, consulta Impostare l'MTU di rete per le interfacce virtuali private o le interfacce virtuali di transito nella Guida per l'utente.AWS Direct Connect
- Per ulteriori informazioni sulle dimensioni MTU supportate per i Transit Gateway, consultare Quote per Transit Gateway in Amazon VPC Transit Gateway.

Miglioramento della latenza di rete per le istanze Amazon EC2 basate su Linux

La latenza di rete è il tempo che un pacchetto di dati impiega per viaggiare dall'origine alla destinazione. Le applicazioni che inviano dati attraverso la rete dipendono da risposte tempestive per fornire un'esperienza utente positiva. Una latenza di rete elevata può portare a vari problemi, come i seguenti:

- Tempi di caricamento lenti per le pagine Web
- Ritardi nello streaming video
- Difficoltà di accesso alle risorse online

Questa sezione descrive le misure che puoi adottare per migliorare la latenza di rete sulle istanze Amazon EC2 in esecuzione su Linux. Per ottenere una latenza ottimale, segui questi passaggi per

configurare le impostazioni dell'istanza, del kernel e del driver ENA. Per ulteriori indicazioni sulla configurazione, consulta la Guida alle best practice e all'ottimizzazione delle prestazioni dei driver ENA Linux suGitHub.

> **Note**
>
> I passaggi e le impostazioni possono variare leggermente a seconda dell'hardware di rete specifico, dell'AMI dalla quale hai avviato l'istanza e del caso d'uso dell'applicazione. Prima di apportare modifiche, verifica e monitora accuratamente le prestazioni della rete per assicurarti di ottenere i risultati desiderati.

Riduzione degli hop di rete

Ogni hop eseguito da un pacchetto di dati mentre si sposta da un router all'altro aumenta la latenza di rete. In genere, il traffico deve compiere più hop per raggiungere la destinazione. Esistono due modi per ridurre gli hop di rete per le istanze Amazon EC2, descritti di seguito:

- Gruppo di posizionamento cluster: quando specifichi un gruppo di posizionamento cluster, Amazon EC2 avvia le istanze che si trovano vicine l'una all'altra, fisicamente all'interno della stessa zona di disponibilità (AZ) con pacchetti più ristretti. La vicinanza fisica delle istanze del gruppo consente loro di sfruttare la connettività ad alta velocità, con conseguente bassa latenza ed elevata velocità di trasmissione effettiva a flusso singolo.
- Host dedicato: un host dedicato è un server fisico dedicato al tuo utilizzo. Con un host dedicato, puoi avviare le tue istanze per eseguirle sullo stesso server fisico. La comunicazione tra istanze eseguite sullo stesso host dedicato può avvenire senza hop di rete aggiuntivi.

Configurazione del kernel Linux

La configurazione del kernel Linux può aumentare o diminuire la latenza di rete. Per raggiungere gli obiettivi di ottimizzazione della latenza, è importante ottimizzare la configurazione del kernel Linux in base ai requisiti specifici del tuo carico di lavoro.

Molte opzioni di configurazione per il kernel Linux potrebbero contribuire a ridurre la latenza di rete. Le opzioni che hanno un impatto maggiore sono le seguenti.

- Abilita la modalità polling occupato: la modalità polling occupato riduce la latenza sul percorso di ricezione della rete. Quando si abilita la modalità polling occupato, il codice del socket layer

può interrogare direttamente la coda di ricezione di un dispositivo di rete. L'aspetto negativo del polling attivo è il maggiore utilizzo della CPU nell'host, derivante dall'analisi di nuovi dati in un ciclo ristretto. Esistono due impostazioni globali che controllano il numero di microsecondi di attesa per i pacchetti in tutte le interfacce.

`busy_read`

Un timeout di polling attivo a bassa latenza per le letture del socket. Controlla il numero di microsecondi di attesa concessi al socket layer per leggere i pacchetti nella coda del dispositivo. Per abilitare la funzionalità a livello globale con il comando sysctl, l'organizzazione del kernel Linux consiglia un valore di 50 microsecondi. Per ulteriori informazioni, consulta busy_read nella Guida per l'utente e l'amministratore del kernel Linux.

```
$ C:\> sudo sysctl -w net.core.busy_read=50
```

`busy_poll`

Un timeout di polling attivo a bassa latenza per il polling e la selezione. Questo timeout controlla il numero di microsecondi di attesa per gli eventi. Il valore consigliato è tra 50-100 microsecondi, in base al numero di socket di cui esegui il polling. Più socket aggiungi, più alto dovrebbe essere il numero.

```
$ C:\> sudo sysctl -w net.core.busy_poll=50
```

- Configura gli stati di alimentazione CPU (C-state): gli stati C-state controllano i livelli di sospensione in cui potrebbe entrare un core quando è inattivo. Potresti voler controllare gli stati C-state per ottimizzare la latenza rispetto alle prestazioni del sistema. Negli stati C più profondi, la CPU è essenzialmente "addormentata" e non può rispondere alle richieste finché non si risveglia e torna in uno stato attivo. Inserire i core nello stato di sospensione richiedete del tempo. Sebbene un core sospeso consenta maggiore capacità aggiuntiva per un altro core per raggiungere una frequenza più elevata, è necessario del tempo affinché il core sospeso torni attivo e in funzione.

  Ad esempio, se un core assegnato per gestire le interruzioni di un pacchetto di rete è addormentato, potrebbe verificarsi un ritardo nel lavoro su tale interruzione. Puoi configurare il sistema in modo che non utilizzi stati C più profondi. Tuttavia, questa configurazione non solo riduce la latenza della reazione del processore, ma anche la capacità disponibile negli altri core per il Turbo Boost.

Per ridurre la latenza di reazione del processore, è possibile limitare gli stati C-state più profondi. Per ulteriori informazioni, consulta Prestazioni elevate e bassa latenza limitando gli stati C più profondi nella Guida per l'utente di Amazon Linux 2.

Configurazione del driver ENA

Il driver di rete ENA consente la comunicazione tra un'istanza e una rete. Il driver elabora i pacchetti di rete e li trasmette allo stack di rete o alla scheda Nitro. Quando arriva un pacchetto di rete, la scheda Nitro genera un'interruzione per consentire alla CPU di notificare al software un evento.

Interruzione

Un'interruzione è un segnale che un dispositivo o un'applicazione invia al processore. L'interruzione indica al processore che si è verificato un evento o è stata soddisfatta una condizione che richiede un'attenzione immediata. Le interruzioni possono gestire attività urgenti come la ricezione di dati da un'interfaccia di rete, la gestione di eventi hardware o di richieste di assistenza da altri dispositivi.

Moderazione delle interruzioni

La moderazione delle interruzioni è una tecnica che riduce il numero di interruzioni generate da un dispositivo aggregandole o ritardandole. Lo scopo della moderazione delle interruzioni è migliorare le prestazioni del sistema riducendo il sovraccarico associato alla gestione di un numero elevato di interruzioni. Troppe interruzioni aumentano l'utilizzo della CPU, influendo negativamente sulla velocità di trasmissione effettiva, mentre un numero insufficiente di interruzioni aumenta la latenza.

Moderazione dinamica delle interruzioni

La moderazione dinamica delle interruzioni è una forma avanzata di moderazione delle interruzioni che regola dinamicamente la frequenza di interruzione in base al carico del sistema e ai modelli di traffico correnti. Ha l'obiettivo di trovare un equilibrio tra la riduzione del sovraccarico delle interruzioni e dei pacchetti al secondo e la larghezza di banda.

> **Note**
>
> La moderazione dinamica delle interruzioni è abilitata per impostazione predefinita in alcune AMI (ma può essere abilitata o disabilitata in tutte le AMI).

Per ridurre al minimo la latenza di rete, potrebbe essere necessario disabilitare la moderazione delle interruzioni. Tuttavia, ciò può anche aumentare il sovraccarico dato dall'elaborazione delle interruzioni. È importante trovare il giusto equilibrio tra riduzione della latenza e riduzione al minimo del sovraccarico. I comandi `ethtool` possono aiutarti a configurare la moderazione delle interruzioni. Per impostazione predefinita, `rx-usecs` è impostato su `20` e `tx-usecs` è impostato su `64`.

Per ottenere la configurazione di modifica dell'interruzione corrente, utilizza il comando seguente.

```
$ C:\> ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on  TX: off
rx-usecs: 20
tx-usecs: 64
```

Per disabilitare la moderazione dell'interruzione e la moderazione dinamica dell'interruzione, utilizza il comando seguente.

```
$ C:\> sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Considerazioni sul sistema Nitro per l'ottimizzazione delle prestazioni

Nitro System è una raccolta di componenti hardware e software generati da AWS che abilitano prestazioni elevate, alta disponibilità ed elevata sicurezza. Il sistema Nitro offre funzionalità simili al bare metal che eliminano il sovraccarico di virtualizzazione e supportano carichi di lavoro che richiedono l'accesso completo all'hardware host. Per informazioni più dettagliate, consulta Nitro System.AWS

Tutti i tipi di istanze EC2 dell'attuale generazione eseguono l'elaborazione dei pacchetti di rete su schede Nitro EC2. Questo argomento tratta la gestione dei pacchetti di alto livello sulla scheda Nitro, gli aspetti comuni dell'architettura e della configurazione di rete che influiscono sulle prestazioni di gestione dei pacchetti e le azioni che è possibile intraprendere per ottenere le massime prestazioni per le istanze basate su Nitro.

Le schede Nitro gestiscono tutte le interfacce di input e output (I/O), come quelle necessarie per i Virtual Private Cloud (VPC). Per tutti i componenti che inviano o ricevono informazioni sulla rete, le schede Nitro fungono da dispositivo informatico autonomo per il traffico I/O, fisicamente separato dalla scheda madre del sistema su cui vengono eseguiti i carichi di lavoro dei clienti.

Flusso di pacchetti di rete sulle schede Nitro

Le istanze EC2 basate sul sistema Nitro dispongono di funzionalità di accelerazione hardware che consentono un'elaborazione dei pacchetti più rapida, misurata in base alla velocità di trasmissione dei pacchetti al secondo (PPS). Quando una scheda Nitro esegue la valutazione iniziale di un nuovo flusso, salva le informazioni che sono le stesse per tutti i pacchetti del flusso, come i gruppi di sicurezza, gli elenchi di controllo degli accessi e le voci della tabella di routing. Quando elabora pacchetti aggiuntivi per lo stesso flusso, può utilizzare le informazioni salvate per ridurre il sovraccarico di tali pacchetti.

La velocità di connessione viene misurata in base alla metrica delle connessioni al secondo (CPS). Ogni nuova connessione richiede un sovraccarico di elaborazione aggiuntivo che deve essere preso in considerazione nelle stime della capacità del carico di lavoro. È importante considerare sia le metriche CPS che PPS quando si progettano i carichi di lavoro.

Come viene stabilita una connessione

Quando viene stabilita una connessione tra un'istanza basata su Nitro e un altro endpoint, la scheda Nitro valuta l'intero flusso del primo pacchetto inviato o ricevuto tra i due endpoint. Per i pacchetti successivi dello stesso flusso, in genere non è necessaria una rivalutazione completa. Esistono tuttavia delle eccezioni. Per ulteriori informazioni sulle eccezioni, vedere. Pacchetti che non utilizzano l'accelerazione hardware

Le seguenti proprietà definiscono i due punti finali e il flusso di pacchetti tra di essi. Queste cinque proprietà insieme sono note come flusso a 5 tuple.

- IP di origine
- Porta sorgente
- IP di destinazione
- Porta di destinazione
- Protocollo di comunicazione

La direzione del flusso di pacchetti è nota come ingresso (in entrata) e uscita (in uscita). Le seguenti descrizioni di alto livello riassumono il flusso di pacchetti di rete end-to-end.

- Ingress: quando una scheda Nitro gestisce un pacchetto di rete in entrata, valuta il pacchetto rispetto alle regole del firewall stateful e agli elenchi di controllo degli accessi. Tiene traccia della

connessione, la contabilizza ed esegue altre azioni, a seconda dei casi. Quindi inoltra il pacchetto alla sua destinazione sulla CPU host.

- Uscita: quando una scheda Nitro gestisce un pacchetto di rete in uscita, cerca la destinazione dell'interfaccia remota, valuta varie funzioni VPC, applica limiti di velocità ed esegue altre azioni pertinenti. Quindi inoltra il pacchetto alla destinazione hop successiva sulla rete.

Progettato per prestazioni ottimali

Per sfruttare le funzionalità prestazionali del sistema Nitro, è necessario comprendere quali sono le esigenze di elaborazione di rete e in che modo tali esigenze influiscono sul carico di lavoro delle risorse Nitro. Quindi puoi progettare per ottenere prestazioni ottimali per il tuo panorama di rete. Le impostazioni dell'infrastruttura e la progettazione e configurazione del carico di lavoro delle applicazioni possono influire sia sull'elaborazione dei pacchetti che sulle velocità di connessione. Ad esempio, se l'applicazione ha un'elevata velocità di creazione delle connessioni, ad esempio un servizio DNS, un firewall o un router virtuale, avrà meno possibilità di sfruttare l'accelerazione hardware che si verifica solo dopo aver stabilito la connessione.

È possibile configurare le impostazioni dell'applicazione e dell'infrastruttura per semplificare i carichi di lavoro e migliorare le prestazioni di rete. Tuttavia, non tutti i pacchetti sono idonei all'accelerazione. Il sistema Nitro utilizza l'intero flusso di rete per nuove connessioni e per pacchetti non idonei all'accelerazione.

La parte restante di questa sezione si concentrerà sulle considerazioni relative alla progettazione di applicazioni e infrastrutture per garantire che i pacchetti fluiscano il più possibile all'interno del percorso accelerato.

Considerazioni

Quando configuri il traffico di rete per la tua istanza, ci sono molti aspetti da considerare che possono influire sulle prestazioni di PPS. Una volta stabilito un flusso, la maggior parte dei pacchetti che entrano o escono regolarmente sono idonei all'accelerazione. Tuttavia, esistono eccezioni per garantire che i progetti dell'infrastruttura e i flussi di pacchetti continuino a soddisfare gli standard del protocollo.

Per ottenere le migliori prestazioni dalla tua scheda Nitro, dovresti considerare attentamente i pro e i contro dei seguenti dettagli di configurazione per la tua infrastruttura e le tue applicazioni.

Considerazioni sull'infrastruttura

La configurazione dell'infrastruttura può influire sul flusso di pacchetti e sull'efficienza di elaborazione. L'elenco seguente include alcune considerazioni importanti.

Configurazione dell'interfaccia di rete con asimmetria

I gruppi di sicurezza utilizzano il tracciamento delle connessioni per tenere traccia delle informazioni sul traffico che fluisce da e verso l'istanza. Il routing asimmetrico, in cui il traffico entra in un'istanza attraverso un'interfaccia di rete e esce attraverso un'altra interfaccia di rete, può ridurre le prestazioni di picco che un'istanza può raggiungere se i flussi vengono tracciati. Per ulteriori informazioni sul tracciamento delle connessioni dei gruppi di sicurezza, sulle connessioni non tracciate e sulle connessioni tracciate automaticamente, vedere. Monitoraggio della connessione al gruppo di sicurezza

Driver di rete

I driver di rete vengono aggiornati e rilasciati regolarmente. Se i driver non sono aggiornati, ciò può compromettere notevolmente le prestazioni. Mantieni aggiornati i driver per assicurarti di disporre delle patch più recenti e di poter sfruttare i miglioramenti delle prestazioni, come la funzionalità di percorso accelerato disponibile solo per i driver di ultima generazione. I driver precedenti non supportano la funzionalità di percorso accelerato.

Per sfruttare la funzionalità di percorso accelerato, ti consigliamo di installare il driver ENA più recente sulle tue istanze.

Istanze Linux: driver ENA Linux 2.2.9 o successivo. Per installare o aggiornare il driver ENA Linux dal GitHub repository Amazon Drivers, consulta la sezione sulla compilazione dei driver del file readme.

Istanze Windows: driver ENA Windows 2.0.0 o successivo. Per installare o aggiornare il driver ENA per Windows, vedere. Installa il driver Elastic Network Adapter (ENA)

Distanza tra i punti finali

Una connessione tra due istanze nella stessa zona di disponibilità può elaborare più pacchetti al secondo rispetto a una connessione tra regioni grazie alla finestra TCP a livello di applicazione, che determina la quantità di dati che possono essere trasmessi in un dato momento. Le lunghe distanze tra le istanze aumentano la latenza e riducono il numero di pacchetti che gli endpoint possono elaborare.

Considerazioni sulla progettazione delle applicazioni

Esistono aspetti della progettazione e della configurazione delle applicazioni che possono influire sull'efficienza di elaborazione. L'elenco seguente include alcune considerazioni importanti.

Dimensioni del pacchetto

Pacchetti di dimensioni maggiori possono aumentare la velocità di trasmissione dei dati che un'istanza può inviare e ricevere sulla rete. Pacchetti di dimensioni inferiori possono aumentare la velocità di elaborazione dei pacchetti, ma ciò può ridurre la larghezza di banda massima ottenuta quando il numero di pacchetti supera le tolleranze PPS.

Se la dimensione di un pacchetto supera l'unità di trasmissione massima (MTU) di un hop di rete, un router lungo il percorso potrebbe frammentarlo. I frammenti di pacchetto risultanti sono considerati eccezioni e vengono elaborati alla velocità standard (non accelerata). Ciò può causare variazioni nelle prestazioni. Amazon EC2 supporta jumbo frame da 9001 byte, tuttavia non tutti i servizi lo supportano. Ti consigliamo di valutare la topologia quando configuri MTU.

Compromessi relativi al protocollo

I protocolli affidabili come TCP hanno un sovraccarico maggiore rispetto ai protocolli inaffidabili come UDP. Il sovraccarico inferiore e l'elaborazione di rete semplificata per il protocollo di trasporto UDP possono comportare un tasso di PPS più elevato, ma a scapito di una consegna affidabile dei pacchetti. Se la consegna affidabile dei pacchetti non è fondamentale per la tua applicazione, UDP potrebbe essere una buona opzione.

Microscoppio

Il microbursting si verifica quando il traffico supera i limiti consentiti per brevi periodi di tempo anziché essere distribuito uniformemente. Ciò si verifica in genere su una scala di microsecondi.

Ad esempio, supponiamo di avere un'istanza in grado di inviare fino a 10 Gbps e che l'applicazione invii tutti i 10 Gb in mezzo secondo. Questo microburst supera il limite consentito durante il primo mezzo secondo e non lascia nulla per il resto del secondo. Anche se avete inviato 10 GB nell'arco di tempo di 1 secondo, le quote consentite nel primo mezzo secondo possono far sì che i pacchetti vengano messi in coda o eliminati.

È possibile utilizzare uno strumento di pianificazione di rete come Linux Traffic Control per velocizzare la velocità di trasmissione ed evitare che i pacchetti vengano messi in coda o persi a causa del microbursting.

Numero di flussi

Un singolo flusso è limitato a 5 Gbps a meno che non si trovi all'interno di un gruppo di posizionamento del cluster che supporta fino a 10 Gbps o se utilizzi ENA Express, che supporta fino a 25 Gbps.

Allo stesso modo, una scheda Nitro può elaborare più pacchetti su più flussi anziché utilizzare un singolo flusso. Per raggiungere la massima velocità di elaborazione dei pacchetti per istanza, consigliamo almeno 100 flussi su istanze con una larghezza di banda aggregata pari o superiore a 100 Gbps. Con l'aumentare delle capacità di larghezza di banda aggregata, aumenta anche il numero di flussi necessari per raggiungere le velocità di elaborazione di picco. Il benchmarking ti aiuterà a determinare la configurazione necessaria per raggiungere le frequenze di picco sulla tua rete.

Numero di code Elastic Network Adapter (ENA)

Per impostazione predefinita, il numero massimo di code ENA viene assegnato a un'interfaccia di rete in base alla dimensione e al tipo di istanza. La riduzione del numero di code può ridurre la velocità PPS massima raggiungibile. Si consiglia di utilizzare l'allocazione della coda predefinita per ottenere prestazioni ottimali.

Per Linux, per impostazione predefinita, un'interfaccia di rete è configurata con il valore massimo. Per le applicazioni basate sul Data Plane Development Kit (DPDK), si consiglia di configurare il numero massimo di code disponibili.

Sovraccarico del processo delle funzionalità

Funzionalità come Traffic Mirroring ed ENA Express possono aumentare il sovraccarico di elaborazione, il che può ridurre le prestazioni assolute di elaborazione dei pacchetti. È possibile limitare l'uso delle funzionalità o disabilitarle per aumentare la velocità di elaborazione dei pacchetti.

Monitoraggio della connessione per mantenere lo stato

I tuoi gruppi di sicurezza utilizzano il tracciamento delle connessioni per archiviare informazioni sul traffico da e verso l'istanza. Il monitoraggio delle connessioni applica regole a ogni singolo flusso di traffico di rete per determinare se il traffico è consentito o negato. La scheda Nitro utilizza il tracciamento del flusso per mantenere lo stato del flusso. Man mano che vengono applicate più regole del gruppo di sicurezza, è necessario più lavoro per valutare il flusso.

> **Note**
>
> Non tutti i flussi di traffico di rete vengono tracciati. Se una regola del gruppo di sicurezza è configurata conConnessioni non tracciate, non è necessario alcun intervento aggiuntivo, ad eccezione delle connessioni che vengono tracciate automaticamente per garantire un routing simmetrico in presenza di più percorsi di risposta validi.

Pacchetti che non utilizzano l'accelerazione hardware

Non tutti i pacchetti possono sfruttare l'accelerazione hardware. La gestione di queste eccezioni comporta un sovraccarico di elaborazione necessario per garantire l'integrità dei flussi di rete. I flussi di rete devono soddisfare in modo affidabile gli standard del protocollo, conformarsi alle modifiche nella progettazione del VPC e indirizzare i pacchetti solo verso destinazioni consentite. Tuttavia, il sovraccarico riduce le prestazioni.

Frammenti di pacchetti

Come indicato nella sezione Considerazioni relative all'applicazione, i frammenti di pacchetto che derivano da pacchetti che superano l'MTU di rete vengono gestiti come eccezioni e non possono sfruttare l'accelerazione hardware.

Connessioni inattive

Quando una connessione non è attiva per un certo periodo di tempo, anche se non ha raggiunto il limite di timeout, il sistema può ridurle la priorità. Quindi, se i dati arrivano dopo l'eliminazione della priorità della connessione, il sistema deve gestirli come un'eccezione per riconnettersi.

Per gestire le connessioni, puoi utilizzare i timeout di tracciamento delle connessioni per chiudere le connessioni inattive. Puoi anche utilizzare i keepalive TCP per mantenere aperte le connessioni inattive. Per ulteriori informazioni, consulta Timeout di tracciamento delle connessioni inattive.

Mutazione VPC

Gli aggiornamenti ai gruppi di sicurezza, alle tabelle di routing e agli elenchi di controllo degli accessi devono essere tutti rivalutati nel percorso di elaborazione per garantire che le voci delle route e le regole dei gruppi di sicurezza continuino ad essere applicate come previsto.

Flussi ICMP

Internet Control Message Protocol (ICMP) è un protocollo a livello di rete utilizzato dai dispositivi di rete per diagnosticare i problemi di comunicazione di rete. Questi pacchetti utilizzano sempre il flusso completo.

Massimizza le prestazioni di rete sul tuo sistema Nitro

Prima di prendere decisioni di progettazione o modificare le impostazioni di rete sulla tua istanza, ti consigliamo di eseguire le seguenti operazioni per assicurarti di ottenere il miglior risultato:

1. Scopri i pro e i contro delle azioni che puoi intraprendere per migliorare le prestazioni esaminando. Considerazioni

   Per ulteriori considerazioni e procedure consigliate per la configurazione dell'istanza, consulta:

   Istanze Linux: guida alle best practice e all'ottimizzazione delle prestazioni dei driver ENA Linux sul GitHub sito Web.

   Istanze Windows —. Best practice per la configurazione delle interfacce di rete
2. Effettua un benchmark dei tuoi carichi di lavoro con il conteggio dei flussi attivi di picco per determinare una base per le prestazioni delle tue applicazioni. Con una baseline delle prestazioni, puoi testare le variazioni nelle impostazioni o nella progettazione dell'applicazione per capire quali considerazioni avranno il maggiore impatto, soprattutto se prevedi di scalare verso l'alto o verso l'alto.

L'elenco seguente contiene le azioni che è possibile intraprendere per ottimizzare le prestazioni del PPS, a seconda delle esigenze del sistema.

- Riduci la distanza fisica tra due istanze. Quando le istanze di invio e ricezione si trovano nella stessa zona di disponibilità o utilizzano gruppi di collocamento in cluster, è possibile ridurre il numero di passaggi necessari a un pacchetto per viaggiare da un endpoint all'altro.
- Utilizza Connessioni non tracciate.
- Utilizza il protocollo UDP per il traffico di rete.
- Per le istanze EC2 con larghezza di banda aggregata pari o superiore a 100 Gbps, distribuisci il carico di lavoro su 100 o più flussi individuali per distribuire il lavoro in modo uniforme sulla scheda Nitro.

Monitora le prestazioni sulle istanze Linux

È possibile utilizzare le metriche Ethtool sulle istanze Linux per monitorare gli indicatori delle prestazioni di rete delle istanze come larghezza di banda, velocità dei pacchetti e tracciamento della connessione. Per ulteriori informazioni, consulta Monitoraggio delle prestazioni di rete per l'istanza EC2.

Ottimizzazione delle prestazioni di rete sulle istanze Windows

Per ottenere le massime prestazioni di rete sulle istanze Windows con reti avanzate, potrebbe essere necessario modificare la configurazione predefinita del sistema operativo. Si consiglia di apportare le seguenti modifiche alla configurazione per le applicazioni che richiedono prestazioni di rete elevate. Altre ottimizzazioni (come l'attivazione dell'offload con checksum e l'abilitazione di RSS, ad esempio) sono già configurate nelle AMI Windows ufficiali.

> **Note**
>
> TCP chimney offload dovrebbe essere disabilitato nella maggior parti dei casi d'uso ed è stato reso obsoleto con Windows Server 2016.

Oltre a queste ottimizzazioni del sistema operativo, devi anche considerare l'unità di trasmissione massima (MTU) del traffico di rete e regolare in base al carico di lavoro e all'architettura di rete. Per ulteriori informazioni, consulta Unità massima di trasmissione (MTU) di rete per istanza EC2.

AWS misura regolarmente le latenze medie di andata e ritorno tra le istanze avviate in un gruppo di posizionamento del cluster di 50us e le latenze di coda di 200us al 99,9%. Se le tue applicazioni richiedono costantemente latenze basse, consigliamo di utilizzare l'ultima versione dei driver ENA nelle istanze basate sul sistema Nitro con prestazioni fisse.

Configurazione di RSS CPU Affinity

Receive Side Scaling (RSS) viene utilizzato per distribuire il carico della CPU del traffico di rete su più processori. Come impostazione predefinita, le AMI Amazon Windows ufficiali sono configurate con RSS abilitato. Gli ENI ENA forniscono fino a otto code RSS. Definendo l'affinità dei CPU per le code RSS, nonché per altri processi del sistema, è possibile distribuire il carico di lavoro della CPU su sistemi multi-core e consentire l'elaborazione di più traffico di rete. Per i tipi di istanza con più di 16 vCPU, si consiglia di utilizzare `Set-NetAdapterRSS` PowerShell il cmdlet, che esclude

manualmente il processore di avvio (processore logico 0 e 1 quando l'hyper-threading è abilitato) dalla configurazione RSS per tutti gli ENI, al fine di evitare conflitti con vari componenti del sistema.

Windows è compatibile con hyperthreading e assicurerà che le code RSS di un singolo NIC vengano sempre posizionate su diversi core fisici. Quindi, almeno che hypertgreading sia disabilitato, per prevenire completamente conflitti con altri NIC, distribuisci la configurazione RSS di ogni NIC in una gamma di 16 processori logici. Il `Set-NetAdapterRss` cmdlet consente di definire la gamma Per-NIC di processori logici validi definendo i valori di,,, e (opzionale). BaseProcessorGroup BaseProcessorNumber MaxProcessingGroup MaxProcessorNumber NumaNode Se non ci sono abbastanza core fisici per eliminare completamente conflitti inter-NIC, minimizza le gamme in sovrapposizione o riduci il numero di processori logici nelle gamme ENI in base al carico di lavoro previsto dell'ENI (in altre parole, un'ENI di rete amministrativa di basso volume potrebbe non aver bisogno di così tante code RSS assegnate). Inoltre, come indicato precedentemente, i vari componenti devono essere eseguiti su CPU 0 e quindi è consigliabile escluderla da tutte le configurazioni RSS quando è disponibile un numero sufficiente di vCPU.

Ad esempio, quando sono presenti tre ENI su un'istanza a 72 vCPU con due nodi NUMA con l'hyper-threading abilitato, i comandi seguenti distribuiscono il carico di rete tra le due CPU senza sovrapposizione e impediscono completamente l'utilizzo del core 0.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -
MaxProcessorNumber 16
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -
MaxProcessorNumber 14
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -
MaxProcessorNumber 30
```

Nota che queste impostazioni sono persistenti per ogni adattatore di rete. Se un'istanza viene ridimensionata a uno con un numero diverso di vCPU, devi rivalutare la configurazione RSS per ogni ENI abilitata. La documentazione Microsoft completa per il cmdlet `Set-NetAdapterRss` è disponibile qui: https://docs.microsoft.com/en-us/powershell/module/netadapter/set-netadapterrss.

Nota speciale per i carichi di lavoro SQL: consigliamo inoltre di controllare le impostazioni di affinità del thread IO assieme alla configurazione RSS dell'ENI per ridurre al minimo i conflitti di I/O e di rete per le stesse CPU. Consulta Opzione di configurazione server maschera affinità.

Elastic Fabric Adapter

Un Elastic Fabric Adapter (EFA) è un dispositivo di rete che è possibile collegare alle istanze Amazon EC2 per accelerare le applicazioni per sistemi computerizzati ad alte prestazioni (HPC) e machine learning. EFA consente di ottenere le prestazioni applicative di un cluster HPC locale, con la scalabilità, la flessibilità e l'elasticità fornite dal cloud. AWS

Gli EFA garantiscono valori di latenza più bassi e coerenti e una velocità di trasmissione effettiva più elevata rispetto al trasporto TCP generalmente utilizzato nei sistemi HPC basati su cloud. Migliora inoltre le prestazioni delle comunicazioni tra istanze, essenziali per il dimensionamento delle applicazioni HPC e machine learning. È ottimizzato per funzionare sull'infrastruttura di AWS rete esistente e può essere scalato in base ai requisiti dell'applicazione.

Gli EFA si integrano con Libfabric versione 1.7.0 e successive e supportano le applicazioni Open MPI 5 e successive e Intel MPI 2019 aggiornamento 5 e successivi per applicazioni HPC e Nvidia Collective Communications Library (NCCL) per le applicazioni machine learning.

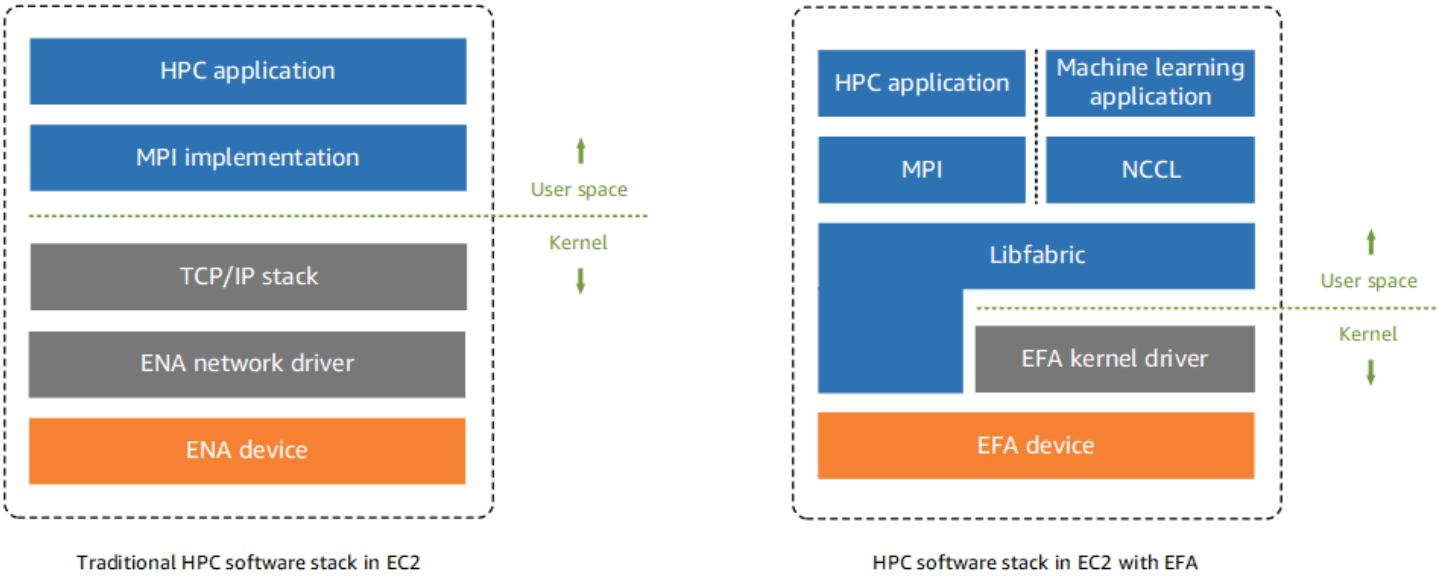
> **Note**
>
> Le funzionalità di bypass del sistema operativo degli EFAs non sono supportate sulle istanze Windows. Se colleghi un EFA a un'istanza Windows, quest'ultima opera come un Elastic Network Adapter, senza le ulteriori funzionalità EFA.

Indice

- Verifica del programma di installazione EFA utilizzando un checksum

Nozioni di base su EFA

Un EFA è un Elastic Network Adapter (ENA) con ulteriori funzionalità. Garantisce tutte le funzionalità di un ENA con in più la funzione di bypass del sistema operativo, ovvero un modello di accesso che consente alle applicazioni HPC e machine learning di comunicare direttamente con l'hardware dell'interfaccia di rete per offrire funzionalità di trasporto affidabili e a bassa latenza.



Per interfacciarsi con il trasporto di rete del sistema, in genere le applicazioni HPC utilizzano l'interfaccia MPI (Message Passing Interface). Nel AWS cloud, ciò significa che le applicazioni si interfacciano con MPI, che utilizza quindi lo stack TCP/IP del sistema operativo e il driver del dispositivo ENA per abilitare la comunicazione di rete tra le istanze.

Con EFA, le applicazioni HPC utilizzano o NCCL per interfacciarsi con l'API Libfabric L'API di Libfabric bypassa il kernel del sistema operativo e comunica direttamente con il dispositivo EFA per immettere in rete i pacchetti. Questo riduce il sovraccarico e consente una più efficiente esecuzione dell'applicazione HPC.

> **Note**
>
> Libfabric è un componente fondamentale del framework OpenFabrics Interfaces (OFI), che definisce ed esporta l'API dello spazio utente di OFI. Per ulteriori informazioni, consulta il sito Web Libfabric. OpenFabrics

Differenze tra EFAs e ENA

Gli Elastic Network Adapter (ENA) forniscono le tradizionali caratteristiche di rete IP necessarie per supportare le reti VPC. Gli EFA forniscono le stesse caratteristiche degli ENA e supportano anche le funzionalità di bypass del sistema operativo. Queste ultime consentono alle applicazioni HPC e machine learning di bypassare il kernel del sistema operativo e di comunicare direttamente con il dispositivo EFA.

Librerie e interfacce supportate

Gli EFA supportano le seguenti interfacce e librerie:

- Open MPI versione 5 e successive
- Per Graviton ti consigliamo di utilizzare Open MPI 4.0 o versioni successive
- Intel MPI 2019 aggiornamento 5 e successivi
- NVIDIA Collective Communications Library (NCCL) 2.4.2 e versioni successive

Tipi di istanze supportati

I seguenti tipi di istanza supportano EFAs:

- Scopo generale: `m5dn.24xlarge` `m5dn.metal` | `m5n.24xlarge` `m5n.metal` | `m5zn.12xlarge` | `m5zn.metal` | `m6a.48xlarge` | `m6a.metal` | `m6i.32xlarge` | `m6i.metal` | `m6id.32xlarge` | `m6id.metal` | `m6idn.32xlarge` | `m6idn.metal` | `m6in.32xlarge` `m6in.metal` | `m7a.48xlarge` | `m7a.metal-48xl` | `m7g.16xlarge` | `m7g.metal` | `m7gd.16xlarge` | `m7gd.metal` | `m7i.48xlarge` `m7i.metal-48xl`
- Ottimizzato per il calcolo: `c5n.9xlarge` `c5n.18xlarge` `c5n.metal` | `c6a.48xlarge` | `c6a.metal` | `c6gn.16xlarge` | `c6i.32xlarge` `c6i.metal` | `c6id.32xlarge` | `c6id.metal` | `c6in.32xlarge` | `c6in.metal` | `c7a.48xlarge` | `c7a.metal-48xl` | `c7g.16xlarge` | `c7g.metal` | `c7gd.16xlarge` | `c7gd.metal` | `c7gn.16xlarge` | `c7gn.metal` | `c7i.48xlarge` `c7i.metal-48xl`
- Memoria ottimizzata: `r5dn.24xlarge` `r5dn.metal` `r5n.24xlarge` `r5n.metal` | `r6a.48xlarge` | `r6a.metal` | `r6i.32xlarge` | `r6i.metal` `r6idn.32xlarge` | `r6idn.metal` | `r6in.32xlarge` | `r6in.metal` | `r6id.32xlarge` | `r6id.metal` | `r7a.48xlarge` | `r7a.metal-48xl` `r7g.16xlarge` | `r7g.metal` | `r7gd.16xlarge` | `r7gd.metal` | `r7i.48xlarge` | `r7i.metal-48xl` | `r7iz.32xlarge` | `r7iz.metal-32xl` `r8g.24xlarge` | `r8g.48xlarge` | `r8g.metal-24xl` | `r8g.metal-48xl` | `u7i-12tb.224xlarge`

| u7in-16tb.224xlarge | u7in-24tb.224xlarge | u7in-32tb.224xlarge x2idn.32xlarge | x2idn.metal | x2iedn.32xlarge | x2iedn.metal | x2iezn.12xlarge x2iezn.metal

- Storage ottimizzato: i3en.12xlarge | i3en.24xlarge | i3en.metal | i4g.16xlarge | i4i.32xlarge | i4i.metal | im4gn.16xlarge
- Calcolo accelerato: dl1.24xlarge dl2q.24xlarge g4dn.8xlarge | g4dn.12xlarge | g4dn.16xlarge | g4dn.metal g5.8xlarge | g5.12xlarge | g5.16xlarge | g5.24xlarge | g5.48xlarge | g6.8xlarge g6.12xlarge | g6.16xlarge | g6.24xlarge | g6.48xlarge | gr6.8xlarge | inf1.24xlarge | p3dn.24xlarge p4d.24xlarge | p4de.24xlarge | p5.48xlarge | trn1.32xlarge | trn1n.32xlarge vt1.24xlarge
- Elaborazione ad alte prestazioni: hpc6a.48xlarge | hpc6id.32xlarge | hpc7a.12xlarge | | hpc7a.24xlarge | hpc7a.48xlarge | | hpc7a.96xlarge | hpc7g.4xlarge hpc7g.8xlarge hpc7g.16xlarge

Per visualizzare i tipi di istanza disponibili che supportano gli EFA in una regione specifica

I tipi di istanza disponibili variano in base alla regione. Per visualizzare i tipi di istanza disponibili che supportano gli EFA in una regione, usa il describe-instance-typescomando con il --region parametro. Includi il parametro --filters per assegnare i risultati ai tipi di istanza che supportano EFA e il parametro --query per assegnare l'output al valore di InstanceType.

```
aws ec2 describe-instance-types  --region us-east-1  --filters Name=network-info.efa-supported,Values=true  --query "InstanceTypes[*].[InstanceType]"  --output text | sort
```

Sistemi operativi supportati

Il supporto del sistema operativo varia a seconda del tipo di processore. La tabella seguente mostra i sistemi operativi supportati.

Sistema operativo	Tipi di istanze Intel/AMD () **x86_64**	AWS Tipi di istanze Graviton () **arm64**
Amazon Linux 2023	✓	✓
Amazon Linux 2	✓	✓

Sistema operativo	Tipi di istanze Intel/AMD () **x86_64**	AWS Tipi di istanze Graviton () **arm64**
CentOS 7	✓	
RHEL 7, 8 e 9	✓	✓
Debian 10 e 11	✓	✓
Rocky Linux 8 e 9	✓	✓
Ubuntu 20.04, 22.04 e 24.04	✓	✓
SUSE Linux Enterprise 15 SP2 e versioni successive	✓	✓
openSUSE Leap 15.5 e versioni successive	✓	

> **Note**
>
> Ubuntu 20.04 consente il supporto diretto peer quando viene utilizzato con istanze `dl1.24xlarge`.

Limitazioni di EFA

Gli EFA hanno le seguenti limitazioni:

- Tutti i tipi di istanza P4d e P5 supportano NVIDIA GPUDirect Remote Direct Memory Access (RDMA).
- Il traffico EFA tra istanze P4d/P4de/DL1 e altri tipi di istanze non è attualmente supportato.

- I tipi di istanza che supportano più schede di rete possono essere configurati con un EFA per scheda di rete. Tutti gli altri tipi di istanza supportati supportano solo un EFA per istanza.
- Per `c7g.16xlarge`, `m7g.16xlarge` e `r7g.16xlarge`, le istanze dedicate e gli host dedicati non sono supportati quando è collegato un EFA.
- Il traffico EFA OS-Bypass è limitato a una singola zona di disponibilità. In altre parole, il traffico EFA non può essere inviato da una zona di disponibilità all'altra. Il normale traffico IP proveniente dall'EFA può essere inviato da una zona di disponibilità a un'altra.
- Il traffico EFA di bypass del sistema operativo non è instradabile, mentre è sempre possibile instradare il normale traffico IP dall'EFA.
- L'EFA deve far parte di un gruppo di sicurezza in cui sia consentito tutto il traffico in entrata e in uscita dal gruppo stesso.
- EFA non è supportato sulle istanze Windows.
- EFA non è supportato su AWS Outposts.

Prezzi EFA

EFA è disponibile come funzionalità di rete Amazon EC2 opzionale che puoi abilitare su qualsiasi istanza supportata senza costi aggiuntivi.

Inizia a utilizzare le istanze P5 ed EFA

Le istanze P5 forniscono 3.200 Gbps di larghezza di banda della rete utilizzando più interfacce EFA. Le istanze P5 supportano 32 schede di rete. Per ulteriori informazioni sulle nozioni di base sulle istanze P5, consulta la pagina Inizia a usare le istanze P5 per Linux.

Consigliamo di definire una singola interfaccia di rete EFA per scheda di rete. Per configurare queste interfacce all'avvio, consigliamo le seguenti impostazioni:

- Per l'interfaccia di rete `0`, specifica l'indice del dispositivo `0`
- Per le interfacce di rete `1` attraverso `31`, specifica l'indice del dispositivo `1`

Se utilizzi la console Amazon EC2, nella procedura guidata di avvio dell'istanza, scegli Modifica nella sezione Impostazioni di rete. Espandi Configurazione di rete avanzata e scegli Aggiungi interfaccia di rete per aggiungere il numero richiesto di interfacce di rete. Per ogni interfaccia di rete, in EFA, seleziona Abilita. Per tutte le interfacce di rete, a eccezione di quella principale, per Indice del dispositivo, specifica 1. Configura le impostazioni rimanenti secondo necessità.

Se utilizzi il AWS CLI, usa il comando run-instances, for`--network-interfaces`, specifica il numero richiesto di interfacce di rete. Per ogni interfaccia di rete, in `InterfaceType`, specifica `efa`. Per l'interfaccia di rete principale, in `NetworkCardIndex` e `DeviceIndex` specifica `0`. Per le restanti interfacce di rete, in `NetworkCardIndex` specifica un valore univoco da `1` a `31` e in `DeviceIndex` specifica `1`.

Il seguente frammento di comando di esempio mostra una richiesta con 32 interfacce di rete EFA.

```
$ aws --region $REGION ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami_id \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
```

```
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
```

```
 "NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
...
```

Se utilizzi un modello di avvio, specifica il numero richiesto di interfacce di rete in tale modello. Per ogni interfaccia di rete, in `InterfaceType`, specifica `efa`. Per l'interfaccia di rete principale, in `NetworkCardIndex` e `DeviceIndex` specifica `0`. Per le restanti interfacce di rete, in `NetworkCardIndex` specifica un valore univoco da `1` a `31` e in `DeviceIndex` specifica `1`. Il seguente frammento mostra un esempio con 3 delle 32 possibili interfacce di rete.

```
"NetworkInterfaces":[
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
```

```
  "NetworkCardIndex": 1,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
}
...
```

Quando avvii un'istanza P5 con più di un'interfaccia di rete, non puoi assegnare automaticamente indirizzi IP pubblici. Tuttavia, è possibile collegare un indirizzo IP elastico all'interfaccia di rete principale (NetworkCardIndex=0, DeviceIndex =0) dopo l'avvio per la connettività Internet. Sia Ubuntu 20.04 e versioni successive che Amazon Linux 2 e versioni successive sono configurati per utilizzare l'interfaccia di rete principale per il traffico Internet quando l'istanza viene avviata come consigliato in precedenza.

Nozioni di base su EFA e MPI

Questo tutorial consente di avviare un EFA e un cluster dell'istanza abilitata all'MPI per i carichi di lavoro HPC. In questo tutorial procedi secondo la procedura descritta di seguito.

Indice

- Fase 7. Conferma dell'installazione
- Fase 8: installazione dell'applicazione HPC
- Fase 9: creazione di un'AMI abilitata per EFA
- Fase 10: avvio delle istanze abilitate per EFA in un gruppo di collocazione cluster
- Fase 11: terminare l'istanza temporanea
- Fase 12: abilitazione di SSH senza password

Fase 1: preparare un gruppo di sicurezza abilitato per EFA

Un EFA richiede un gruppo di sicurezza in cui sia consentito tutto il traffico in entrata e in uscita dal gruppo stesso. La procedura seguente crea un gruppo di sicurezza che consente tutto il traffico in entrata e in uscita da e verso se stesso e che consente il traffico SSH in entrata da qualsiasi indirizzo IPv4 per la connettività SSH.

> **Important**
>
> Questo gruppo di sicurezza è destinato esclusivamente a scopi di test. Per i tuoi ambienti di produzione, consigliamo di creare una regola SSH in entrata che consenta il traffico solo dall'indirizzo IP da cui ti connetti, ad esempio l'indirizzo IP del tuo computer o un intervallo di indirizzi IP nella tua rete locale.

Per altri scenari, consulta Regole del gruppo di sicurezza per diversi casi d'uso.

Per creare un gruppo di sicurezza abilitato per EFA

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Security Groups (Gruppi di sicurezza) e quindi Create Security Group (Crea gruppo di sicurezza).
3. Nella finestra Create Security Group (Crea gruppo di sicurezza) effettuare le operazioni seguenti:
   a. In Nome gruppo di sicurezza, immettere un nome descrittivo per il gruppo di sicurezza, ad esempio `EFA-enabled security group`.
   b. (Facoltativo) In Description (Descrizione), inserire una breve descrizione del gruppo di sicurezza.
   c. In VPC, selezionare il VPC in cui avviare le istanze abilitate per EFA.

   d. Scegliere Create Security Group (Crea gruppo di sicurezza).

4. Seleziona il gruppo di sicurezza creato e nella scheda Details (Dettagli) copia il valore Security group ID (ID gruppo di sicurezza).
5. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit inbound rules (Modifica le regole in entrata) ed esegui le operazioni di seguito:

   a. Scegliere Add rule (Aggiungi regola).
   b. In Type (Tipo), selezionare All traffic (Tutto il traffico).
   c. Per Source type (Tipo di origine), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.
   d. Scegli Aggiungi regola.
   e. Per Type (Tipo) scegli SSH.
   f. Per Source type (Tipo di origine), scegli Anywhere-IPv4 (Ovunque-IPv4).
   g. Scegliere Salva regole.
6. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit outbound rules (Modifica le regole in uscita) ed esegui le operazioni di seguito:

   a. Scegliere Add rule (Aggiungi regola).
   b. In Type (Tipo), selezionare All traffic (Tutto il traffico).
   c. Per Destination type (Tipo di destinazione), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.
   d. Scegliere Salva regole.

Fase 2: avviare un'istanza temporanea

Avvia un'istanza temporanea da utilizzare per installare e configurare i componenti software EFA. L'istanza serve anche per creare un'AMI abilitata per EFA da cui avviare le istanze abilitate per EFA.

Per avviare un'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.

3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=EFA-instance`).
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI per uno dei sistemi operativi supportati.
5. Nella sezione Instance type (Tipo di istanza), seleziona un tipo di istanza supportato.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:
   a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.
   b. Per Firewall (security groups) (Firewall [gruppi di sicurezza]), scegli Select existing security group (Seleziona gruppo di sicurezza esistente) e quindi seleziona il gruppo di sicurezza creato nella fase precedente.
   c. Espandi la sezione Advanced network configuration (Configurazione di rete avanzata) e per Elastic Fabric Adapter seleziona Enable (Abilita).
8. Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.
9. Nel pannello Summary (Riepilogo) a destra, scegli Launch instance (Avvia istanza).

> **Note**
>
> Prendi in considerazione la possibilità di richiedere l'uso di IMDSv2 per l'istanza temporanea e per l'AMI che creerai nel passaggio 9, a meno che tu non abbia già impostato IMDSv2 come predefinito per l'account. Per ulteriori informazioni sui passaggi di configurazione di IMDSv2, vedere. Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze

Fase 3: installare il software EFA

Installare il kernel abilitato EFA, i driver EFA, Libfabric e lo stack Open MPI necessari per supportare EFA sull'istanza temporanea.

Le fasi variano a seconda che si intenda utilizzare EFA con Open MPI, con Intel MPI o con Open MPI e Intel MPI..

Per installare il software EFA

1. Connettersi all'istanza avviata. Per ulteriori informazioni, consulta Connessione all'istanza di Linux.
2. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza. Questo processo può richiedere alcuni minuti.

   - Amazon Linux 2023, Amazon Linux 2, RHEL 7/8/9, CentOS 7, Rocky Linux 8/9

     ```
     $ sudo yum update -y
     ```

   - Ubuntu e Debian

     ```
     $ sudo apt-get update && sudo apt-get upgrade -y
     ```

   - SUSE Linux Enterprise

     ```
     $ sudo zypper update -y
     ```

3. Riavviare l'istanza e riconnettersi a essa.
4. Scarica i file di installazione del software. I file di installazione del software sono riuniti in un file (`.tar.gz`) tarball compresso. Per scaricare l'ultima versione stabile, utilizzare il comando seguente.

   ```
   $ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz
   ```

   È inoltre possibile ottenere l'ultima versione sostituendo il numero della versione con `latest` nel comando qui sopra.
5. (Opzionale) Verifica l'autenticità e l'integrità del file tarball EFA (`.tar.gz`).

   È consigliabile eseguire questa operazione per verificare l'identità dell'autore del software e che il file non sia stato alterato o danneggiato dopo la pubblicazione. Se non desideri verificare il file tarball, ignora questo passaggio.

   > **Note**
   >
   > In alternativa, se preferisci verificare il file tarball utilizzando un checksum MD5 o SHA256, consulta Verifica del programma di installazione EFA utilizzando un checksum.

a. Scarica la chiave pubblica GPG e importala nel tuo keyring.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

Il comando dovrebbe restituire un valore di chiave. Prendere nota del valore della chiave poiché sarà necessario nella fase successiva.

b. Verifica l'impronta digitale della chiave GPG. Esegui questo comando e specifica la chiave valore creata nella fase precedente.

```
$ gpg --fingerprint key_value
```

Il comando dovrebbe restituire un'impronta digitale identica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Se l'impronta digitale non corrisponde, non eseguire lo script di installazione EFA e contatta AWS Support.

c. Scarica il file di firma e verifica la firma del file tarball EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.33.0.tar.gz.sig
```

Di seguito viene mostrato l'output di esempio.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Se il risultato include `Good signature` e se l'impronta digitale corrisponde a quella restituita nel passaggio precedente, procedi alla fase successiva. In caso contrario, non eseguire lo script di installazione EFA e contatta AWS Support.

6. Estrarre i file dal file `.tar.gz` compresso e andare alla directory estratta.

```
$ C:\> tar -xf aws-efa-installer-1.33.0.tar.gz && cd aws-efa-installer
```

7. Installare il software EFA. Eseguire una delle seguenti operazioni, a seconda del caso d'uso:

> **Note**
>
> EFA non supporta NVIDIA GPUDirect con SUSE Linux. Se utilizzi SUSE Linux, devi specificare anche l'opzione `--skip-kmod` per impedire l'installazione di kmod. Per impostazione predefinita, SUSE Linux non consente i moduli del kernel. out-of-tree

Open MPI and Intel MPI

Se intendi utilizzare EFA con Open MPI e Intel MPI, devi installare il software EFA con Libfabric e Open MPI e completare la Fase 5: installare Intel MPI.

Per installare il software EFA con Libfabric e Open MPI, eseguire il seguente comando.

> **Note**
>
> A partire da EFA 1.30.0, per impostazione predefinita vengono installati sia Open MPI 4 che Open MPI 5. Facoltativamente, è possibile specificare la versione di Open MPI che si desidera installare. Per installare solo Open MPI 4, includere `--mpi=openmpi4`. Per installare solo Open MPI 5, includere `--mpi=openmpi5`. Per installare entrambi, omettere l'opzione `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

Libfabric è installato su `/opt/amazon/efa`. Open MPI 4 è installato su `/opt/amazon/openmpi`. Open MPI 5 è installato su `/opt/amazon/openmpi5`.

Open MPI only

Se intendi utilizzare EFA solo con Open MPI, devi installare il software EFA con Libfabric e Open MPI e puoi ignorare la Fase 5: installare Intel MPI. Per installare il software EFA con Libfabric e Open MPI, eseguire il seguente comando.

> **Note**
>
> A partire da EFA 1.30.0, per impostazione predefinita vengono installati sia Open MPI 4 che Open MPI 5. Facoltativamente, è possibile specificare la versione di

Open MPI che si desidera installare. Per installare solo Open MPI 4, includere `--mpi=openmpi4`. Per installare solo Open MPI 5, includere `--mpi=openmpi5`. Per installare entrambi, omettere l'opzione `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

Libfabric è installato su `/opt/amazon/efa`. Open MPI 4 è installato su `/opt/amazon/openmpi`. Open MPI 5 è installato su `/opt/amazon/openmpi5`.

Intel MPI only

Se si intende utilizzare solo EFA con Intel MPI, è possibile installare il software EFA senza Libfabric e Open MPI. In tal caso, Intel MPI utilizza Libfabric incorporato. Se si sceglie di eseguire questa operazione, è necessario completare la Fase 5: installare Intel MPI.

Per installare il software EFA senza Libfabric e Open MPI, eseguire il seguente comando.

```
$ sudo ./efa_installer.sh -y --minimal
```

8. Se il programma di installazione di EFA richiede il riavvio dell'istanza, eseguire questa operazione e riconnettersi all'istanza. In caso contrario, disconnettersi dall'istanza e quindi accedere di nuovo per completare l'installazione.

Fase 4: (facoltativa) abilitare Open MPI 5

> **Note**
>
> Esegui questa fase solo se intendi utilizzare Open MPI 5.

A partire da EFA 1.30.0, per impostazione predefinita vengono installati sia Open MPI 4 che Open MPI 5. In alternativa, puoi scegliere di installare solo Open MPI 4 oppure Open MPI 5.

Se scegli di installare Open MPI 5 nella Fase 3: installare il software EFA e desideri utilizzarlo, devi eseguire questa procedura per abilitarlo.

Abilitazione di Open MPI 5

1. Aggiungi Open MPI 5 alla variabile di ambiente PATH.

   ```
   $ module load openmpi5
   ```

2. Verifica che Open MPI 5 sia abilitato per l'uso.

   ```
   $ which mpicc
   ```

   Il comando dovrebbe restituire la directory di installazione di Open MPI 5: `/opt/amazon/openmpi5`.

3. (Facoltativo) Per garantire che Open MPI 5 venga aggiunto alla variabile di ambiente PATH a ogni avvio dell'istanza, esegui le seguenti operazioni:

   bash shell

   Aggiungi `module load openmpi5` a `/home/`*`username`*`/.bashrc` e `/home/`*`username`*`/.bash_profile`.

   csh and tcsh shells

   Aggiungere `module load openmpi5` a `/home/`*`username`*`/.cshrc`.

Se è necessario rimuovere Open MPI 5 dalla variabile di ambiente PATH, esegui il seguente comando e rimuovilo dagli script shell di avvio.

```
$ module unload openmpi5
```

Fase 5 (facoltativa): installare Intel MPI

> **Important**
>
> Esegui questa fase solo se intendi utilizzare Intel MPI. Se intendi utilizzare Open MPI, salta questa fase.

Intel MPI richiede un'installazione aggiuntiva e la configurazione di una variabile d'ambiente.

Prerequisito

Verificare che l'utente che esegue le fasi seguenti disponga delle autorizzazioni sudo.

Per installare Intel MPI

1. Per scaricare lo script di installazione Intel MPI, procedi come indicato di seguito

   a. Visita il sito Web Intel.

   b. Nella sezione Intel MPI Library (Libreria Intel MPI) della pagina Web, scegli il collegamento per il programma di installazione offline della Libreria Intel MPI per Linux.

2. Esegui lo script di installazione scaricato nel passaggio precedente.

   ```
   $ sudo bash installation_script_name.sh
   ```

3. Nel programma di installazione, scegli Accetta e installa.

4. Leggi il programma Intel Improvement, scegli l'opzione appropriata, quindi scegli Begin Installation (Inizia l'installazione).

5. Al termine dell'installazione, scegliere Chiudi.

6. Per impostazione predefinita, Intel MPI utilizza il proprio Libfabric incorporato (interno). Puoi tuttavia configurare Intel MPI per utilizzare il componente Libfabric fornito con il programma di installazione EFA. In genere, il programma di installazione EFA viene fornito con una versione successiva di Libfabric rispetto a Intel MPI. In alcuni casi, il componente Libfabric fornito con il programma di installazione EFA è anche più performante di quello di Intel MPI. Per configurare Intel MPI per l'utilizzo del componente Libfabric fornito con il programma di installazione EFA, esegui una delle operazioni seguenti, in base alla shell in uso.

   bash shells

   Aggiungi l'istruzione seguente a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   export I_MPI_OFI_LIBRARY_INTERNAL=0
   ```

   csh and tcsh shells

   Aggiungi l'istruzione seguente a /home/*username*/.cshrc.

   ```
   setenv I_MPI_OFI_LIBRARY_INTERNAL 0
   ```

7. Aggiungi il comando di origine seguente allo script della shell per generare lo script `vars.sh` dalla directory di installazione e impostare l'ambiente del compilatore ad ogni avvio dell'istanza. Eseguire uno dei seguenti, a seconda della regione in uso:

   bash shells

   Aggiungi l'istruzione seguente a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.sh
   ```

   csh and tcsh shells

   Aggiungi l'istruzione seguente a /home/*username*/.cshrc.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.csh
   ```

8. Se EFA non è disponibile a causa di una configurazione errata, Intel MPI utilizza per impostazione predefinita lo stack di rete TCP/IP, il che potrebbe comportare un rallentamento delle prestazioni dell'applicazione. Per evitare questo comportamento, imposta `I_MPI_OFI_PROVIDER` su `efa`. Se EFA non è disponibile, Intel MPI mostra l'errore seguente:

   ```
   Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
    error,
   MPIR_Init_thread (XXX).......:
   MPID_Init (XXXX).............:
   MPIDI_OFI_mpi_init_hook (XXXX):
   open_fabric (XXXX)...........:
   find_provider (XXXX).........:
   OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
   ```

   Eseguire uno dei seguenti, a seconda della regione in uso:

   bash shells

   Aggiungi l'istruzione seguente a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   export I_MPI_OFI_PROVIDER=efa
   ```

csh and tcsh shells

Aggiungi l'istruzione seguente a /home/*username*/.cshrc.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. Per impostazione predefinita, Intel MPI non stampa le informazioni di debug. Per controllare tali informazioni, puoi specificare livelli di verbosità diversi. I valori possibili (secondo la quantità di dettagli che forniscono) sono: `0` (impostazione predefinita), `1`, `2`, `3`, `4`, `5`. Il livello `1` e i livelli superiori stampano `libfabric version` e `libfabric provider`. Utilizza `libfabric version` per verificare se Intel MPI sta usando il componente Libfabric interno o quello fornito con il programma di installazione EFA. Se sta usando il componente Libfabric interno, la versione presenta il suffisso `impi`. Utilizza `libfabric provider` per verificare se Intel MPI sta usando EFA o la rete TCP/IP. Se utilizza EFA, il valore è `efa`. Se utilizza la rete TCP/IP, il valore è `tcp;ofi_rxm`.

   Per abilitare le informazioni di debug, esegui una delle operazioni seguenti, in base alla shell in uso.

   bash shells

   Aggiungi l'istruzione seguente a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   export I_MPI_DEBUG=value
   ```

   csh and tcsh shells

   Aggiungi l'istruzione seguente a /home/*username*/.cshrc.

   ```
   setenv I_MPI_DEBUG value
   ```

10. Per impostazione predefinita, Intel MPI utilizza la memoria condivisa del sistema operativo (`shm`) per le comunicazioni intranodo e Libfabric (`ofi`) per le comunicazioni internodo. In generale, questa configurazione offre le prestazioni migliori. In alcuni casi, tuttavia, il fabric shm Intel MPI può causare il blocco di alcune applicazioni a tempo indeterminato.

Per risolvere questo problema, puoi forzare Intel MPI a utilizzare Libfabric sia per le comunicazioni intranodo che per quelle internodo. A tal scopo, esegui una delle operazioni seguenti, in base alla shell in uso.

bash shells

Aggiungi l'istruzione seguente a `/home/username/.bashrc` e `/home/username/.bash_profile`.

```
export I_MPI_FABRICS=ofi
```

csh and tcsh shells

Aggiungi l'istruzione seguente a `/home/username/.cshrc`.

```
setenv I_MPI_FABRICS ofi
```

> **Note**
>
> Il provider Libfabric di EFA utilizza la memoria condivisa del sistema operativo per le comunicazioni intranodo. Ciò significa che impostando `I_MPI_FABRICS` su `ofi` si ottengono prestazioni simili a quelle della configurazione `shm:ofi` predefinita.

11. Disconnettersi e quindi riconnettersi all'istanza.

Se non si desidera più utilizzare Intel MPI, rimuovere le variabili di ambiente dagli script shell di startup.

Fase 6: disabilitare la protezione Ptrace

Per migliorare le prestazioni dell'applicazione HPC, Libfabric utilizza la memoria locale dell'istanza per le comunicazioni tra processi quando i processi sono in esecuzione sulla stessa istanza.

La funzione di memoria condivisa utilizza Cross Memory Attach (CMA), che non è supportato con la protezione ptrace. Se si utilizza una distribuzione Linux con protezione ptrace abilitata per impostazione predefinita, come Ubuntu, è necessario disabilitarla. Se la tua distribuzione Linux non ha la protezione ptrace abilitata per impostazione predefinita, ignorare questo passaggio.

Per disabilitare la protezione ptrace

Scegliere una delle seguenti operazioni:

- Per disabilitare temporaneamente la protezione ptrace a scopo di test, esegui il comando seguente.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Per disabilitare in modo permanente la protezione ptrace, aggiungere `kernel.yama.ptrace_scope = 0` a `/etc/sysctl.d/10-ptrace.conf` e riavviare l'istanza.

Fase 7. Conferma dell'installazione

Verifica della corretta installazione

1. Per verificare che MPI sia stato correttamente installato, esegui il comando seguente:

   ```
   $ which mpicc
   ```

   - Per Open MPI, il percorso restituito deve includere `/opt/amazon/`.
   - Per Intel MPI, il percorso restituito deve includere `/opt/intel/`. Se non ottieni l'output previsto, assicurati di aver fornito lo script `vars.sh` di Intel MPI.
2. Per confermare che i componenti software EFA e Libfabric siano stati installati correttamente, emetti il comando seguente.

   ```
   $ fi_info -p efa -t FI_EP_RDM
   ```

   Il comando deve restituire informazioni sulle interfacce EFA Libfabric. L'esempio seguente mostra l'output del comando.

   ```
   provider: efa
       fabric: EFA-fe80::94:3dff:fe89:1b70
       domain: efa_0-rdm
       version: 2.0
       type: FI_EP_RDM
       protocol: FI_PROTO_EFA
   ```

Fase 8: installazione dell'applicazione HPC

Installa l'applicazione HPC sull'istanza temporanea. La procedura di installazione varia in base alla specifica applicazione HPC. Per ulteriori informazioni, consulta Gestisci il software sulla tua istanza AL2 nella Guida per l'utente di Amazon Linux 2.

> **Note**
>
> Per le istruzioni di installazione, consulta la documentazione dell'applicazione HPC.

Fase 9: creazione di un'AMI abilitata per EFA

Dopo aver installato i componenti software necessari, procedi con la creazione di un'AMI che puoi riutilizzare per avviare le istanze abilitate per EFA.

Per creare un'AMI dall'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona l'istanza temporanea creata e seleziona Actions (Operazioni), Image (Immagine), Create Image (Crea immagine).
4. Per Create image (Crea immagine), effettua le seguenti operazioni:
   a. In Image name (Nome immagine), immettere un nome descrittivo per l'AMI.
   b. (Facoltativo) In Image description (Descrizione immagine), inserire una breve descrizione dell'AMI.
   c. Scegliere Create Image (Crea immagine).
5. Nel riquadro di navigazione scegliere AMIs (AMI).
6. Individuare nell'elenco l'AMI creata. Prima di procedere con la fase seguente, attendi che lo stato passi da `pending` a `available`.

Fase 10: avvio delle istanze abilitate per EFA in un gruppo di collocazione cluster

Avvia le istanze abilitate per EFA in un gruppo di collocazione cluster tramite l'AMI abilitata per EFA creata nella Fase 7 e il gruppo di sicurezza abilitato per EFA creato nella Fase 1.

> **Note**
>
> - Avviare le istanze abilitate per l'EFA in un gruppo di collocazione cluster non è un requisito in assoluto. È tuttavia consigliabile eseguire le istanze abilitate per EFA in un gruppo di collocazione cluster perché le istanze vengono così avviate in gruppo a bassa latenza in un'unica zona di disponibilità.
> - Per garantire che la capacità sia disponibile durante il dimensionamento delle istanze del cluster, è possibile creare una prenotazione della capacità per il gruppo di collocazione cluster. Per ulteriori informazioni, consulta Le Prenotazioni della capacità in gruppi di collocazione cluster..

Per avviare un'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.
3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=`*`EFA-instance`*).
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), scegli My AMIs (Le mie AMI), quindi seleziona l'AMI creata nella fase precedente.
5. Nella sezione Instance type (Tipo di istanza), seleziona un tipo di istanza supportato.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:
   a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.
   b. Per Firewall (security groups) (Firewall [gruppi di sicurezza]), scegli Select existing security group (Seleziona gruppo di sicurezza esistente) e quindi seleziona il gruppo di sicurezza creato nella fase precedente.
   c. Espandi la sezione Advanced network configuration (Configurazione di rete avanzata) e per Elastic Fabric Adapter seleziona Enable (Abilita).
8. (Opzionale) Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.

9. Nella sezione Advanced details (Dettagli avanzati), per Placement group name (Nome del gruppo di collocazione), seleziona il gruppo di collocazione cluster in cui avviare le istanze. Se occorre creare un nuovo gruppo di collocazione cluster, scegli Create new placement group (Crea nuovo gruppo di collocazione).
10. Nel pannello Summary (Riepilogo) a destra, per Number of instances (Numero di istanze), inserisci il numero di istanze abilitate per EFA che desideri avviare, quindi seleziona Launch instance (Avvia istanza).

Fase 11: terminare l'istanza temporanea

A questo punto, non è più necessaria l'istanza lanciata nella fase 2. È possibile terminare l'istanza per evitare di incorrere in costi aggiuntivi.

Per terminare l'istanza temporanea

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza temporanea creata, quindi scegliere Actions (Operazioni), Instance state (Stato istanza), Terminate instance (Termina istanza).
4. Quando viene richiesta la conferma, seleziona Termina.

Fase 12: abilitazione di SSH senza password

Per consentire l'esecuzione delle applicazioni in tutte le istanze del cluster, è necessario abilitare l'accesso SSH senza password dal nodo leader ai nodi membro. Il nodo principale è l'istanza da cui vengono eseguite le applicazioni. Le restanti istanze del cluster sono i nodi membro.

Per abilitare SSH senza password tra le istanze del cluster

1. Selezionare un'istanza nel cluster come nodo principale e connettersi a essa.
2. Disabilita `strictHostKeyChecking` e abilita `ForwardAgent` sul nodo principale. Aprire il file `~/.ssh/config` utilizzando qualsiasi editor di testo e aggiungere il seguente script.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Generare una coppia di chiavi RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

   La coppia di chiavi viene creata nella directory `$HOME/.ssh/`.

4. Modifica le autorizzazioni della chiave privata sul nodo principale.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Aprire `~/.ssh/id_rsa.pub` utilizzando l'editor di testo preferito e copiare la chiave.
6. Per ogni nodo membro nel cluster, procedere nel modo seguente:

   a. Collegarsi all'istanza.

   b. Aprire `~/.ssh/authorized_keys` utilizzando qualsiasi editor di testo e aggiungere la chiave pubblica copiata in precedenza.

7. Per verificare che SSH senza password funzioni come previsto, connettersi al nodo leader ed eseguire il seguente comando.

```
$ ssh member_node_private_ip
```

   La connessione al nodo membro non dovrebbe richiedere una chiave o una password.

Nozioni di base su EFA e NCCL

NVIDIA Collective Communications Library (NCCL) è una libreria di routine di comunicazione collettive standard per più GPU su un singolo nodo o su più nodi. NCCL può essere utilizzato con EFA, Libfabric e MPI per supportare diversi carichi di lavoro di machine learning. Per ulteriori informazioni, consulta il sito Web NCCL.

I passaggi seguenti consentono di iniziare a utilizzare EFA e NCCL utilizzando un'AMI di base per uno dei sistemi operativi supportati.

> **Note**
>
> - Solo i tipi di istanza `p3dn.24xlarge`, `p4d.24xlargee` `p5.48xlarge` sono supportati.
> - Sono supportate solo le AMI di base Amazon Linux 2 e Ubuntu 20.04/22.04.

- Solo NCCL 2.4.2 e versione successiva è supportata da EFA.
- Per ulteriori informazioni sull'esecuzione di carichi di lavoro di machine learning con EFA e NCCL utilizzando un AWS Deep Learning AMI, consulta Using EFA on the DLAMI nella Developer Guide.AWS Deep Learning AMI

Fasi

Fase 1: preparare un gruppo di sicurezza abilitato per EFA

Un EFA richiede un gruppo di sicurezza in cui sia consentito tutto il traffico in entrata e in uscita dal gruppo stesso. La procedura seguente crea un gruppo di sicurezza che consente tutto il traffico in entrata e in uscita da e verso se stesso e che consente il traffico SSH in entrata da qualsiasi indirizzo IPv4 per la connettività SSH.

Important

Questo gruppo di sicurezza è destinato esclusivamente a scopi di test. Per i tuoi ambienti di produzione, consigliamo di creare una regola SSH in entrata che consenta il traffico solo

dall'indirizzo IP da cui ti connetti, ad esempio l'indirizzo IP del tuo computer o un intervallo di indirizzi IP nella tua rete locale.

Per altri scenari, consulta Regole del gruppo di sicurezza per diversi casi d'uso.

Per creare un gruppo di sicurezza abilitato per EFA

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Security Groups (Gruppi di sicurezza) e quindi Create Security Group (Crea gruppo di sicurezza).
3. Nella finestra Create Security Group (Crea gruppo di sicurezza) effettuare le operazioni seguenti:
   a. In Nome gruppo di sicurezza, immettere un nome descrittivo per il gruppo di sicurezza, ad esempio `EFA-enabled security group`.
   b. (Facoltativo) In Description (Descrizione), inserire una breve descrizione del gruppo di sicurezza.
   c. In VPC, selezionare il VPC in cui avviare le istanze abilitate per EFA.
   d. Scegliere Create Security Group (Crea gruppo di sicurezza).
4. Seleziona il gruppo di sicurezza creato e nella scheda Details (Dettagli) copia il valore Security group ID (ID gruppo di sicurezza).
5. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit inbound rules (Modifica le regole in entrata) ed esegui le operazioni di seguito:
   a. Scegliere Add rule (Aggiungi regola).
   b. In Type (Tipo), selezionare All traffic (Tutto il traffico).
   c. Per Source type (Tipo di origine), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.
   d. Scegli Aggiungi regola.
   e. Per Type (Tipo) scegli SSH.
   f. Per Source type (Tipo di origine), scegli Anywhere-IPv4 (Ovunque-IPv4).
   g. Scegliere Salva regole.
6. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit outbound rules (Modifica le regole in uscita) ed esegui le operazioni di seguito:

a. Scegliere Add rule (Aggiungi regola).

b. In Type (Tipo), selezionare All traffic (Tutto il traffico).

c. Per Destination type (Tipo di destinazione), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.

d. Scegliere Salva regole.

Fase 2: avviare un'istanza temporanea

Avvia un'istanza temporanea da utilizzare per installare e configurare i componenti software EFA. L'istanza serve anche per creare un'AMI abilitata per EFA da cui avviare le istanze abilitate per EFA.

Per avviare un'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.
3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=`*`EFA-instance`*).
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI per uno dei sistemi operativi supportati. Sono supportati solo Amazon Linux 2, Ubuntu 20.04 e Ubuntu 22.04.
5. Nella sezione Tipo di istanza seleziona `p3dn.24xlarge`, `p4d.24xlarge` o `p5.48xlarge`.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:

   a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.

   b. Per Firewall (security groups) (Firewall [gruppi di sicurezza]), scegli Select existing security group (Seleziona gruppo di sicurezza esistente) e quindi seleziona il gruppo di sicurezza creato nella fase precedente.

   c. Espandi la sezione Advanced network configuration (Configurazione di rete avanzata) e per Elastic Fabric Adapter seleziona Enable (Abilita).

8. Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.

> **Note**
>
> Devi effettuare un provisioning aggiuntivo di 10-20 GiB di spazio di archiviazione per Nvidia CUDA Toolkit. Se non effettui il provisioning di uno spazio di archiviazione sufficiente, riceverai un errore `insufficient disk space` durante il tentativo di installare i driver Nvidia e il toolkit CUDA.

9. Nel pannello Summary (Riepilogo) a destra, scegli Launch instance (Avvia istanza).

Fase 3: installare driver GPU Nvidia, il kit di strumenti Nvidia CUDA e cuDNN

Amazon Linux 2

Per installare driver GPU Nvidia, il kit di strumenti Nvidia CUDA e cuDNN

1. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza.

```
$ sudo yum upgrade -y && sudo reboot
```

   Dopo il riavvio, riconnettersi all'istanza.

2. Installare le utilità che sono richieste per installare i driver GPU Nvidia e il toolkit CUDA Nvidia.

```
$ sudo yum groupinstall 'Development Tools' -y
```

3. Disabilitare i driver open source `nouveau`.

   a. Installare le utility richieste e il pacchetto delle intestazioni kernel per la versione del kernel attualmente in esecuzione.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

   b. Aggiungere `nouveau` al file dell'elenco dei `/etc/modprobe.d/blacklist.conf` negati.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Aggiungere `GRUB_CMDLINE_LINUX="rdblacklist=nouveau"` al file `grub` e ricompilare il file di configurazione di Grub.

```
$ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
default/grub \
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Riavviare l'istanza e riconnettersi a essa.
5. Preparare i repository richiesti

a. Installare il repository EPEL per DKMS e abilitare qualsiasi repository opzionale per la distribuzione Linux.

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
```

b. Installare la chiave GPG pubblica del repository CUDA.

```
$ distribution='rhel7'
```

c. Impostare il repository di rete CUDA e aggiornare la cache del repository.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

d. (Solo kernel versione 5.10) Eseguire questi passaggi solo se si utilizza Amazon Linux 2 con kernel versione 5.10. Se si utilizza Amazon Linux 2 con kernel versione 4.12, saltare questi passaggi. Per controllare la versione del kernel, eseguire uname -r.

i. Creare il file di configurazione del driver Nvidia denominato `/etc/dkms/nvidia.conf`.

```
$ sudo mkdir -p /etc/dkms \
&& echo "MAKE[0]=\"'make' -j2 module SYSSRC=\${kernel_source_dir}
 IGNORE_XEN_PRESENCE=1 IGNORE_PREEMPT_RT_PRESENCE=1 IGNORE_CC_MISMATCH=1
 CC=/usr/bin/gcc10-gcc\"" | sudo tee /etc/dkms/nvidia.conf
```

ii. (Solo `p4d.24xlarge` e `p5.48xlarge`) Copia il file di configurazione del driver Nvidia.

```
$ sudo cp /etc/dkms/nvidia.conf /etc/dkms/nvidia-open.conf
```

6. Installare i driver GPU Nvidia, il toolkit NVIDIA CUDA e cuDNN.

   - `p3dn.24xlarge`

   ```
   $ sudo yum clean all \
   && sudo yum -y install kmod-nvidia-latest-dkms nvidia-driver-latest-dkms \
   && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
   ```

   - `p4d.24xlarge` e `p5.48xlarge`

   ```
   $ sudo yum clean all \
   && sudo yum -y install kmod-nvidia-open-dkms nvidia-driver-latest-dkms \
   && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
   ```

7. Riavviare l'istanza e riconnettersi a essa.

8. (Solo `p4d.24xlarge` e `p5.48xlarge`) Avviare il servizio Nvidia Fabric Manager e assicurarsi che venga avviato automaticamente all'avvio dell'istanza. Nvidia Fabric Manager è necessario per la gestione degli switch NV.

   ```
   $ sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
   fabricmanager
   ```

9. Assicurarsi che i percorsi CUDA siano impostati ogni volta che viene avviata l'istanza.

   - Per le shell bash, aggiungere le seguenti istruzioni a /home/*username*/`.bashrc` e /home/*username*/`.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Per le shell tcsh, aggiungere le seguenti istruzioni a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

10. Per confermare che i driver GPU di Nvidia GPU siano funzionanti, eseguire questo comando.

```
$ nvidia-smi -q | head
```

Il comando deve restituire le informazioni sulle GPU Nvidia, sui driver GPU Nvidia e su Nvidia CUDA toolkit.

Ubuntu 20.04/22.04

Per installare driver GPU Nvidia, il kit di strumenti Nvidia CUDA e cuDNN

1. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza.

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

2. Installare le utilità che sono richieste per installare i driver GPU Nvidia e il toolkit CUDA Nvidia.

```
$ sudo apt-get update && sudo apt-get install build-essential -y
```

3. Per utilizzare il driver GPU Nvidia, è necessario prima disabilitare i driver open source nouveau.

   a. Installare le utility richieste e il pacchetto delle intestazioni kernel per la versione del kernel attualmente in esecuzione.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

b. Aggiungere nouveau al file dell'elenco dei /etc/modprobe.d/blacklist.conf negati.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Aprire il file /etc/default/grub utilizzando qualsiasi editor di testo e aggiungere il seguente script.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Ricompilare il file di configurazione di Grub.

```
$ sudo update-grub
```

4. Riavviare l'istanza e riconnettersi a essa.
5. Aggiungere il repository CUDA e installare i driver GPU Nvidia, il toolkit NVIDIA CUDA e cuDNN.

   • p3dn.24xlarge

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
```

```
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

- `p4d.24xlarge` e `p5.48xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-kernel-open-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Riavviare l'istanza e riconnettersi a essa.
7. (Solo `p4d.24xlarge` e `p5.48xlarge`) Installare Nvidia Fabric Manager.

   a. È necessario installare la versione di Nvidia Fabric Manager che corrisponde alla versione del modulo del kernel Nvidia installata al passaggio precedente.

      Eseguire questo comando per determinare la versione del modulo del kernel Nvidia.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

      Di seguito è riportato un output di esempio.

      ```
      NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15
       21:26:37 UTC 2021
      ```

      Nell'esempio precedente, è stata installata la versione principale `450` del modulo del kernel. Ciò significa che è necessario installare la versione `450` di Nvidia Fabric Manager.

b. Installare Nvidia Fabric Manager. Eseguire questo comando e specificare la versione principale identificata nella fase precedente.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-major_version_number
```

Ad esempio, se è stata installata la versione principale 450 del modulo del kernel, utilizzare il seguente comando per installare la versione corrispondente di Nvidia Fabric Manager.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-450
```

c. Avviare il servizio e assicurarsi che venga avviato automaticamente all'avvio dell'istanza. Nvidia Fabric Manager è necessario per la gestione degli switch NV.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Assicurarsi che i percorsi CUDA siano impostati ogni volta che viene avviata l'istanza.

- Per le shell bash, aggiungere le seguenti istruzioni a /home/*username*/.bashrc e /home/*username*/.bash_profile.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Per le shell tcsh, aggiungere le seguenti istruzioni a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Per confermare che i driver GPU di Nvidia GPU siano funzionanti, eseguire questo comando.

```
$ nvidia-smi -q | head
```

Il comando deve restituire le informazioni sulle GPU Nvidia, sui driver GPU Nvidia e su Nvidia CUDA toolkit.

Fase 4: installazione del GDRCopy

Installa GDRCopy per migliorare le prestazioni di Libfabric. Per ulteriori informazioni su GDRCopy, consulta il repository GDRCopy.

Amazon Linux 2

Installazione del GDRCopy

1. Installare le dipendenze richieste.

```
$ sudo yum -y install dkms rpm-build make check check-devel subunit subunit-
devel
```

2. Scarica ed estrai il pacchetto GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz ; cd gdrcopy-2.4/packages
```

3. Crea il pacchetto RPM GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Installa il pacchetto RPM GDRCopy.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.4-1dkms.noarch*.rpm \
&& sudo rpm -Uvh gdrcopy-2.4-1.x86_64*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.4-1.noarch*.rpm
```

Ubuntu 20.04/22.04

Installazione del GDRCopy

1. Installare le dipendenze richieste.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Scarica ed estrai il pacchetto GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
```

```
&& tar xf v2.4.tar.gz \
&& cd gdrcopy-2.4/packages
```

3. Crea il pacchetto RPM GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Installa il pacchetto RPM GDRCopy.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

Fase 5: installazione del software EFA

Installa il kernel abilitato EFA, i driver EFA, Libfabric e lo stack Open MPI necessari per supportare EFA sull'istanza temporanea.

Per installare il software EFA

1. Connettersi all'istanza avviata. Per ulteriori informazioni, consulta Connessione all'istanza di Linux.
2. Scarica i file di installazione del software. I file di installazione del software sono riuniti in un file (`.tar.gz`) tarball compresso. Per scaricare l'ultima versione stabile, utilizzare il comando seguente.

   ```
   $ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz
   ```

   È inoltre possibile ottenere l'ultima versione sostituendo il numero della versione con `latest` nel comando qui sopra.
3. (Opzionale) Verifica l'autenticità e l'integrità del file tarball EFA (`.tar.gz`).

   È consigliabile eseguire questa operazione per verificare l'identità dell'autore del software e che il file non sia stato alterato o danneggiato dopo la pubblicazione. Se non desideri verificare il file tarball, ignora questo passaggio.

> **Note**
>
> In alternativa, se preferisci verificare il file tarball utilizzando un checksum MD5 o SHA256, consulta Verifica del programma di installazione EFA utilizzando un checksum.

a. Scarica la chiave pubblica GPG e importala nel tuo keyring.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

Il comando dovrebbe restituire un valore di chiave. Prendere nota del valore della chiave poiché sarà necessario nella fase successiva.

b. Verifica l'impronta digitale della chiave GPG. Esegui questo comando e specifica la chiave valore creata nella fase precedente.

```
$ gpg --fingerprint key_value
```

Il comando dovrebbe restituire un'impronta digitale identica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Se l'impronta digitale non corrisponde, non eseguire lo script di installazione EFA e contatta AWS Support.

c. Scarica il file di firma e verifica la firma del file tarball EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.33.0.tar.gz.sig
```

Di seguito viene mostrato l'output di esempio.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Se il risultato include `Good signature` e se l'impronta digitale corrisponde a quella restituita nel passaggio precedente, procedi alla fase successiva. In caso contrario, non eseguire lo script di installazione EFA e contatta AWS Support.

4. Estrarre i file dal file `.tar.gz` compresso e andare alla directory estratta.

```
$ C:\> tar -xf aws-efa-installer-1.33.0.tar.gz && cd aws-efa-installer
```

5. Eseguire lo script di installazione del software EFA.

> **Note**
>
> A partire da EFA 1.30.0, per impostazione predefinita vengono installati sia Open MPI 4 che Open MPI 5. A meno che non sia necessario Open MPI 5, consigliamo di installare solo Open MPI 4. Il seguente comando installa solo Open MPI 4. Se si desidera installare sia Open MPI 4 che Open MPI 5, rimuovere `--mpi=openmpi4`.

```
$ sudo ./efa_installer.sh -y --mpi=openmpi4
```

Libfabric è installato nella directory `/opt/amazon/efa`, mentre Open MPI è installato nella directory `/opt/amazon/openmpi`.

6. Se il programma di installazione di EFA richiede il riavvio dell'istanza, eseguire questa operazione e riconnettersi all'istanza. In caso contrario, disconnettersi dall'istanza e quindi accedere di nuovo per completare l'installazione.
7. Verificare la corretta installazione dei componenti software EFA.

```
$ fi_info -p efa -t FI_EP_RDM
```

Il comando deve restituire informazioni sulle interfacce EFA Libfabric. L'esempio seguente mostra l'output del comando.

- `p3dn.24xlarge` con interfaccia di rete singola

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-rdm
version: 2.0
```

```
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` e `p5.48xlarge` con più interfacce di rete

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Fase 6: installare NCCL

Installare NCCL. Per ulteriori informazioni su NCCL, consulta il repository NCCL.

Per installare NCCL

1. Passa alla directory `/opt`.

```
$ cd /opt
```

2. Clonare il repository NCCL ufficiale sull'istanza e navigare nel repository clonato locale.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git && cd nccl
```

3. Creare e installare NCCL e specificare la directory di installazione CUDA.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

Passaggio 7: installa il plugin aws-ofi-nccl

Il aws-ofi-nccl plugin mappa le API di trasporto orientate alla connessione di NCCL all'interfaccia affidabile senza connessione di Libfabric. Ciò consente di utilizzare Libfabric come provider di rete mentre si eseguono applicazioni basate su NCCL. Per ulteriori informazioni sul plugin, consulta il repository. aws-ofi-nccl aws-ofi-nccl

Per installare il plugin aws-ofi-nccl

1. Passare alla home directory.

```
$ cd $HOME
```

2. Installa le utilità richieste.

   - Amazon Linux 2

   ```
   $ sudo yum install hwloc-devel
   ```

   - Ubuntu

   ```
   $ sudo apt-get install libhwloc-dev
   ```

3. Scarica i file del aws-ofi-nccl plugin. I file sono riuniti in un file tarball compresso (`.tar.gz`).

```
$ wget https://github.com/aws/aws-ofi-nccl/releases/download/v1.9.2-aws/aws-ofi-
nccl-1.9.2-aws.tar.gz
```

4. Estrai i file dal file .tar.gz compresso e vai alla directory estratta.

```
$ tar -xf aws-ofi-nccl-1.9.2-aws.tar.gz && cd aws-ofi-nccl-1.9.2-aws
```

5. Per generare i file make, eseguire lo script `configure` e specificare le directory di installazione MPI, Libfabric, NCCL e CUDA.

```
$ ./configure --prefix=/opt/aws-ofi-nccl --with-mpi=/opt/amazon/openmpi \
--with-libfabric=/opt/amazon/efa \
--with-cuda=/usr/local/cuda \
--enable-platform-aws
```

6. Aggiungi la directory Open MPI alla variabile `PATH`.

```
$ export PATH=/opt/amazon/openmpi/bin/:$PATH
```

7. Installa il aws-ofi-nccl plugin.

```
$ make && sudo make install
```

Fase 8: installare i test NCCL

Installare i test NCCL. I test NCCL consentono di confermare che NCCL sia installato correttamente e che funzioni come previsto. Per ulteriori informazioni sui test NCCL, consulta il repository nccl-tests.

Per installare i test NCCL

1. Passare alla home directory.

```
$ cd $HOME
```

2. Clonare il repository nccl-tests ufficiale sull'istanza e navigare nel repository clonato locale.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Aggiungere la directory Libfabric alla variabile `LD_LIBRARY_PATH`.

   - Amazon Linux 2

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
```

   - Ubuntu

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
```

4. Installare i test NCCL e specificare le directory di installazione MPI, NCCL e CUDA.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/
local/cuda
```

Fase 9: test della configurazione EFA e NCCL

Eseguire un test per accertare che l'istanza temporanea sia configurata adeguatamente per EFA e NCCL.

Per testare la configurazione EFA ed NCCL

1. Creare un file host che specifichi gli host su cui eseguire i test. Il comando seguente crea un file di host denominato `my-hosts` che include un riferimento all'istanza stessa.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
   hosts
   ```

2. Eseguire il test e specificare il file host (`--hostfile`) e il numero di GPU per utilizzare (`-n`). Il comando seguente effettua il test `all_reduce_perf` su GPU 8 sull'istanza stessa e specifica le variabili d'ambiente seguenti.

   - `FI_EFA_USE_DEVICE_RDMA=1`: (solo `p4d.24xlarge`) utilizza la funzionalità RDMA del dispositivo per il trasferimento unilaterale e bilaterale.
   - `NCCL_DEBUG=INFO`: consente un output di debug dettagliato. È possibile inoltre specificare `VERSION` per stampare solo la versione NCCL all'inizio del test o `WARN` per ricevere solo i messaggi di errore.

Per ulteriori informazioni sugli argomenti di test NCCL, consulta README Test NCCL nel repository ufficiale nccl-tests.

- `p3dn.24xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
 none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- `p4d.24xlarge` e `p5.48xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
-x FI_EFA_USE_DEVICE_RDMA=1 \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
 none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. È possibile confermare che EFA sia attivo come provider sottostante per NCCL quando viene stampato il log `NCCL_DEBUG`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

Le seguenti informazioni aggiuntive vengono visualizzate quando si utilizza un'istanza `p4d.24xlarge`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Fase 10: installare applicazioni di Machine Learning

Installa le applicazioni di machine learning sull'istanza temporanea. La procedura di installazione varia in base alla specifica applicazione di machine learning. Per ulteriori informazioni sull'installazione del software sulla tua istanza Linux, consulta Gestire il software sull'istanza Amazon Linux 2.

> **Note**
>
> Per le istruzioni di installazione, consulta la documentazione dell'applicazione di machine learning.

Fase 11: creazione di un EFA e di un'AMI abilitata NCCL

Dopo aver installato i componenti software necessari, procedi con la creazione di un'AMI che puoi riutilizzare per avviare le istanze abilitate per EFA.

Per creare un'AMI dall'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona l'istanza temporanea creata e seleziona Actions (Operazioni), Image (Immagine), Create Image (Crea immagine).
4. Per Create image (Crea immagine), effettua le seguenti operazioni:
   a. In Image name (Nome immagine), immettere un nome descrittivo per l'AMI.
   b. (Facoltativo) In Image description (Descrizione immagine), inserire una breve descrizione dell'AMI.
   c. Scegliere Create Image (Crea immagine).
5. Nel riquadro di navigazione scegliere AMIs (AMI).
6. Individuare nell'elenco l'AMI creata. Prima di procedere con la fase seguente, attendi che lo stato passi da `pending` a `available`.

Fase 12: terminare l'istanza temporanea

A questo punto l'istanza temporanea avviata non è più necessaria. È possibile terminare l'istanza per evitare di incorrere in costi aggiuntivi.

Per terminare l'istanza temporanea

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza temporanea creata, quindi scegliere Actions (Operazioni), Instance state (Stato istanza), Terminate instance (Termina istanza).
4. Quando viene richiesta la conferma, seleziona Termina.

Fase 13: avvio delle istanze EFA e delle istanze abilitate NCCL in un gruppo di collocazione cluster

Avvia le istanze abilitate per EFA e NCCL in un gruppo di collocazione cluster tramite l'AMI abilitata per EFA e il gruppo di sicurezza abilitato per EFA creati in precedenza.

> **Note**
>
> - Avviare le istanze abilitate per l'EFA in un gruppo di collocazione cluster non è un requisito in assoluto. È tuttavia consigliabile eseguire le istanze abilitate per EFA in un gruppo di collocazione cluster perché le istanze vengono così avviate in gruppo a bassa latenza in un'unica zona di disponibilità.
> - Per garantire che la capacità sia disponibile durante il dimensionamento delle istanze del cluster, è possibile creare una prenotazione della capacità per il gruppo di collocazione cluster. Per ulteriori informazioni, consulta Le Prenotazioni della capacità in gruppi di collocazione cluster..

New console

Per avviare un'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.
3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=EFA-instance`).
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), scegli My AMIs (Le mie AMI), quindi seleziona l'AMI creata nella fase precedente.
5. Nella sezione Instance type (Tipo di istanza), seleziona `p3dn.24xlarge` o `p4d.24xlarge`.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:

    a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.

    b. Per Firewall (security groups) (Firewall [gruppi di sicurezza]), scegli Select existing security group (Seleziona gruppo di sicurezza esistente) e quindi seleziona il gruppo di sicurezza creato nella fase precedente.

    c. Espandi la sezione Advanced network configuration (Configurazione di rete avanzata) e per Elastic Fabric Adapter seleziona Enable (Abilita).
8. (Opzionale) Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.
9. Nella sezione Advanced details (Dettagli avanzati), per Placement group name (Nome del gruppo di collocazione), seleziona il gruppo di collocazione cluster in cui avviare l'istanza. Se occorre creare un nuovo gruppo di collocazione cluster, scegli Create new placement group (Crea nuovo gruppo di collocazione).
10. Nel pannello Summary (Riepilogo) a destra, per Number of instances (Numero di istanze), inserisci il numero di istanze abilitate per EFA che desideri avviare, quindi seleziona Launch instance (Avvia istanza).

Old console

Per avviare le istanze abilitate per EFA e NCCL in un gruppo di collocazione cluster

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).

3. Nella pagina Choose an AMI (Scegli un'AMI), seleziona My AMIs (Le mie AMI), trova l'AMI creata in precedenza e quindi scegli Select (Seleziona).
4. Nella pagina Choose an Instance Type (Scegli il tipo di istanza), seleziona p3dn.24xlarge e scegli Next: Configure Instance Details (Fase successiva: configurazione dei dettagli dell'istanza).
5. Nella pagina Configure Instance Details (Configura i dettagli dell'istanza), procedere come segue:

   a. In Number of instances (Numero di istanze), immettere il numero di istanze abilitate per EFA e NCCL che si desidera avviare.
   b. In Network (Rete) e Subnet (Sottorete), selezionare il VPC e la sottorete in cui avviare le istanze.
   c. In Placement group (Gruppo di posizionamento), selezionare la casella Add instance to placement group (Aggiungi istanza a gruppo di posizionamento).
   d. In Placement group name (Nome del gruppo di posizionamento), selezionare Add to a new placement group (Aggiungi a un nuovo gruppo di posizionamento) e immettere un nome descrittivo per il gruppo di posizionamento. Quindi, in Placement group strategy (Strategia gruppo di posizionamento), selezionare Cluster.
   e. In EFA, scegliere Enable (Abilita).
   f. Nella sezione Network Interfaces (Interfacce di rete), per il dispositivo eth0 scegliere New network interface (Nuova interfaccia di rete). Facoltativamente, è possibile specificare un indirizzo IPv4 primario e uno o più indirizzi IPv4 secondari. Se l'istanza viene avviata in una sottorete alla quale è associato un blocco CIDR IPv6, è possibile specificare un indirizzo IPv6 primario e uno o più indirizzi IPv6 secondari.
   g. Scegliere Next: Add Storage (Successivo: aggiungi storage).
6. Nella pagina Add archiviazione (Aggiungi archiviazione), specificare i volumi da collegare all'istanza, oltre a quelli specificati dall'AMI (ad esempio il volume del dispositivo di root). Quindi selezionare Next: Add Tags (Fase successiva: aggiungere tag).
7. Nella pagina Add Tags (Aggiungi tag) specificare i tag per l'istanza, ad esempio un nome intuitivo, quindi selezionare Next: Configure Security Group (Successivo: configurazione del gruppo di sicurezza).
8. Nella pagina Configure Security Group (Configura gruppo di sicurezza), scegliere Assign a security group (Assegna un gruppo di sicurezza), selezionare Select an existing security group (Seleziona un gruppo di sicurezza esistente) e quindi selezionare il gruppo di sicurezza creato in precedenza.

9. Scegliere Review and Launch (Analizza e avvia).
10. Nella pagina Review Instance Launch (Verifica avvio istanza) controllare le impostazioni e selezionare Launch (Avvia) per scegliere una coppia di chiavi e avviare l'istanza.

Fase 14: abilitare SSH senza password

Per consentire l'esecuzione delle applicazioni in tutte le istanze del cluster, è necessario abilitare l'accesso SSH senza password dal nodo leader ai nodi membro. Il nodo principale è l'istanza da cui vengono eseguite le applicazioni. Le restanti istanze del cluster sono i nodi membro.

Per abilitare SSH senza password tra le istanze del cluster

1. Selezionare un'istanza nel cluster come nodo principale e connettersi a essa.
2. Disabilita `strictHostKeyChecking` e abilita `ForwardAgent` sul nodo principale. Aprire il file `~/.ssh/config` utilizzando qualsiasi editor di testo e aggiungere il seguente script.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Generare una coppia di chiavi RSA.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   La coppia di chiavi viene creata nella directory `$HOME/.ssh/`.
4. Modifica le autorizzazioni della chiave privata sul nodo principale.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Aprire `~/.ssh/id_rsa.pub` utilizzando l'editor di testo preferito e copiare la chiave.
6. Per ogni nodo membro nel cluster, procedere nel modo seguente:

   a. Collegarsi all'istanza.

   b. Aprire `~/.ssh/authorized_keys` utilizzando qualsiasi editor di testo e aggiungere la chiave pubblica copiata in precedenza.

7. Per verificare che SSH senza password funzioni come previsto, connettersi al nodo leader ed eseguire il seguente comando.

```
$ ssh member_node_private_ip
```

La connessione al nodo membro non dovrebbe richiedere una chiave o una password.

Utilizzo di EFA

Un EFA può essere creato, utilizzato e gestito proprio come qualsiasi altra interfaccia di rete elastica in Amazon EC2. Tuttavia, a differenza delle interfacce di rete elastica, EFAs non può essere collegato o scollegato da un'istanza in uno stato di esecuzione.

Requisiti EFA

Per utilizzare un EFA, assicurati di:

- Scegliere uno dei tipi di istanza supportati.
- Utilizza un'AMI per uno dei sistemi operativi supportati.
- Installare i componenti software EFA Per ulteriori informazioni, consulta Fase 3: installare il software EFA e Fase 5 (facoltativa): installare Intel MPI.
- Utilizzare un gruppo di sicurezza in cui sia consentito tutto il traffico in entrata e in uscita dal gruppo stesso. Per ulteriori informazioni, consulta Fase 1: preparare un gruppo di sicurezza abilitato per EFA.

Indice

Creazione di un EFA

Puoi creare un EFA in una sottorete di un VPC. Non puoi spostare l'EFA in un'altra sottorete dopo averlo creato. Puoi solo collegarlo alle istanze terminate nella stessa zona di disponibilità.

Per creare un nuovo EFA utilizzando la console:

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Scegliere Create Network Interface (Crea interfaccia di rete).
4. In Description (Descrizione), immettere un nome descrittivo per l'EFA.
5. In Subnet (Sottorete), selezionare la sottorete in cui creare l'EFA.
6. In Private IP (IP privato), immettere l'indirizzo IPv4 privato primario. Se non viene specificato un indirizzo IPv4, verrà selezionato un indirizzo IPv4 privato disponibile nella sottorete selezionata.
7. (Solo IPv6) se è stata selezionata una sottorete associata a un blocco CIDR IPv6, è possibile specificare un indirizzo IPv6 nel campo IPv6 IP (IP IPv6).
8. In Security groups (Gruppi di sicurezza), selezionare uno o più gruppi di sicurezza.
9. In EFA, scegliere Enabled (Abilitato).
10. Selezionare Yes, Create (Sì, crea).

Per creare un nuovo EFA utilizzando il AWS CLI

Utilizzate il create-network-interfacecomando e for`interface-type`, specificate`efa`, come illustrato nell'esempio seguente.

```
aws ec2 create-network-interface --subnet-id subnet-01234567890 --
description example_efa --interface-type efa
```

Collegare un EFA a un'istanza arrestata

È possibile collegare un EFA a qualsiasi tipo di istanza supportato che sia in stato `stopped`. Non è possibile collegare un EFA a un'istanza in stato `running`. Per ulteriori informazioni sui tipi di istanza supportati, vedi Tipi di istanze supportati.

Collegare EFA a un'istanza nello stesso modo in cui si collega un'interfaccia di rete elastica a un'istanza. Per ulteriori informazioni, consulta Collegamento di un'interfaccia di rete a un'istanza.

Collegare un EFA all'avvio di un'istanza

Come collegare un EFA esistente all'avvio di un'istanza (AWS CLI)

Utilizzate il comando run-instances e for NetworkInterfaceId, specificate l'ID dell'EFA, come mostrato nell'esempio seguente.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,NetworkInterfaceId=efa_id,Groups=sg_id,SubnetId=subnet_id
```

Come collegare un nuovo EFA all'avvio di un'istanza (AWS CLI)

Utilizzate il comando run-instances e for InterfaceType, specify`efa`, come illustrato nell'esempio seguente.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,InterfaceType=efa,Groups=sg_id,SubnetId=subnet_id
```

Aggiunta di un EFA a un modello di avvio

È possibile creare un modello di avvio contenente le informazioni di configurazione necessarie per avviare istanze abilitate per EFA. Per creare un modello di avvio abilitato per EFA, è necessario creare un nuovo modello di avvio e specificare un tipo di istanza supportato, l'AMI abilitata per l'EFA e il gruppo di sicurezza abilitato per l'EFA. Per ulteriori informazioni, consulta Nozioni di base su EFA e MPI.

Puoi impiegare i modelli di avvio per avviare istanze abilitate per EFA con altri servizi AWS , ad esempio AWS Batch o AWS ParallelCluster.

Per ulteriori informazioni sulla creazione dei modelli di lancio, consulta Creazione di un modello di avvio.

Gestire gli indirizzi IP per un EFA

È possibile modificare gli indirizzi IP associati a un file EFA. Se disponi di un indirizzo IP elastico (IPv4), puoi associarlo a un EFA. Se l'EFA è assegnato a una sottorete con un blocco CIDR IPv6 associato, puoi assegnare uno o più indirizzo IPv6 all'EFA.

La procedura per assegnare un indirizzo IP elastico (IPv4) e IPv6 a un EFA è uguale a quella usata per assegnare un indirizzo IP a un'ENI. Per ulteriori informazioni, vedere Gestione degli indirizzi IP.

Modifica del gruppo di sicurezza per EFA

Puoi modificare un gruppo di sicurezza collegato a un EFA. Per abilitare la funzionalità di bypass del sistema operativo, l'EFA deve far parte di un gruppo di sicurezza in cui sia consentito tutto il traffico in entrata e in uscita dal gruppo stesso.

La procedura per modificare il gruppo di sicurezza associato a un EFA è uguale a quella usata per modificare il gruppo di sicurezza associato a un'ENI. Per ulteriori informazioni, vedere Modifica del gruppo di protezione.

Scollegare un EFA

Per scollegare un EFA da un'istanza, devi prima arrestare tale istanza. Non è possibile scollegare un EFA da un'istanza in esecuzione.

Scollegare EFA da un'istanza nello stesso modo in cui si scollega un'interfaccia di rete elastica dall'istanza. Per ulteriori informazioni, consulta Scollegamento di un'interfaccia di rete da un'istanza.

Visualizzare gli EFAs

Puoi visualizzare tutti gli EFAs presenti nel tuo account.

Visualizzare EFAs nello stesso modo in cui si visualizzano le interfacce di rete elastica. Per ulteriori informazioni, consulta Visualizzazione dei dettagli relativi a un'interfaccia virtuale.

Eliminazione di un EFA

Per eliminare un EFA devi prima scollegarlo dall'istanza. Non è possibile eliminare un EFA mentre è ancora collegato a un'istanza.

Eliminare EFAs nello stesso modo in cui si eliminano le interfacce di rete elastica. Per ulteriori informazioni, consulta Eliminazione di un'interfaccia di rete.

Monitoraggio di un EFA

Puoi utilizzare le seguenti funzionalità per monitorare le prestazioni dei tuoi Elastic Fabric Adapter.

Log di flusso Amazon VPC

Puoi creare un log di flusso Amazon VPC per acquisire informazioni sul traffico da e per un EFA. I dati dei log di flusso possono essere pubblicati su Amazon CloudWatch Logs e Amazon S3. Dopo aver creato un log di flusso, puoi recuperare e visualizzarne i dati nella destinazione scelta. Per ulteriori informazioni, consulta l'argomento relativo ai Log di flusso VPC nella Guida per l'utente di Amazon VPC.

La procedura per creare un log di flusso per EFA è uguale a quella per crearlo per un'ENI. Per ulteriori informazioni, consulta Creazione di un log di flusso nella Guida per l'utente di Amazon VPC.

Nelle voci dei log di flusso, il traffico EFA è identificato da `srcAddress` e `destAddress`, entrambi formattati come indirizzi MAC, come mostrato nel seguente esempio.

```
version accountId  eniId        srcAddress        destAddress       sourcePort destPort
 protocol packets bytes start      end        action log-status
2       3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -          -
 -        9       5689  1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

Amazon CloudWatch fornisce metriche che ti consentono di monitorare i tuoi EFA in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi che inviino una notifica o intraprendano azioni quando un parametro specificato raggiunge una determinata soglia. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.

Verifica del programma di installazione EFA utilizzando un checksum

Facoltativamente, è possibile verificare il tarball EFA (file.tar.gz) utilizzando un checksum MD5 o SHA256. È consigliabile eseguire questa operazione per verificare l'identità dell'autore del software e che l'applicazione non sia stata alterata o danneggiata dopo la pubblicazione.

Per verificare il tarball

Utilizzare l'utilità md5sum per il checksum MD5 o l'utilità sha256sum per il checksum SHA256 e specificare il nome del file tarball. È necessario eseguire il comando dalla directory in cui è stato salvato il file tarball.

- MD5

```
$  md5sum tarball_filename.tar.gz
```

- SHA256

```
$  sha256sum tarball_filename.tar.gz
```

I comandi devono restituire un valore di checksum nel formato seguente.

```
checksum_value tarball_filename.tar.gz
```

Confrontare il valore di checksum restituito dal comando con il valore di checksum fornito nella tabella seguente. Se i checksum corrispondono, allora è sicuro eseguire lo script di installazione. Se i checksum non corrispondono, non eseguire lo script di installazione e contattare AWS Support.

Ad esempio, il comando seguente verifica il tarball EFA 1.9.4 utilizzando il checksum SHA256.

```
$  sha256sum aws-efa-installer-1.9.4.tar.gz
```

Output di esempio:

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

Nella tabella seguente sono elencati i checksum per le versioni recenti di EFA.

Versione	Scarica il URL	Checksum
EFA 1.33.0	https://efa-installer.amazonaws.com/aws-efa-installer -1.33.0.tar.gz	MD5: `e2f61fccbcaa11e2ccfddd3660522276` SHA256: `0372877b87c6a7337bb7791d255e1053b907d030489fb2c3732ba70069185fce`
EFA 1.32.0	https://efa-installer.amazonaws.com/aws-efa-installer -1.32.0.tar.gz	MD5: `db8d65cc028d8d08b5a9f2d88881c1b1`

Versione	Scarica il URL	Checksum
		SHA256: 5f7233760be57f6fee6de8c09acbfbf59238de848e06048dc54d156ef578fc66
EFA 1.31.0	https://efa-installer.amazonaws.com/aws-efa-installer -1.31.0.tar.gz	MD5: 856352f12bef2ccbadcd75e35aa52aaf SHA256: 943325bd37902a4300ac9e5715163537d56ecb4e7b87b37827c3e547aa1897bf
EFA 1.30.0	https://efa-installer.amazonaws.com/-1.30.0.tar.gz aws-efa-installer	MD5: 31f48e1a47fe93ede8ebd273fb747358 SHA256: 876ab9403e07a0c3c91a1a34685a52eced890ae052df94857f6081c5f6c78a0a
EFA 1.29.1	https://efa-installer.amazonaws.com/-1,29,1.tar.gz aws-efa-installer	MD5: e1872ca815d752c1d7c2b5c175e52a16 SHA256: 178b263b8c25845b63dc93b25bcdff5870df5204ec509af26f43e8d283488744
EFA 1.29.0	https://efa-installer.amazonaws.com/-1.29.0.tar.gz aws-efa-installer	MD5: 39d06a002154d94cd982ed348133f385 SHA256: 836655f87015547e733e7d9f7c760e4e24697f8bbc261bb5f3560abd4206bc36

Versione	Scarica il URL	Checksum
EFA 1.28.0	https://efa-installer.amazonaws.com/-1.28.0.tar.gz aws-efa-installer	MD5: 9dc13b744666582605e66febe074035 SHA256: 2e625d2d6d3e073b5178e8e861891273d896b66d03cb1a32244fd56789f1c435
EFA 1.27.0	https://efa-installer.amazonaws.com/-1.27.0.tar.gz aws-efa-installer	MD5: 98bfb515ea3e8d93f554020f3837fa15 SHA256: 1d49a97b0bf8d964d91652a79ac851f2550e33a5bf9d0cf86ec9357ff6579aa3
EFA 1.26.1	https://efa-installer.amazonaws.com/-1,26.1.tar.gz aws-efa-installer	MD5: 884e74671fdef4725501f7cd2d451d0c SHA256: c616994c924f54ebfabfab32b7fe8ac56947fae00a0ff453d975e298d174fc96
EFA 1.26.0	https://efa-installer.amazonaws.com/-1.26.0.tar.gz aws-efa-installer	MD5: f8839f12ff2e3b9ba09ae8a82b30e663 SHA256: bc1abc1f76e97d204d3755d2a9ca307fc423e51c63141f798c2f15be3715aa11

Versione	Scarica il URL	Checksum
EFA 1.25.1	https://efa-installer.amazonaws.com/-1,25.tar.gz aws-efa-installer	MD5: 6d876b894547847a45bb8854d4431f18 SHA256: d2abc553d22b89a4ce92882052c1fa6de450d3a801fe005da718b7d4b9602b06
EFA 1,25.0	https://efa-installer.amazonaws.com/-1.25.0.tar.gz aws-efa-installer	MD5: 1993836ca749596051da04694ea0d00c SHA256: 98b7b26ce031a2d6a93de2297cc71b03af647194866369ca53b60d82d45ad342
EFA 1.24.1	https://efa-installer.amazonaws.com/-1.24.1.tar.gz aws-efa-installer	MD5: 211b249f39d53086f3cb0c07665f4e6f SHA256: 120cfeec233af0955623ac7133b674143329f9561a9a8193e473060f596aec62
EFA 1.24.0	https://efa-installer.amazonaws.com/-1.24.0.tar.gz aws-efa-installer	MD5: 7afe0187951e2dd2c9cc4b572e62f924 SHA256: 878623f819a0d9099d76ecd41cf4f569d4c3aac0c9bb7ba9536347c50b6bf88e

Versione	Scarica il URL	Checksum
EFA 1.23.1	https://efa-installer.amazonaws.com/-1,23.1.tar.gz aws-efa-installer	MD5: 22491e114b6ee7160a8290145dca0c28 SHA256: 5ca848d8e0ff4d1571cd443c36f8d27c8cdf2a0c97e9068ebf000c303fc40797
EFA 1.23.0	https://efa-installer.amazonaws.com/-1.23.0.tar.gz aws-efa-installer	MD5: 38a6d7c1861f5038dba4e441ca7683ca SHA256: 555d497a60f22e3857fdeb3dfc53aa86d05926023c68c916d15d2dc3df6525bd
EFA 1.22.1	https://efa-installer.amazonaws.com/-1.22.1.tar.gz aws-efa-installer	MD5: 600c0ad7cdbc06e8e846cb763f92901b SHA256: f90f3d5f59c031b9a964466b5401e86fd0429272408f6c207c3f9048254e9665
EFA 1.22.0	https://efa-installer.amazonaws.com/-1.22.0.tar.gz aws-efa-installer	MD5: 8f100c93dc8ab519c2aeb5dab89e98f8 SHA256: f329e7d54a86a03ea51da6ea9a5b68fb354fbae4a57a02f9592e21fce431dc3a

Versione	Scarica il URL	Checksum
EFA 1.21.0	https://efa-installer.amazonaws.com/-1.21.0.tar.gz aws-efa-installer	MD5: 959ccc3a4347461909ec02ed3ba7c372 SHA256: c64e6ca34ccfc3ebe8e82d08899ae8442b3ef552541cf5429c43d11a04333050
EFA 1.20.0	https://efa-installer.amazonaws.com/-1.20.0.tar.gz aws-efa-installer	MD5: 7ebfbb8e85f1b94709df4ab3db47913b SHA256: aeefd2681ffd5c4c631d1502867db5b831621d6eb85b61fe3ec80df983d1dcf0
EFA 1.19.0	https://efa-installer.amazonaws.com/-1.19.0.tar.gz aws-efa-installer	MD5: 2fd45324953347ec5518da7e3fefa0ec SHA256: 99b77821b9e72c8dea015cc92c96193e8db307deee05b91a58094cc331f16709
EFA 1.18.0	https://efa-installer.amazonaws.com/-1.18.0.tar.gz aws-efa-installer	MD5: fc2571a72f5d3c7b7b576ce2de38d91e SHA256: acb18a0808aedb9a5e485f1469225b9ac97f21db9af78e4cd6939700debe1cb6

Versione	Scarica il URL	Checksum
EFA 1.17.3	https://efa-installer.amazonaws.com/-1.17.3.tar.gz aws-efa-installer	MD5: `0517df4a190356ab559235147174cafd` SHA256: `5130998b0d2883bbae189b21ab215ecbc1b01ae0231659a9b4a17b0a33ebc6ca`
EFA 1.17.2	https://efa-installer.amazonaws.com/-1.17.2.tar.gz aws-efa-installer	MD5: `a329dedab53c4832df218a24449f4c9a` SHA256: `bca1fdde8b32b00346e175e597ffab32a09a08ee9ab136875fb38283cc4cd099`
EFA 1.17.1	https://efa-installer.amazonaws.com/-1.17.1.tar.gz aws-efa-installer	MD5: `733ae2cfc9d14b52017eaf0a2ab6b0ff` SHA256: `f29322640a88ae9279805993cb836276ea240623820848463ca686c8ce02136f`
EFA 1.17.0	https://efa-installer.amazonaws.com/-1.17.0.tar.gz aws-efa-installer	MD5: `d430fc841563c11c3805c5f82a4746b1` SHA256: `75ab0cee4fb6bd38889dce313183f5d3a83bd233e0a6ef6205d8352821ea901d`

Versione	Scarica il URL	Checksum
EFA 1.16.0	https://efa-installer.amazonaws.com/-1.16.0.tar.gz aws-efa-installer	MD5: 399548d3b0d2e812d74dd67937b696b4 SHA256: cecec36495a1bc6fdc82f97761a541e4fb6c9a3cbf3cfcb145acf25ea5dbd45b
EFA 1.15.2	https://efa-installer.amazonaws.com/-1.15.2.tar.gz aws-efa-installer	MD5: 955fea580d5170b05823d51acde7ca21 SHA256: 84df4fbc1b3741b6c073176287789a601a589313accc8e6653434e8d4c20bd49
EFA 1.15.1	https://efa-installer.amazonaws.com/-1.15.1.tar.gz aws-efa-installer	MD5: c4610267039f72bbe4e35d7bf53519bc SHA256: be871781a1b9a15fca342a9d169219260069942a8bda7a8ad06d4baeb5e2efd7
EFA 1.15.0	https://efa-installer.amazonaws.com/-1.15.0.tar.gz aws-efa-installer	MD5: 9861694e1cc00d884fadac07d22898be SHA256: b329862dd5729d2d098d0507fb486bf859d7c70ce18b61c302982234a3a5c88f

Versione	Scarica il URL	Checksum
EFA 1.14.1	https://efa-installer.amazonaws.com/-1.14.1.tar.gz aws-efa-installer	MD5: 50ba56397d359e57872fde1f74d4168a SHA256: c7b1b48e86fe4b3eaa4299d3600930919c4fe6d88cc6e2c7e4a408a3f16452c7
EFA 1.14.0	https://efa-installer.amazonaws.com/-1.14.0.tar.gz aws-efa-installer	MD5: 40805e7fd842c36ececb9fd7f921b1ae SHA256: 662d62c12de85116df33780d40e0533ef7dad92709f4f613907475a7a1b60a97
EFA 1.13.0	https://efa-installer.amazonaws.com/-1.13.0.tar.gz aws-efa-installer	MD5: c91d16556f4fd53becadbb345828221e SHA256: ad6705eb23a3fce44af3afc0f7643091595653a723ad0374084f4f2b715192e1
EFA 1.12.3	https://efa-installer.amazonaws.com/-1,12.3.tar.gz aws-efa-installer	MD5: 818aee81f097918cfaebd724eddea678 SHA256: 2c225321824788b8ca3fbc118207b944cdb096b847e1e0d1d853ef2f0d727172

Versione	Scarica il URL	Checksum
EFA 1.12.2	https://efa-installer.amazonaws.com/-1.12.2.tar.gz aws-efa-installer	MD5: 956bb1fc5ae0d6f0f87d2e481d49fccf SHA256: 083a868a2c212a5a4fcf3e4d732b685ce39cceb3ca7e5d50d0b74e7788d06259
EFA 1.12.1	https://efa-installer.amazonaws.com/-1.12.1.tar.gz aws-efa-installer	MD5: f5bfe52779df435188b0a2874d0633ea SHA256: 5665795c2b4f09d5f3f767506d4d4c429695b36d4a17e5758b27f033aee58900
EFA 1.12.0	https://efa-installer.amazonaws.com/-1.12.0.tar.gz aws-efa-installer	MD5: d6c6b49fafb39b770297e1cc44fe68a6 SHA256: 28256c57e9ecc0b0778b41c1f777a9982b4e8eae782343dfe1246079933dca59
EFA 1.11.2	https://efa-installer.amazonaws.com/-1.11.2.tar.gz aws-efa-installer	MD5: 2376cf18d1353a4551e35c33d269c404 SHA256: a25786f98a3628f7f54f7f74ee2b39bc6734ea9374720507d37d3e8bf8ee1371

Versione	Scarica il URL	Checksum
EFA 1.11.1	https://efa-installer.amazonaws.com/-1.11.1.tar.gz aws-efa-installer	MD5: `026b0d9a0a48780cc7406bd51997b1c0` SHA256: `6cb04baf5ffc58ddf319e956b5461289199c8dd805fe216f8f9ab8d102f6d02a`
EFA 1.11.0	https://efa-installer.amazonaws.com/-1.11.0.tar.gz aws-efa-installer	MD5: `7d9058e010ad65bf2e14259214a36949` SHA256: `7891f6d45ae33e822189511c4ea1d14c9d54d000f6696f97be54e915ce2c9dfa`
EFA 1.10.1	https://efa-installer.amazonaws.com/-1.10.1.tar.gz aws-efa-installer	MD5: `78521d3d668be22976f46c6fecc7b730` SHA256: `61564582de7320b21de319f532c3a677d26cc46785378eb3b95c636506b9bcb4`
EFA 1.10.0	https://efa-installer.amazonaws.com/-1.10.0.tar.gz aws-efa-installer	MD5: `46f73f5a7afe41b4bb918c81888fefa9` SHA256: `136612f96f2a085a7d98296da0afb6fa807b38142e2fc0c548fa986c41186282`

Versione	Scarica il URL	Checksum
EFA 1.9.5	https://efa-installer.amazonaws.com/-1.9.5.tar.gz aws-efa-installer	MD5: 95edb8a209c18ba8d250409846eb6ef4 SHA256: a4343308d7ea4dc943ccc21bcebed913e8868e59bfb2ac93599c61a7c87d7d25
EFA 1.9.4	https://efa-installer.amazonaws.com/-1.9.4.tar.gz aws-efa-installer	MD5: f26dd5c350422c1a985e35947fa5aa28 SHA256: 1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14
EFA 1.9.3	https://efa-installer.amazonaws.com/-1.9.3.tar.gz aws-efa-installer	MD5: 95755765a097802d3e6d5018d1a5d3d6 SHA256: 46ce732d6f3fcc9edf6a6e9f9df0ad136054328e24675567f7029edab90c68f1
EFA 1.8.4	https://efa-installer.amazonaws.com/-1.8.4.tar.gz aws-efa-installer	MD5: 85d594c41e831afc6c9305263140457e SHA256: 0d974655a09b213d7859e658965e56dc4f23a0eee2dc44bb41b6d039cc5bab45

Topologia dell'istanza Amazon EC2

La descrizione della topologia dell'istanza fornisce una visualizzazione gerarchica della relativa prossimità tra le istanze. È possibile utilizzare queste informazioni per gestire l'infrastruttura

di elaborazione ad alte prestazioni (HPC) e l'apprendimento automatico (ML) su larga scala, ottimizzando al contempo l'inserimento lavorativo. I processi HPC e ML sono sensibili alla latenza e alla velocità di trasmissione effettiva. È possibile utilizzare la topologia dell'istanza per rilevare la posizione delle istanze e quindi utilizzare queste informazioni per ottimizzare i processi HPC e ML eseguendoli su istanze fisicamente più vicine tra loro.

È possibile utilizzare la topologia delle istanze per rilevare la posizione delle istanze esistenti, ma non per scegliere di avviare una nuova istanza fisicamente vicino a un'istanza esistente. Per influenzare il posizionamento dell'istanza, puoi usareLe Prenotazioni della capacità in gruppi di collocazione cluster..

Prezzi

Non sono previsti costi aggiuntivi per descrivere la topologia dell'istanza.

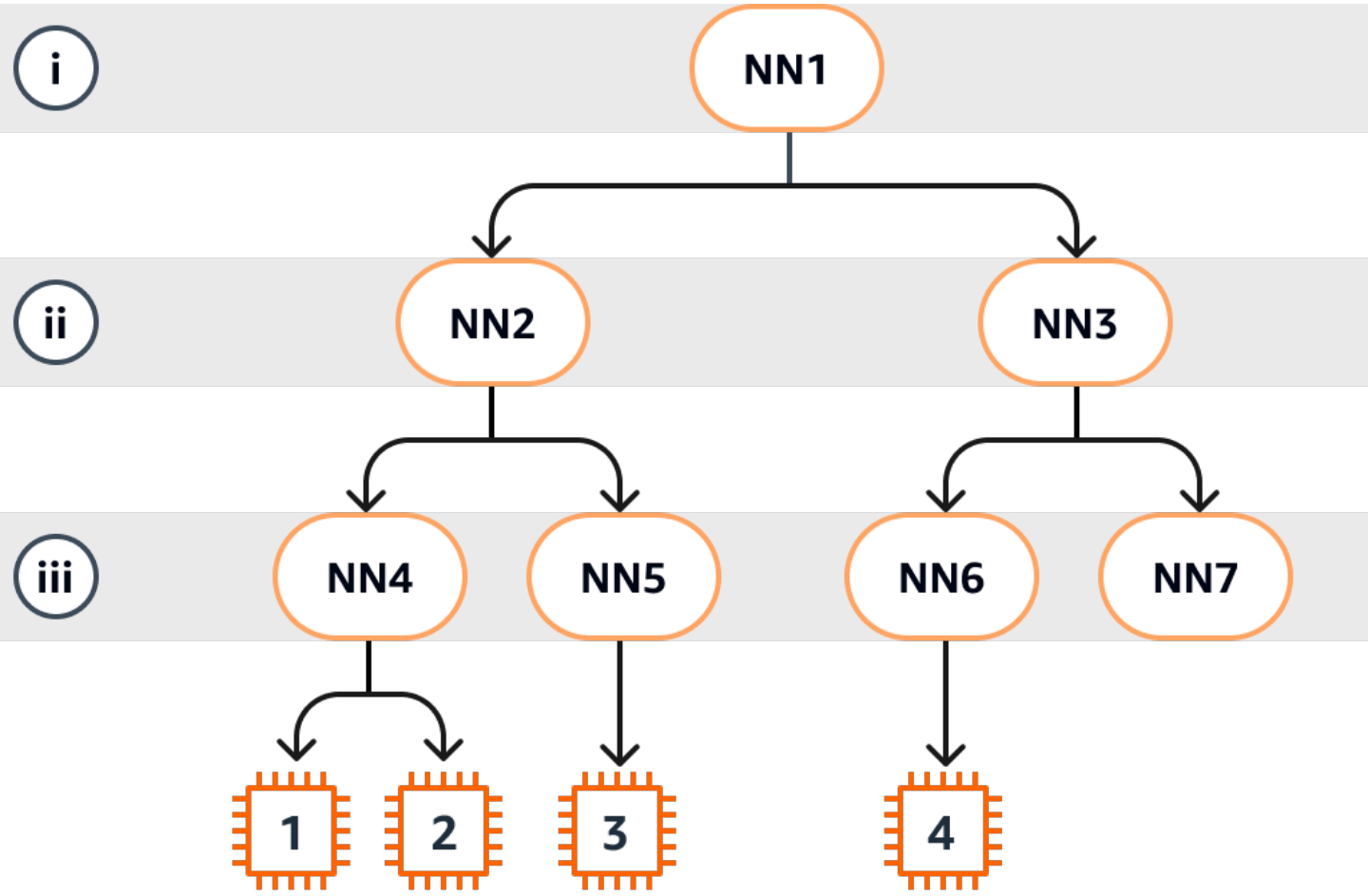
Indice

Come funziona la topologia delle istanze

Ogni istanza EC2 si connette a un set di nodi. Un set di nodi comprende tre nodi di rete, ognuno dei quali rappresenta un livello diverso della AWS rete. I livelli di rete sono disposti in una gerarchia di 3 o più livelli. Il set di nodi fornisce la visualizzazione dall'alto verso il basso di questa gerarchia, con il livello inferiore connesso più vicino a un'istanza.

Le informazioni sul set di nodi sono chiamate topologia dell'istanza.

Il diagramma seguente fornisce una rappresentazione visiva che è possibile utilizzare per comprendere la topologia dell'istanza. I nodi di rete sono identificati come NN1 — NN7. I numeri i, ii e iii identificano i livelli di rete. I numeri 1, 2, 3 e 4 identificano le istanze EC2. Le istanze si connettono a un nodo nel livello inferiore, identificato da iii. Più istanze possono connettersi allo stesso nodo.



In questo esempio:

- L'istanza 1 si connette al nodo di rete 4 (NN4) nel livello iii. NN4 si connette al nodo di rete 2 (NN2) nel livello ii e NN2 si connette al nodo di rete 1 (NN1) nel livello i, che è la parte superiore della gerarchia di rete in questo esempio. Il set di nodi di rete comprende NN1, NN2 e NN4, espressi gerarchicamente dai livelli superiori al livello inferiore.
- L'istanza 2 si connette anche al nodo di rete 4 (NN4). L'istanza 1 e l'istanza 2 condividono lo stesso set di nodi di rete: NN1, NN2 e NN4.
- L'istanza 3 si connette al nodo di rete 5 (NN5). NN5 si connette a NN2 e NN2 si connette a NN1. Il set di nodi di rete per l'istanza 3 è NN1, NN2 e NN5.
- L'istanza 4 si connette al nodo di rete 6 (NN6). Il set di nodi di rete è NN1, NN3 e NN6.

Se si considera la vicinanza delle istanze 1, 2 e 3, le istanze 1 e 2 sono più vicine tra loro perché si connettono allo stesso nodo di rete (NN4), mentre l'istanza 3 è più lontana perché si connette a un nodo di rete diverso (NN5).

Se si considera la prossimità di tutte le istanze in questo diagramma, le istanze 1, 2 e 3 sono più vicine tra loro rispetto all'istanza 4 perché condividono NN2 nel loro set di nodi di rete.

Come regola generale, se il nodo di rete connesso a due istanze qualsiasi è lo stesso, queste istanze sono fisicamente vicine l'una all'altra, come nel caso delle istanze 1 e 2. Inoltre, minore è il numero di salti tra i nodi di rete, più le istanze sono vicine tra loro. Ad esempio, le istanze 1 e 3 hanno meno passaggi verso un nodo di rete comune (NN2) rispetto al nodo di rete (NN1) che hanno in comune con l'istanza 4 e sono quindi più vicine tra loro di quanto non lo siano all'istanza 4.

In questo esempio non ci sono istanze in esecuzione nel nodo di rete 7 (NN7) e pertanto l'output dell'API non includerà NN7.

Come interpretare l'output

È possibile ottenere le informazioni sulla topologia dell'istanza utilizzando l'API. DescribeInstanceTopology L'output fornisce una visualizzazione gerarchica della topologia di rete sottostante per un'istanza.

Il seguente output di esempio corrisponde alle informazioni sulla topologia di rete delle quattro istanze del diagramma precedente. Ai fini di questo esempio, i commenti sono inclusi nell'output di esempio.

È importante tenere presente le seguenti informazioni nell'output:

- `NetworkNodes` descrive il set di nodi di rete di un'istanza.
- In ogni set di nodi di rete, i nodi di rete sono elencati in ordine gerarchico dall'alto verso il basso.
- Il nodo di rete connesso all'istanza è l'ultimo nodo di rete nell'elenco (il livello inferiore).
- Per capire quali istanze sono vicine tra loro, individua innanzitutto i nodi di rete comuni nel livello inferiore. Se non ci sono nodi di rete comuni nel livello inferiore, individua i nodi di rete comuni nei livelli superiori.

Nel seguente output di esempio, le istanze `i-1111111111example` e `i-2222222222example` sono posizionate più vicine l'una all'altra rispetto alle altre istanze di questo esempio, perché hanno il nodo di rete `nn-4444444444example` in comune nel livello inferiore.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",  //Corresponds to instance 1
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
```

```
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 in layer i
                "nn-2222222222example",           //Corresponds to NN2 in layer ii
                "nn-4444444444example"            //Corresponds to NN4 in layer iii -
bottom layer, connected to the instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",  //Corresponds to instance 2
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-4444444444example"            //Corresponds to NN4 - layer iii -
connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",  //Corresponds to instance 3
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-5555555555example"            //Corresponds to NN5 - layer iii -
connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-444444444example",  //Corresponds to instance 4
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",          //Corresponds to NN1 - layer i
                "nn-3333333333example",          //Corresponds to NN3 - layer ii
                "nn-6666666666example"           //Corresponds to NN6 - layer iii -
connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
```

```
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Limitazioni

Si applicano le limitazioni seguenti:

- Le istanze devono trovarsi nello stato. `running`
- La vista della topologia di ogni istanza è unica per account.
- non AWS Management Console supporta la visualizzazione della topologia dell'istanza.

Prerequisiti, ad esempio la topologia

Prima di descrivere la topologia delle istanze, assicurati che le istanze soddisfino i seguenti requisiti.

Requisiti per descrivere la topologia delle istanze

- Regioni AWS
- Tipi di istanza
- Stato istanza
- Autorizzazione IAM

Regioni AWS

Supportato: Regioni AWS

- Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon)
- Asia Pacifico (Seoul), Asia Pacifico (Tokyo)
- Canada (Centrale)
- Europa (Francoforte), Europa (Irlanda), Europa (Stoccolma)

Tipi di istanza

Tipi di istanze supportati:

- `hpc6a.48xlarge` | `hpc6id.32xlarge` | `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc7g.4xlarge` | `hpc7g.8xlarge` | `hpc7g.16xlarge`
- `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge`
- `trn1.2xlarge` | `trn1.32xlarge` | `trn1n.32xlarge`

Visualizzazione dei tipi di istanza disponibili in una Regione specifica

I tipi di istanza disponibili variano in base alla regione. Per verificare se un tipo di istanza è disponibile in una Regione, utilizza il comando describe-instance-types-offerings con il parametro `--region`. Includi il parametro `--filters` per assegnare i risultati alla famiglia dell'istanza o al tipo di istanza desiderato e il parametro `--query` per assegnare l'output al valore di `InstanceType`.

```
aws ec2 describe-instance-type-offerings \
    --region us-east-2 \
    --filters 'Name=instance-type, Values=trn1*' \
    --query 'InstanceTypeOfferings[].InstanceType'
```

Output previsto

```
[
    "trn1.2xlarge",
    "trn1.32xlarge",
    "trn1n.32xlarge"
]
```

Stato istanza

Le istanze devono essere nello stato `running`. Non è possibile ottenere informazioni sulla topologia delle istanze per le istanze che si trovano in un altro stato.

Autorizzazione IAM

La tua identità IAM (utente, gruppo di utenti o ruolo) richiede la seguente autorizzazione IAM:

- `ec2:DescribeInstanceTopology`

Esempi di topologia di istanze Amazon EC2

Puoi usare il comando describe-instance-topologyCLI per descrivere la topologia dell'istanza per le tue istanze EC2.

Quando utilizzi il comando `describe-instance-topology` senza parametri o filtri, la risposta includerà tutte le istanze che corrispondono ai tipi di istanza supportati per questo comando nella Regione specificata. È possibile specificare la Regione includendo il parametro `--region` o impostando una Regione predefinita. Per ulteriori informazioni sull'impostazione di una Regione predefinita, consulta Specificazione della regione di una risorsa.

È possibile includere parametri per restituire istanze che corrispondono agli ID di istanza o ai nomi dei gruppi di posizionamento specificati. È inoltre possibile includere filtri per restituire istanze che corrispondono a un tipo o una famiglia di istanze specifici o istanze in una zona di disponibilità o una zona locale specificata. È possibile includere un singolo parametro o filtro o una combinazione di parametri e filtri.

L'output è impaginato, con un massimo di 20 istanze per pagina per impostazione predefinita. È possibile specificare fino a 100 istanze per pagina utilizzando il parametro `--max-results`.

Per ulteriori informazioni, consulta la sezione describe-instance-topology nella Documentazione di riferimento della AWS CLI .

Autorizzazioni richieste

È richiesta la seguente autorizzazione per descrivere la topologia dell'istanza:

- `ec2:DescribeInstanceTopology`

Esempi

Esempio 1: Nessun parametro o filtro

Descrizione della topologia dell'istanza di tutte le istanze

Utilizza il comando describe-instance-topology della CLI senza specificare parametri o filtri.

```
aws ec2 describe-instance-topology --region us-west-2
```

La risposta restituirà solo le istanze che corrispondono ai tipi di istanze supportati per questa API. Le istanze possono trovarsi in diverse zone di disponibilità, zone locali (`ZoneId`) e gruppi di posizionamento (`GroupName`). Se un'istanza non si trova in un gruppo di posizionamento, il campo `GroupName` non sarà visualizzato nell'output. Nel seguente output di esempio, in un gruppo di posizionamento si trova solo una istanza.

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "my-ml-cpg",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
```

```
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Esempio 2: Filtro per tipo di istanza

È possibile filtrare in base a un tipo di istanza specificato (corrispondenza esatta) o a una famiglia di istanze (utilizzando un carattere jolly). È inoltre possibile combinare un filtro per tipo di istanza specificato e un filtro per una famiglia di istanze.

Esempio 2a: Filtro di corrispondenza esatta per un tipo di istanza specificato

Descrizione della topologia delle istanze di tutte le istanze che corrispondono a un tipo di istanza specificato

Usa il comando describe-instance-topology della CLI con il filtro `instance-type`. In questo esempio, l'output viene filtrato per le istanze `trn1n.32xlarge`. La risposta restituirà solo le istanze che corrispondono al tipo di istanza specificato.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1n.32xlarge
```

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Esempio 2b: Filtro con carattere jolly per una famiglia di istanze

Descrizione della topologia delle istanze di tutte le istanze che corrispondono a una famiglia di istanze

Usa il comando describe-instance-topology della CLI con il filtro `instance-type`. In questo esempio, l'output viene filtrato per le istanze `trn1*`. La risposta restituirà solo le istanze che corrispondono alla famiglia di istanze specificata.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1*
```

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```


Esempio 2c: Filtri combinati per famiglia di istanze e corrispondenza esatta

Descrizione della topologia delle istanze di tutte le istanze che corrispondono a una famiglia di istanze o a un tipo di istanza specificati

Usa il comando describe-instance-topology della CLI con il filtro `instance-type`. In questo esempio, l'output viene filtrato per le istanze `pd4d*` o `trn1n.32xlarge`. La risposta restituirà le istanze che corrispondono ai filtri specificati.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"
```

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-4343434343example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Esempio 3: Filtro per ID zona

È possibile utilizzare il filtro `zone-id` per filtrare in base a una zona di disponibilità o una zona locale. È inoltre possibile combinare un filtro per la zona di disponibilità e un filtro per la zona locale.

Esempio 3a: Filtro per zona di disponibilità

Descrizione della topologia delle istanze di tutte le istanze che corrispondono a una zona di disponibilità specificata

Usa il comando describe-instance-topology della CLI con il filtro `zone-id`. In questo esempio, l'output viene filtrato utilizzando l'ID della zona di disponibilità. `use1-az1` La risposta restituirà solo le istanze che corrispondono alla zona di disponibilità specificata.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1
```

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Esempio 3b: Filtro per zona locale

Per descrivere la topologia delle istanze di tutte le istanze che corrispondono a una zona locale specificata

Usa il comando describe-instance-topology della CLI con il filtro `zone-id`. In questo esempio, l'output viene filtrato utilizzando l'ID della zona locale. `use1-atl2-az1` La risposta restituirà solo le istanze che corrispondono alla zona locale specificata.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-atl2-az1
```

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Esempio 3c: Filtri combinati per zona di disponibilità e zona locale

Descrizione della topologia delle istanze di tutte le istanze che corrispondono a una zona di disponibilità o zona locale specificata

Usa il comando describe-instance-topology della CLI con il filtro `zone-id`. In questo esempio, l'output viene filtrato utilizzando l'ID della zona di disponibilità `use1-az1` e l'ID della zona locale. `use1-atl2-az1` La risposta restituirà le istanze che corrispondono ai filtri specificati.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Esempio 4: Filtri combinati per tipo di istanza e ID zona

È possibile combinare tutti i filtri in un unico comando.

Descrizione della topologia delle istanze di tutte le istanze che corrispondono a un tipo di istanza, una famiglia di istanze, una zona di disponibilità o una zona locale specificati

Usa il comando describe-instance-topology della CLI con i filtri `instance-type` e `zone-id`. In questo esempio, l'output viene filtrato in base alla famiglia di `p4d*` istanze, al tipo di `trn1n.32xlarge` istanza, all'ID della zona di `use1-az1` disponibilità e all'ID della zona `use1-atl2-az1` locale. La risposta restituirà le istanze che corrispondono a `p4d*` oppure le istanze `trn1n.32xlarge` nella `us-east-1a` oppure le zone `us-east-1-atl-2a`.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" "Name=zone-
id,Values=use1-az1,use1-atl2-az1"
```

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Esempio 5: Parametro relativo al nome del gruppo di posizionamento

Descrizione della topologia di tutte le istanze in un gruppo di posizionamento specificato

Utilizza il comando describe-instance-topology della CLI con il parametro `group-names`. Nell'esempio seguente, le istanze possono appartenere al gruppo di posizionamento `ML-group` o `HPC-group`. La risposta restituirà le istanze che si trovano in uno dei gruppi di posizionamento.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --group-names ML-group HPC-group
```

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Esempio 6: ID istanza

Descrizione della topologia dell'istanza specificata

Utilizza il comando describe-instance-topology della CLI con il parametro `--instance-ids`. La risposta restituirà le istanze che corrispondono agli ID istanza specificati.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --instance-ids i-1111111111example i-2222222222example
```

Output di esempio

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Gruppi di collocamento

Per soddisfare le esigenze del tuo carico di lavoro, puoi avviare un gruppo di istanze EC2 interdipendenti in un gruppo di collocamento per influire sul collocamento.

A seconda del tipo di carico di lavoro, puoi creare un gruppo di collocamento con una delle strategie seguenti:

- Cluster: raggruppa le istanze in una zona di disponibilità. Questa strategia consente ai carichi di lavoro di raggiungere le prestazioni di rete a bassa latenza necessarie per node-to-node comunicazioni strettamente accoppiate tipiche delle applicazioni HPC (High Performance Computing).
- Partizione: distribuisce le istanze sulle partizioni logiche, garantendo così che le istanze in una partizione non condividano l'hardware sottostante con gruppi di istanze in altre partizioni. Questa strategia di solito viene utilizzata in grandi carichi di lavoro distribuiti e replicati, come Hadoop, Cassandra e Kafka.
- Distribuzione: distribuisce un piccolo gruppo di istanze in uno specifico hardware sottostante per ridurre gli errori correlati.

I gruppi di collocamento sono facoltativi. Se non avvii le istanze in un gruppo di collocamento, EC2 prova a posizionarle in modo che tutte le istanze siano distribuite in tutto l'hardware sottostante, così da ridurre al minimo gli errori correlati.

La creazione dei gruppi di collocamento non prevede l'applicazione di costi.

Strategie di posizionamento

È possibile creare un gruppo di posizionamento utilizzando una delle seguenti strategie.

Strategie di posizionamento:

- Gruppi di collocazione cluster
- Gruppi di collocamento di partizione
- Gruppi di collocamento sparsi

Gruppi di collocazione cluster

Un gruppo di collocazione cluster è un raggruppamento logico di istanze all'interno di una singola zona di disponibilità. Le istanze non sono isolate in un singolo rack. Un gruppo di posizionamento cluster può comprendere reti private virtuali (VPC) collegate in peering che si trovano nella stessa Regione. Le istanze dello stesso gruppo di collocazione cluster godono di un limite di velocità effettiva per flusso superiore per il traffico TCP/IP e vengono collocate nello stesso segmento di larghezza di banda ad alta bisezione della rete.

La seguente immagine mostra istanze collocate in un gruppo di collocazione cluster.

I gruppi di collocazione cluster sono consigliati per le applicazioni a bassa latenza di rete, velocità effettiva di rete elevata o entrambe. Sono consigliati anche quando la maggior parte del traffico di rete si trova tra le istanze del gruppo. Per fornire la latenza più bassa e le massime prestazioni di packet-per-second rete per il tuo gruppo di collocamento, scegli un tipo di istanza che supporti la rete avanzata. Per ulteriori informazioni, consulta la sezione relativa alle reti avanzate.

Si consiglia di avviare le istanze nel modo seguente:

- Utilizzare una singola richiesta di avvio per avviare il numero di istanze necessarie nel gruppo di posizionamento.
- Utilizzare lo stesso tipo di istanza per tutte le istanze del gruppo di posizionamento.

Se provi ad aggiungere altre istanze al gruppo di collocamento in un secondo momento o se provi ad avviare più di un tipo di istanza nel gruppo di collocamento, avrai più possibilità di ricevere un errore di capacità non sufficiente.

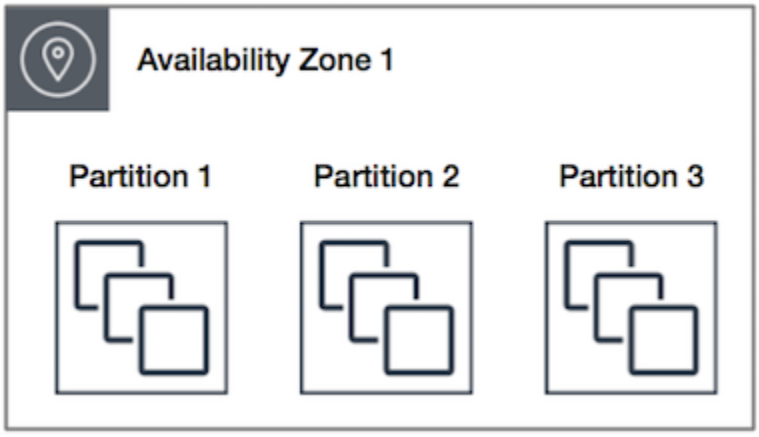
Se arresti un'istanza in un gruppo di collocamento e poi la riavvii, quest'ultima continua a essere eseguita nel gruppo di collocamento. Tuttavia, l'avvio non riesce se non è presente capacità sufficiente per l'istanza.

Se ricevi un errore di capacità durante l'avvio di un'istanza in un gruppo di collocamento nel quale sono già in esecuzione delle istanze, arresta e avvia tutte le istanze del gruppo di collocamento e prova a ripetere l'accesso. Il riavvio delle istanze potrebbe causarne la migrazione sull'hardware che dispone della capacità per tutte le istanze richieste.

Gruppi di collocamento di partizione

I gruppi di collocamento di partizione contribuiscono a ridurre le probabilità di errori correlati all'hardware per l'applicazione. Quando si utilizzano gruppi di collocamento di partizione, Amazon EC2 divide ogni gruppo in segmenti logici denominati partizioni. Amazon EC2 assicura che ogni partizione nell'ambito di un gruppo di collocamento abbia un proprio set di rack. Ciascun rack dispone di rete e alimentazione proprie. Due partizioni nell'ambito di un gruppo di collocazione non possono condividere gli stessi rack, consentendoti di isolare l'impatto degli errori hardware all'interno della tua applicazione.

L'immagine seguente è una semplice rappresentazione visiva di un gruppo di collocazione di una partizione in una singola zona di disponibilità. Mostra istanze collocate in un gruppo di collocamento con tre partizioni—Partition 1 (Partizione 1), Partition 2 (Partizione 2) e Partition 3 (Partizione 3). Ogni partizione include più istanze. Le istanze di una partizione non condividono i rack con le istanze di altre partizioni, limitando così l'impatto di un singolo errore hardware alla sola partizione associata.



I gruppi di collocamento di partizione possono essere impiegati per distribuire carichi di lavoro ampiamente diffusi e replicati come HDFS, HBase e Cassandra su rack diversi. Quando si avviano istanze in un gruppo di collocamento di partizione, Amazon EC2 tenta di distribuirle in modo

omogeneo nel numero di partizioni specificato. È inoltre possibile avviare le istanze in una partizione specifica per avere maggior controllo sulla destinazione delle istanze.

Un gruppo di collocamento di partizione può avere partizioni in più zone di disponibilità della stessa regione. Un gruppo di collocamento di partizione può avere al massimo sette partizioni per zona di disponibilità. Il numero di istanze avviabili in un gruppo di collocamento di partizione è limitato solo dalle restrizioni vigenti nel proprio account.

I gruppi di collocamento di partizione offrono inoltre visibilità sulle partizioni, poiché consentono di controllare quali istanze sono su determinate partizioni. Puoi condividere queste informazioni con applicazioni che supportano la topologia, come HDFS, HBase e Cassandra. Questa applicazioni utilizzano queste informazioni per prendere decisioni intelligenti sulla replica dei dati per aumentare la disponibilità e la durabilità dei dati.

Se si avvia un'istanza in un gruppo di collocamento di partizione e l'hardware univoco è insufficiente per l'esecuzione della richiesta, quest'ultima produce un errore. Amazon EC2 rende disponibile ulteriore hardware separato nel tempo, per consentire di riprovare a effettuare la richiesta in un secondo momento.

Gruppi di collocamento sparsi

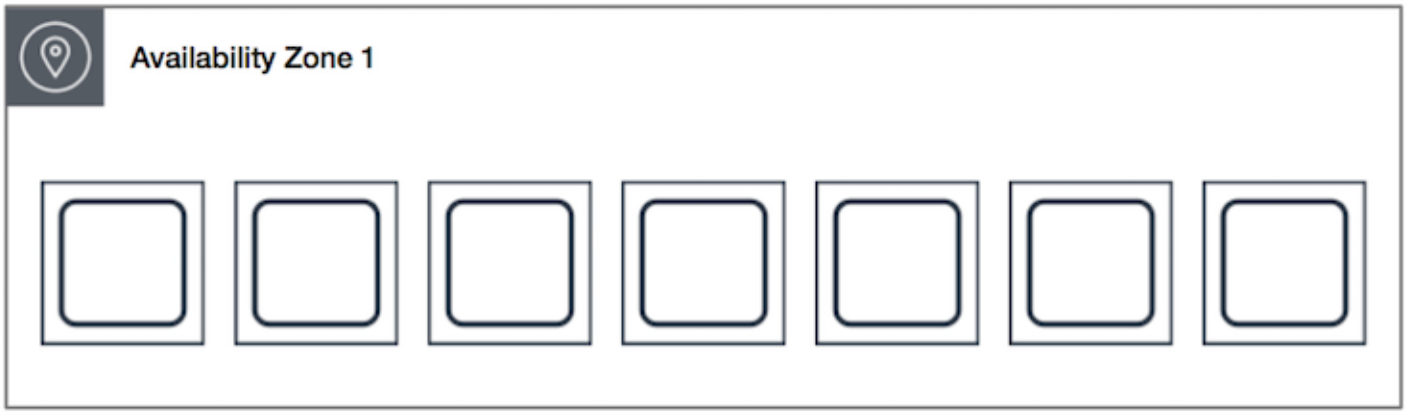
Un gruppo di posizionamento sparso è un gruppo di istanze, ognuna delle quali collocata su un hardware distinto.

I gruppi di collocamento sparsa sono consigliati per le applicazioni con un numero ridotto di istanze critiche che è necessario tenere separate. L'avvio delle istanze in un gruppo di posizionamento sparso riduce il rischio degli errori simultanei che possono verificarsi quando le istanze condividono la stessa apparecchiatura. I gruppi di posizionamento sparso forniscono l'accesso a hardware distinto, per cui sono adatti per mescolare tipi di istanze diversi o per avviare le istanze nel tempo.

Se si avvia un'istanza in un gruppo di collocamento sparso e l'hardware univoco è insufficiente per l'esecuzione della richiesta, quest'ultima produce un errore. Amazon EC2 rende disponibile ulteriore hardware separato nel tempo, per consentire di riprovare a effettuare la richiesta in un secondo momento. I gruppi di posizionamento possono distribuire istanze tra rack o host. I gruppi di collocamento distribuiti a livello di rack possono essere utilizzati nelle AWS regioni e così via AWS Outposts. I gruppi di spread placement a livello di host possono essere utilizzati AWS Outposts solo con.

Gruppi di posizionamento dello spread a livello di rack

La seguente immagine mostra sette istanze in esecuzione in una sola zona di disponibilità e collocate in un gruppo di collocamento sparsa. Le sette istanze sono collocate su sette rack diversi, ognuno dei quali è dotato di una propria rete e alimentazione.



Un gruppo di distribuzione a livello di rack può estendersi su più zone di disponibilità nella stessa regione. In una regione, un gruppo di distribuzione dello spread a livello di rack può avere un massimo di sette istanze in esecuzione per zona di disponibilità per gruppo. Con Outposts, un gruppo di spread placement a livello di rack può contenere tante istanze quanti sono i rack presenti nella distribuzione Outpost.

Gruppi di posizionamento sparso a livello di host

I gruppi di collocamento distribuiti a livello di host sono disponibili solo con. AWS Outposts Un gruppo di collocamento a livello di host può contenere tante istanze quanti sono gli host presenti nella distribuzione di Outpost. Per ulteriori informazioni, consulta the section called “Gruppi di posizionamento su AWS Outposts”.

Limitazioni e regole del gruppo di collocamento

Argomenti

- Regole e limitazioni generali
- Regole e limitazioni del gruppo di collocazione cluster
- Regole e limitazioni del gruppo di collocamento della partizione
- Regole e limitazioni del gruppo di collocamento sparso

Regole e limitazioni generali

Prima di utilizzare i gruppi di collocamento, tieni presente le regole seguenti:

- In ogni Regione puoi creare un massimo di 500 gruppi di posizionamento per account.
- Il nome specificato per un gruppo di collocazione deve essere univoco nell'account AWS per la regione.
- Non è possibile unire i gruppi di collocamento.
- È possibile avviare un'istanza in un gruppo di collocamento alla volta e l'istanza non può essere presente su più gruppi di collocamento.
- Le prenotazioni di capacità su richiesta e le istanze riservate zonali consentono di riservare la capacità per le istanze EC2 nelle zone di disponibilità. Quando avvii un'istanza, se gli attributi dell'istanza corrispondono a quelli specificati da una prenotazione di capacità su richiesta o da un'istanza riservata zonale, la capacità riservata viene utilizzata automaticamente dall'istanza. Questo vale anche se si avvia l'istanza in un gruppo di collocamento.

  Se intendi avviare le istanze in un gruppo di posizionamento del cluster, ti consigliamo di riservare la capacità in modo esplicito nel gruppo di posizionamento del cluster. È possibile farlo creando una prenotazione di capacità su richiesta in un gruppo di collocamento del cluster specificato. Tieni presente che, sebbene sia possibile prenotare la capacità in questo modo utilizzando le prenotazioni di capacità su richiesta, lo stesso non si può fare con le istanze riservate zonali in quanto non possono riservare la capacità in modo esplicito in un gruppo di collocamento.
- Non puoi eseguire l'avvio di host dedicati nei gruppi di posizionamento.
- Non puoi avviare un'istanza spot configurata per l'arresto o l'ibernazione in caso di interruzione in un gruppo di posizionamento.

Regole e limitazioni del gruppo di collocazione cluster

Ai gruppi di collocazione cluster si applicano le regole seguenti:

- Sono supportati i seguenti tipi di istanza:
  - Istanze della generazione attuale, ad eccezione delle istanze a prestazioni espandibili (ad esempio, T2), delle istanze Mac1 e delle istanze M7i-Flex.
  - Le seguenti istanze di generazione precedente: A1, C3, C4, I2, M4, R3 e R4.
- Un gruppo di collocazione cluster non può estendersi in più zone di disponibilità.

- La velocità effettiva massima di rete del traffico tra due istanze di un gruppo di collocazione cluster è limitata dall'istanza più lenta tra le due. Per le applicazioni con requisiti di velocità effettiva elevata, scegli un tipo di istanza con connettività di rete in grado di soddisfare i tuoi requisiti.
- Per i tipi di istanza abilitati per le reti avanzate, si applicano le seguenti regole:
  - Le istanze all'interno di un gruppo di collocazione cluster possono utilizzare fino a 10 Gbps per il traffico a flusso singolo. Le istanze che non si trovano all'interno di un gruppo di collocazione cluster possono utilizzare fino a 5 Gbps per il traffico di un flusso singolo.
  - Il traffico verso e dai bucket Amazon S3 all'interno della stessa regione sullo spazio dell'indirizzo IP pubblico o tramite un endpoint VPC può utilizzare tutta la larghezza di banda aggregata dell'istanza disponibile.
- Puoi avviare più tipi di istanza in un gruppo di collocazione cluster. Tuttavia, ciò riduce le probabilità che la capacità necessaria sia disponibile per garantire la riuscita dell'avvio. Consigliamo di utilizzare lo stesso tipo di istanza per tutte le istanze in un gruppo di collocazione cluster.
- Il traffico di rete verso Internet e tramite una AWS Direct Connect connessione a risorse locali è limitato a 5 Gbps per i gruppi di collocamento dei cluster.

Regole e limitazioni del gruppo di collocamento della partizione

Ai gruppi di collocamento di partizione si applicano le regole seguenti:

- Un gruppo di collocamento di partizione supporta al massimo sette partizioni per zona di disponibilità. Il numero di istanze avviabili in un gruppo di collocamento di partizione pe limitato solo dalle restrizioni vigenti nel proprio account.
- Quando si avviano istanze in un gruppo di collocamento di partizione, Amazon EC2 tenta di distribuirle in modo omogeneo in tutte le partizioni. Amazon EC2 non garantisce una distribuzione omogenea delle istanze in tutte le partizioni.
- Un gruppo di collocamento di partizione con Istanze dedicate può avere al massimo due partizioni.
- Le prenotazioni della capacità non riservano capacità in un gruppo di collocamento di partizione.

Regole e limitazioni del gruppo di collocamento sparso

Ai gruppi di collocamento sparsa si applicano le regole seguenti:

- Un gruppo di posizionamento sparso supporta fino a 7 istanze in esecuzione per ogni zona di disponibilità. Ad esempio, in una regione con tre zone di disponibilità, puoi eseguire fino a 21

istanze nel gruppo, con sette istanze in ogni zona di disponibilità. Se provi ad avviare un'ottava istanza nella stessa zona di disponibilità e nello stesso gruppo di collocamento sparsa, l'istanza non si avvia. Se occorrono più di 7 istanze in una zona di disponibilità, è preferibile utilizzare più gruppi di posizionamento sparso. L'utilizzo di più gruppi di posizionamento sparso non fornisce garanzie sulla distribuzione delle istanze tra gruppi, ma garantisce la distribuzione per ogni gruppo, limitando in tal modo l'impatto di determinate classi di errori.

- I gruppi di collocazione sparsa non sono supportati per le Istanze dedicate.
- I gruppi di collocamento distribuiti a livello di host sono supportati solo per i gruppi di collocamento su. AWS Outposts Un gruppo di spread placement a livello di host può contenere tante istanze quanti sono gli host presenti nella distribuzione di Outpost.
- In una regione, un gruppo di spread placement a livello di rack può avere un massimo di sette istanze in esecuzione per zona di disponibilità per gruppo. Inoltre AWS Outposts, un gruppo di spread placement a livello di rack può contenere tante istanze quanti sono i rack presenti nella distribuzione Outpost.
- Le prenotazioni della capacità non riservano capacità in un gruppo di collocamento sparso.

Lavorare con gruppi di collocamento

Indice

Creazione di un gruppo di collocamento

È possibile creare un gruppo di posizionamento utilizzando uno dei metodi descritti di seguito.

Console

Per creare un gruppo di collocazione tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Placement Groups (Gruppi di collocamento).
3. Scegli Crea gruppo di collocamento.
4. Specifica un nome per il gruppo.
5. Scegli la strategia di posizionamento per il gruppo.
   - Se scegli Spread (Sparso), scegli il livello di distribuzione.
     - Rack - senza restrizioni
     - Host - solo per Outposts
   - Se scegli Partition (Partizione), specifica il numero di partizioni all'interno del gruppo.
6. Per assegnare tag al gruppo di posizionamento, scegli Add tag (Aggiungi tag) e quindi inserisci una chiave e un valore. Scegli Aggiungi tag per ogni tag da aggiungere.
7. Seleziona Crea gruppo.

AWS CLI

Per creare un gruppo di collocamento utilizzando il AWS CLI

Utilizza il comando create-placement-group. Nell'esempio seguente viene creato un gruppo di collocazione denominato `my-cluster` che utilizza la strategia di collocazione `cluster` e viene applicato un tag con una chiave `purpose` e un valore pari a `production`.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --tag-specifications 'ResourceType=placement-
group,Tags={Key=purpose,Value=production}'
```

Per creare un gruppo di posizionamento delle partizioni utilizzando il AWS CLI

Utilizza il comando create-placement-group. Specificare il `--strategy` parametro con il valore `partition`, e specificare il `--partition-count` parametro con il numero desiderato di partizioni. In questo esempio, il gruppo di collocamento di partizione si chiama `HDFS-Group-A` e viene creato con cinque partizioni.

```
aws ec2 create-placement-group \
    --group-name HDFS-Group-A \
    --strategy partition \
    --partition-count 5
```

PowerShell

Per creare un gruppo di posizionamento utilizzando il AWS Tools for Windows PowerShell

Utilizza il comando New-EC2PlacementGroup.

Visualizzate le informazioni sul gruppo di collocamento

È possibile visualizzare tutti i gruppi di collocamento e le relative informazioni utilizzando uno dei seguenti metodi.

Console

Per visualizzare informazioni su uno o più gruppi di collocamento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, in Rete e sicurezza, scegliete Gruppi di posizionamento.
3. Nella tabella Gruppi di collocamento, per ogni gruppo di collocamento, è possibile visualizzare le seguenti informazioni:
   - Nome del gruppo: il nome che avete assegnato al gruppo di collocamento.
   - ID del gruppo: l'ID del gruppo di collocamento.
   - Strategia: la strategia di posizionamento per il gruppo di collocamento.
   - Stato: lo stato del gruppo di collocamento.
   - Partizione: il numero di partizioni. Valido solo se la strategia è la partizione.
   - ARN di gruppo: Amazon Resource Name (ARN) del gruppo di collocamento.

AWS CLI

Per descrivere tutti i tuoi gruppi di collocamento

Usa il describe-placement-groups AWS CLI comando.

```
aws ec2 describe-placement-groups
```

Example response

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster-pg",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789example",
            "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
        },
            ...
     ]
}
```

Per descrivere un gruppo di collocamento specificato

Utilizzate il describe-placement-groups AWS CLI comando. È possibile specificare il `--group-id` o il `--group-name` parametro.

Specificate l'ID del gruppo di posizionamento:

```
aws ec2 describe-placement-groups --group-id pg-0123456789example
```

Specificate il nome del gruppo di posizionamento:

```
aws ec2 describe-placement-groups --group-name my-cluster-pg
```

Example response

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster-pg",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789example",
            "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
```

```
        }
    ]
}
```

Tagging di un gruppo di collocamento

Per facilitare la categorizzazione e la gestione dei gruppi di collocamento esistenti, è possibile contrassegnarli con metadati personalizzati. Per ulteriori informazioni sul funzionamento dei tag, consultare Tagging delle risorse Amazon EC2..

Quando si contrassegna un gruppo di collocamento, le istanze avviate nel gruppo di collocamento non vengono contrassegnate automaticamente. È necessario contrassegnare esplicitamente le istanze avviate nel gruppo di collocamento. Per ulteriori informazioni, consulta Aggiunta di un tag all'avvio di un'istanza.

È possibile visualizzare, aggiungere e applicare tag utilizzando uno dei metodi descritti di seguito.

Console

Per visualizzare, aggiungere o eliminare un tag per un gruppo di collocamento esistente

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Placement Groups (Gruppi di collocamento).
3. Selezionare un gruppo di collocamento, quindi scegliere Actions (Operazioni), Manage tags (Gestisci tag).
4. Nella schermata Gestisci tag vengono visualizzati tutti i tag assegnati al gruppo di collocamento.
   - Per aggiungere un tag, scegliere Add tag (Aggiungi tag), quindi immettere la chiave e il valore del tag. È possibile aggiungere fino a 50 tag per gruppo di collocamento. Per ulteriori informazioni, consulta Limitazioni applicate ai tag.
   - Per eliminare un tag, scegli Remove (Rimuovi) accanto al tag che desideri eliminare.
5. Selezionare Salva.

AWS CLI

Per visualizzare i tag dei gruppi di collocamento

Utilizzare il comando describe-tags per visualizzare i tag per la risorsa specificata. Nell'esempio seguente vengono descritti i tag per tutti i gruppi di collocamento.

```
aws ec2 describe-tags \
    --filters Name=resource-type,Values=placement-group
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        },
        {
            "Key": "Environment",
            "ResourceId": "pg-9876543210EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
}
```

È inoltre possibile utilizzare il comando describe-tags per visualizzare i tag di un gruppo di collocamento specificandone l'ID. Nell'esempio seguente vengono descritti i tag per pg-0123456789EXAMPLE.

```
aws ec2 describe-tags \

    --filters Name=resource-id,Values=pg-0123456789EXAMPLE
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
}
```

È inoltre possibile visualizzare i tag di un gruppo di collocamento descrivendo il gruppo di collocamento.

Utilizzate il describe-placement-groupscomando per visualizzare la configurazione del gruppo di posizionamento specificato, che include tutti i tag specificati per il gruppo di posizionamento.

```
aws ec2 describe-placement-groups \
    --group-name my-cluster
```

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789EXAMPLE",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                }
            ]
        }
    ]
}
```

Per etichettare un gruppo di posizionamento esistente utilizzando il AWS CLI

Utilizzare il seguente comando create-tags per aggiungere un tag alle risorse esistenti. Nell'esempio seguente, il gruppo di posizionamento esistente è contrassegnato con `Key=Cost-Center` e `Value=CC-123`.

```
aws ec2 create-tags \
    --resources pg-0123456789EXAMPLE \
    --tags Key=Cost-Center,Value=CC-123
```

Per eliminare un tag da un gruppo di posizionamento utilizzando il AWS CLI

È possibile utilizzare il comando delete-tags per eliminare i tag dalle risorse esistenti. Per degli esempi, consulta Esempi in Riferimento ai comandi AWS CLI .

PowerShell

Per visualizzare i tag dei gruppi di collocamento

Utilizza il comando Get-EC2Tag.

Per descrivere i tag per un gruppo di collocamento specifico

Utilizza il comando Get-EC2PlacementGroup.

Per applicare tag a un gruppo di collocamento esistente

Utilizza il comando New-EC2Tag.

Come eliminare un tag da un gruppo di collocamento

Utilizza il comando Remove-EC2Tag.

Avvio di istanze in un gruppo di collocamento

È possibile avviare un'istanza in un gruppo di posizionamento se le regole e le limitazioni del gruppo di posizionamento sono soddisfatte utilizzando uno dei metodi descritti di seguito.

Console

Per avviare le istanze in un gruppo di collocamento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di controllo della console EC2, nella sezione Avvia istanza, scegli Avvia istanza. Completa il modulo come indicato, prestando attenzione alle seguenti operazioni:
   - Nella pagina Instance type (Scegli un tipo di istanza) seleziona un tipo di istanza che è possibile avviare in un gruppo di posizionamento.
   - Nella casella Summary (Riepilogo), in Number of instances (Numero di istanze), immetti il numero totale di istanze necessarie in questo gruppo di posizionamento, poiché potrebbe non essere possibile aggiungere istanze al gruppo di posizionamento in un secondo momento.
   - In Advanced details (Dettagli avanzati), per Placement group name (Nome gruppo di posizionamento), puoi scegliere di aggiungere l'istanza a un gruppo di posizionamento nuovo o esistente. Se scegli un gruppo di posizionamento con una strategia partizioni, per Target partition (Partizione di destinazione) scegli la partizione in cui avviare le istanze.

AWS CLI

Per avviare le istanze in un gruppo di collocamento

Utilizza il comando run-instances, quindi indica il gruppo di collocamento e la partizione utilizzando il parametro `--placement "GroupName = my-cluster"`. In questo esempio, il gruppo di posizionamento è denominato `my-cluster`.

```
aws ec2 run-instances --placement "GroupName = my-cluster"
```

Per avviare le istanze in una partizione specifica di un gruppo di posizionamento delle partizioni utilizzando il AWS CLI

Utilizza il comando run-instances, quindi indica il gruppo di collocamento e la partizione utilizzando il parametro `--placement "GroupName = HDFS-Group-A, PartitionNumber = 3"`. In questo esempio, il gruppo di collocamento di partizione si chiama `HDFS-Group-A` e le partizioni sono 3.

```
aws ec2 run-instances --placement "GroupName = HDFS-Group-A, PartitionNumber = 3"
```

PowerShell

Per avviare le istanze in un gruppo di collocamento tramite la AWS Tools for Windows PowerShell

Utilizzate il New-EC2Instancecomando e specificate il nome del gruppo di posizionamento utilizzando il parametro. `-Placement_GroupName`

Descrizione di istanze in un gruppo di collocamento

È possibile visualizzare le informazioni di posizionamento delle istanze utilizzando uno dei metodi descritti di seguito. È inoltre possibile filtrare i gruppi di posizionamento delle partizioni in base al numero di partizione utilizzando l'opzione AWS CLI.

Console

Per visualizzare il gruppo di collocamento e il numero di partizione di un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.

4. Nella scheda Details (Dettagli) in Host and placement group (Host e gruppo di collocamento), trovare Placement group (Gruppo di collocamento). Se l'istanza non si trova in un gruppo di collocamento, il campo sarà vuoto. In caso contrario, contiene il nome del nome del gruppo di collocamento. Se il gruppo di collocamento è un gruppo di collocamento di partizione, Partition number (Numero partizione) contiene il numero di partizione per l'istanza.

AWS CLI

Per visualizzare il numero di partizioni per istanza in un gruppo di posizionamento delle partizioni

Utilizza il comando describe-instances e indica il parametro `--instance-id`.

```
aws ec2 describe-instances --instance-id i-0123a456700123456
```

La risposta include le informazioni di collocamento, che a loro volta comprendono il nome del gruppo di collocamento e il numero di partizioni per l'istanza.

```
"Placement": {
     "AvailabilityZone": "us-east-1c",
     "GroupName": "HDFS-Group-A",
     "PartitionNumber": 3,
     "Tenancy": "default"
}
```

Per filtrare le istanze di un determinato gruppo di posizionamento delle partizioni e numero di partizioni

Utilizza il comando describe-instances e indica il parametro `--filters` con i filtri `placement-group-name` e `placement-partition-number`. In questo esempio, il gruppo di collocamento di partizione si chiama `HDFS-Group-A` e le partizioni sono 7.

```
aws ec2 describe-instances --filters "Name = placement-group-name, Values = HDFS-
Group-A" "Name = placement-partition-number, Values = 7"
```

Nella risposta sono elencate tutte le istanze incluse nella partizione specificata all'interno del gruppo di collocamento indicato. L'output seguente è un esempio in cui sono mostrati solo l'ID e il tipo di istanza e le informazioni di collocazione delle istanze restituite.

```
"Instances": [
               {
```

```
                "InstanceId": "i-0a1bc23d4567e8f90",
                "InstanceType": "r4.large",
                },

                "Placement": {
                    "AvailabilityZone": "us-east-1c",
                    "GroupName": "HDFS-Group-A",
                    "PartitionNumber": 7,
                    "Tenancy": "default"
                }

            {
                "InstanceId": "i-0a9b876cd5d4ef321",
                "InstanceType": "r4.large",
                },

                "Placement": {
                    "AvailabilityZone": "us-east-1c",
                    "GroupName": "HDFS-Group-A",
                    "PartitionNumber": 7,
                    "Tenancy": "default"
                }
        ],
```

Modifica del gruppo di collocamento per un'istanza

È possibile modificare il gruppo di collocamento per un'istanza in questo modo:

- Spostare un'istanza esistente in un gruppo di posizionamento
- Spostare un'istanza da un gruppo di posizionamento a un altro

Prima di poter spostare un'istanza, tale istanza deve trovarsi nello stato `stopped`.

Console

Per spostare un'istanza in un gruppo di collocamento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e poi scegli Stato istanza e Arresta istanza.

4. Con l'istanza selezionata, scegli Operazioni, Impostazioni istanza, Modifica posizionamento delle istanze.
5. Per Gruppo di collocamento, seleziona il gruppo di collocamento in cui spostare l'istanza.
6. Selezionare Salva.

AWS CLI

Per spostare un'istanza in un gruppo di collocamento

1. Arrestare l'istanza utilizzando il comando stop-istanze.
2. Utilizzate il modify-instance-placementcomando e specificate il nome del gruppo di posizionamento in cui spostare l'istanza.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup
```

3. Avviare l'istanza utilizzando il comando start-instances.

PowerShell

Per spostare un'istanza in un gruppo di collocazione tramite la AWS Tools for Windows PowerShell

1. Arrestate l'istanza utilizzando il Stop-EC2Instancecomando.
2. Utilizzate il Edit-EC2InstancePlacementcomando e specificate il nome del gruppo di posizionamento in cui spostare l'istanza.
3. Avviate l'istanza utilizzando il Start-EC2Instancecomando.

Rimuovere un'istanza da un gruppo di posizionamento

È possibile rimuovere un'istanza da un gruppo di posizionamento utilizzando uno dei metodi descritti di seguito.

Prima di poter rimuovere un'istanza da un gruppo di posizionamento, tale istanza deve trovarsi nello stato `stopped`.

Console

Per rimuovere un'istanza da un gruppo di posizionamento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza e poi scegli Stato istanza e Arresta istanza.
4. Con l'istanza selezionata, scegli Operazioni, Impostazioni istanza, Modifica posizionamento delle istanze.
5. Per Gruppo di collocamento, scegli Nessuno.
6. Selezionare Salva.

AWS CLI

Per rimuovere un'istanza da un gruppo di posizionamento

1. Arrestare l'istanza utilizzando il comando stop-istanze.
2. Utilizzate il modify-instance-placementcomando e specificate una stringa vuota per il nome del gruppo di posizionamento.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name ""
```

3. Avviare l'istanza utilizzando il comando start-instances.

PowerShell

Per rimuovere un'istanza da un gruppo di collocazione tramite la AWS Tools for Windows PowerShell

1. Arrestate l'istanza utilizzando il Stop-EC2Instancecomando.
2. Utilizzate il Edit-EC2InstancePlacementcomando e specificate una stringa vuota per il nome del gruppo di posizionamento.
3. Avviate l'istanza utilizzando il Start-EC2Instancecomando.

Eliminazione di un gruppo di collocamento

Puoi eliminare un gruppo di collocamento se devi sostituirlo o se non ti serve più. È possibile eliminare un gruppo di posizionamento utilizzando uno dei metodi descritti di seguito.

Prerequisito

Prima di poter eliminare un gruppo di posizionamento, non deve contenere istanze. È possibile terminare tutte le istanze avviate nel gruppo di collocamento, spostare le istanze avviate in un altro gruppo di collocamento oppure eliminarle dal gruppo di collocamento.

Console

Per eliminare un gruppo di collocamento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Placement Groups (Gruppi di collocamento).
3. Selezionare il gruppo di collocamento e scegliere Actions (Operazioni, Delete (Elimina).
4. Quando viene richiesta la conferma, immettere **`Delete`** e quindi scegliere Elimina.

AWS CLI

Per eliminare un gruppo di collocamento

Utilizzate il delete-placement-groupcomando e specificate il nome del gruppo di posizionamento per eliminare il gruppo di posizionamento. In questo esempio, il nome del gruppo di posizionamento è `my-cluster`.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Per eliminare un gruppo di posizionamento utilizzando il AWS Tools for Windows PowerShell

Utilizzate il Remove-EC2PlacementGroupcomando per eliminare il gruppo di posizionamento.

Condivisione di un gruppo di posizionamento

La condivisione del gruppo di collocamento consente di influenzare il posizionamento di istanze interdipendenti di proprietà di account separati AWS . Puoi condividere un gruppo di collocamento

tra più AWS account o all'interno delle tue organizzazioni. Puoi avviare istanze in un gruppo di posizionamento condiviso.

Il proprietario di un gruppo di posizionamento può condividere un gruppo di posizionamento con:

- AWS Account specifici all'interno o all'esterno della sua organizzazione
- Un'unità organizzativa all'interno dell'organizzazione
- L'intera organizzazione

> **Note**
>
> L' AWS account da cui desideri condividere un gruppo di collocamento deve disporre delle seguenti autorizzazioni nella policy IAM.
>
> - `ec2:PutResourcePolicy`
> - `ec2:DeleteResourcePolicy`

Argomenti

Regole e limitazioni

Le seguenti regole e limitazioni si applicano quando condividi un gruppo di posizionamento o quando un gruppo di posizionamento viene condiviso con te.

- Per condividere un gruppo di collocamento, devi possederlo nel tuo AWS account. Non puoi condividere un gruppo di posizionamento che è stato condiviso con te.
- Quando si condivide una partizione o un gruppo di posizionamento degli spread, i limiti del gruppo di posizionamento non cambiano. Un gruppo di posizionamento delle partizioni condiviso supporta

al massimo sette partizioni per zona di disponibilità, mentre un gruppo di posizionamento degli spread supporta un massimo di sette istanze in esecuzione per zona di disponibilità.

- Per condividere un gruppo di collocamento con la propria organizzazione o un'unità organizzativa all'interno dell'organizzazione, è necessario abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta la pagina Condivisione delle risorse AWS.
- La gestione delle istanze di tua proprietà in un gruppo di posizionamento condiviso è una tua responsabilità.
- Non è possibile visualizzare o modificare le istanze e le prenotazioni della capacità associate a un gruppo di posizionamento condiviso con te ma non di tua proprietà.

Condivisione tra zone di disponibilità

Per garantire che le risorse vengano distribuite tra le zone di disponibilità di una regione, mappiamo in modo indipendente le zone di disponibilità ai nomi per ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la zona `us-east-1a` di disponibilità del tuo AWS account potrebbe non avere la stessa posizione `us-east-1a` di un altro AWS account.

Per individuare la posizione dell'Host dedicati relativamente ai tuoi account, devi utilizzare l'ID della zona di disponibilità. L'ID della zona di disponibilità è un identificatore univoco e coerente per una zona di disponibilità in tutti gli account AWS . Ad esempio, `use1-az1` è un ID di zona di disponibilità per la regione `us-east-1` e identifica la stessa posizione in ogni account AWS .

Per visualizzare gli ID delle zone di disponibilità nel tuo account

1. Apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram.
2. Gli ID delle zone di disponibilità per la Regione corrente sono visualizzati nel pannello Your AZ ID (ID della tua AZ) nel riquadro destro.

Condivisione di un gruppo di posizionamento

Per condividere un gruppo di posizionamento, devi aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che consente di condividere le risorse tra AWS account. Un condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise.

Se fai parte di un'organizzazione, la AWS Organizations condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene concesso l'accesso al gruppo di collocamento condiviso.

Se il gruppo di collocamento è condiviso con un AWS account esterno all'organizzazione, il proprietario dell' AWS account riceverà un invito a partecipare alla condivisione delle risorse. Potrà accedere al gruppo di posizionamento condiviso dopo aver accettato l'invito.

Puoi condividere un gruppo di collocamento tra più AWS account utilizzando https://console.aws.amazon.com/ram oppure AWS CLI.

AWS RAM console

Per condividere un gruppo di posizionamento di tua proprietà utilizzando la https://console.aws.amazon.com/ram, consulta la pagina Creating a resource share (Creazione di una condivisione di risorse).

AWS CLI

Per condividere un gruppo di collocamento di tua proprietà, usa il create-resource-sharecomando.

Identificazione di un gruppo di posizionamento condiviso

L'Amazon Resource Name (ARN) di un gruppo di collocamento contiene l'ID account a 12 cifre dell'account proprietario del gruppo di collocamento. Puoi utilizzare l'ID dell'account per identificare il proprietario di un gruppo di collocamento condiviso con te.

È possibile trovare l'ARN del gruppo di collocamento utilizzando uno dei seguenti metodi. Per ulteriori informazioni, consulta Visualizzate le informazioni sul gruppo di collocamento.

Amazon EC2 console

Per identificare un gruppo di collocamento condiviso

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, in Rete e sicurezza, scegliete Gruppi di posizionamento.
3. La tabella Gruppi di collocamento elenca tutti i gruppi di collocamento di tua proprietà e condivisi con te. La colonna Group ARN mostra l'ARN del gruppo di collocamento.

Se la colonna Group ARN non è visibile, scegli settings
(
)
nell'angolo in alto a destra, attiva Group ARN e scegli Conferma.

AWS CLI

Per identificare un gruppo di collocamento condiviso

Usa `describe-placement-groups`il comando per elencare tutti i gruppi di collocamento che sono di tua proprietà e condivisi con te. Nella risposta, il `GroupId` parametro visualizza l'ARN di un gruppo di posizionamento.

Avvio di istanze in un gruppo di posizionamento condiviso

> **Important**
>
> Quando si utilizza il AWS CLI per avviare un'istanza in un gruppo di posizionamento condiviso, è necessario specificare l'ID del gruppo di posizionamento utilizzando il `GroupId` parametro.

Potete utilizzare il nome del gruppo di posizionamento solo se siete il proprietario del gruppo di posizionamento condiviso. Ti consigliamo di utilizzare l'ID del gruppo di collocamento per evitare potenziali collisioni tra i nomi del gruppo di collocamento tra AWS gli account.

Puoi trovare l'ID di un gruppo di collocamento nella console Amazon EC2 nella schermata Placement Groups o utilizzando il `describe-placement-groups` AWS CLI comando. Per ulteriori informazioni, consulta Visualizzate le informazioni sul gruppo di collocamento.

Console

Per avviare le istanze in un gruppo di collocamento condiviso

1. Seguite la procedura per avviare un'istanza, ma non avviate l'istanza prima di aver completato i seguenti passaggi per specificare le impostazioni per il gruppo di collocamento.
2. In Instance type (Tipo di istanza), seleziona un tipo di istanza supportato. Per ulteriori informazioni, consulta Limitazioni e regole del gruppo di collocamento.

3. Espandi i dettagli avanzati e configura le impostazioni del gruppo di collocamento come segue:

   a. Per Gruppo di collocamento, selezionate il gruppo di collocamento che è stato condiviso con voi.

   > **Note**
   >
   > Se ci sono gruppi di collocamento con lo stesso nome, controllate l'ID del gruppo di collocamento per assicurarvi di selezionare il gruppo di posizionamento corretto.

   b. Se scegliete un gruppo di collocamento con una strategia di partizione, per Target partition, scegliete la partizione in cui avviare l'istanza.

4. Nel pannello Riepilogo, effettuate le seguenti operazioni:

   a. Per Number of instances (Numero di istanze), immetti il numero totale di istanze necessarie in questo gruppo di collocamento, poiché potrebbe non essere possibile aggiungere le istanze al gruppo di collocamento in un secondo momento.

   b. Controlla la configurazione dell'istanza, quindi scegli Launch instance.

Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

AWS CLI

Avvio di istanze in un gruppo di posizionamento condiviso

Utilizzate il `run-instances` comando e specificate l'ID del gruppo di posizionamento condiviso.

```
aws ec2 run-instances —-placement "GroupId = pg-0123456789example"
```

Avvio di istanze in una partizione specifica di un gruppo di posizionamento delle partizioni condiviso

Utilizzate il `run-instances` comando e specificate l'ID del gruppo di posizionamento e il numero di partizione del gruppo di posizionamento condiviso.

```
aws ec2 run-instances –-placement "GroupId = pg-0123456789example, PartitionNumber
 = 3"
```

> **Tip**
>
> Utilizza il peering VPC per connettere istanze di proprietà di AWS account separati e ottenere tutti i vantaggi in termini di latenza offerti dai gruppi di collocamento di cluster condivisi. Per ulteriori informazioni, consulta Che cos'è il VPC in peering?

Annullamento della condivisione di un gruppo di posizionamento condiviso

Il proprietario del gruppo di posizionamento può annullare la condivisione di un gruppo di posizionamento condiviso in qualsiasi momento.

Quando annulli la condivisione di un gruppo di posizionamento condiviso, le modifiche seguenti avranno effetto.

- Gli AWS account con cui è stato condiviso un gruppo di collocamento non saranno più in grado di avviare istanze o riservare capacità.
- Se le tue istanze erano in esecuzione in un gruppo di posizionamento condiviso, verranno dissociate dal gruppo di posizionamento ma continueranno a funzionare normalmente nel tuo account AWS .
- Se disponevi di prenotazioni di capacità in un gruppo di collocamento condiviso, queste verranno dissociate dal gruppo di collocamento, ma continuerai ad accedervi nel tuo AWS account.

È possibile annullare la condivisione di un gruppo di posizionamento condiviso utilizzando uno dei metodi descritti di seguito.

AWS RAM console

Per annullare la condivisione di un gruppo di posizionamento condiviso utilizzando la https://console.aws.amazon.com/ram, consulta la pagina Deleting a resource share (Eliminazione di una condivisione di risorse).

AWS CLI

Per annullare la condivisione di un gruppo di collocamento condiviso utilizzando AWS Command Line Interface, utilizzate il disassociate-resource-sharecomando.

Gruppi di posizionamento su AWS Outposts

AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura, i servizi, le API e gli strumenti alle sedi dei clienti. Fornendo l'accesso locale all'infrastruttura AWS gestita, AWS Outposts consente ai clienti di creare ed eseguire applicazioni in locale utilizzando le stesse interfacce di programmazione AWS delle regioni, utilizzando al contempo risorse di elaborazione e archiviazione locali per esigenze di elaborazione dati locali e latenza inferiori.

Un Outpost è un pool di capacità di AWS elaborazione e archiviazione distribuito presso la sede di un cliente. AWS gestisce, monitora e gestisce questa capacità come parte di una regione. AWS

Puoi creare gruppi di posizionamento su outpost creati nel tuo account. In tal modo è possibile distribuire istanze sull'hardware sottostante su un outpost nel tuo sito. Puoi creare e utilizzare gruppo di posizionamento su outpost nella stessa maniera con cui crei e utilizzi gruppi di posizionamento in zone di disponibilità normali. Quando crei un gruppo di posizionamento con una strategia di diffusione su un outpost, puoi scegliere di distribuire le istanze del gruppo di posizionamento tra host o rack. La diffusione di istanze tra host consente di utilizzare una strategia di distribuzione con l'outpost di un singolo rack.

Considerazioni

- Un gruppo di spread placement a livello di rack può contenere tante istanze quanti sono i rack presenti nella distribuzione Outpost.
- Un gruppo di spread placement a livello di host può contenere tante istanze quanti sono gli host presenti nella distribuzione di Outpost.

Prerequisito

Devi avere un Outpost installato presso il tuo sito. Per ulteriori informazioni, consulta Creazione di un Outpost e ordinazione della capacità Outpost nella Guida per l'utente di AWS Outposts .

Per utilizzare un gruppo di posizionamento su un outpost

1. Creare una sottorete nell'Outpost. Per ulteriori informazioni, consulta Creazione di una sottorete nella Guida per l'utente di AWS Outposts .
2. Crea un gruppo di posizionamento nella regione dell'outpost associata. Se crei un gruppo di collocamento con una strategia di diffusione, puoi scegliere la distribuzione a livello di host o rack per determinare in che modo il gruppo distribuirà le istanze sull'hardware sottostante di Outpost. Per ulteriori informazioni, consulta the section called “Creazione di un gruppo di collocamento”.
3. Avvia un'istanza nel gruppo di posizionamento. Per Subnet (Sottorete) scegli la sottorete creata nel passaggio 1 e per Placement group name (Nome gruppo di posizionamento) seleziona il gruppo di posizionamento creato nel passaggio 2. Per ulteriori informazioni, consulta Avvio di un'istanza sull'Outpost nella Guida per l'utente di AWS Outposts .

Unità massima di trasmissione (MTU) di rete per istanza EC2

L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto maggiore consentito trasferibile attraverso la connessione. Maggiore è la MTU di una connessione, maggiore è la quantità di dati trasferibili in un unico pacchetto. I pacchetti Ethernet sono costituiti dal pacchetto o dai dati effettivi che invii e le informazioni sul sovraccarico della rete circostante.

I frame Ethernet possono presentarsi in diversi formati; il formato più comune è il formato di frame standard Ethernet v2. Supporta 1500 MTU, ovvero la dimensione del pacchetto Ethernet maggiore supportata nella maggior parte di Internet. La MTU massima supportata per un'istanza dipende dal tipo di istanza.

Le seguenti regole si applicano alle istanze che si trovano nelle zone di Wavelength:

- Il traffico che va da un'istanza all'altra all'interno di un VPC nella stessa zona di Wavelength ha un MTU pari a 1300.
- Il traffico che va da un'istanza all'altra che utilizza l'IP portante all'interno di una zona Wavelength ha un MTU pari a 1500.
- Il traffico che va da un'istanza all'altra tra una zona di Wavelength e la regione che utilizza un indirizzo IP pubblico ha un MTU pari a 1500.
- Il traffico che va da un'istanza all'altra tra una zona di Wavelength e la regione che utilizza un indirizzo IP privato ha un MTU pari a 1300.

Le seguenti regole si applicano alle istanze che si trovano in Outposts:

- Il traffico che va da un'istanza in Outposts a un'istanza nella regione ha un MTU pari a 1300.

Indice

Frame jumbo (9001 MTU)

I frame jumbo consentono più di 1500 byte di dati aumentando la dimensione di payload per pacchetto, aumentando quindi la percentuale del pacchetto che non suppone un sovraccarico del pacchetto. È quindi necessario un numero minore di pacchetti per inviare la stessa quantità di dati utilizzabili. Tuttavia, il traffico è limitato a un MTU massimo di 1500 nei seguenti casi:

- Traffico su un gateway Internet
- Traffico su una connessione di peering VPC tra regioni
- Traffico su connessioni VPN
- Traffico al di fuori di una determinata AWS regione

Se i pacchetti sono maggiori di 1500 byte, vengono frammentati o interrotti se è impostato il flag `Don't Fragment` nell'intestazione IP.

I frame jumbo devono essere utilizzati con cautela per il traffico vincolato a Internet o qualsiasi traffico che esca da un VPC. I pacchetti vengono frammentati da sistemi intermedi, i quali rallentano tale traffico. Per utilizzare i frame jumbo all'interno di un VPC e non rallentare il traffico vincolato al di fuori del VPC, puoi configurare la dimensione della MTU in base alla route oppure puoi utilizzare più interfacce di rete elastica con diverse dimensioni dell'MTU e diverse route.

Per le istanze collocate in un gruppo di collocazione cluster, i frame jumbo aiutano a raggiungere il massimo throughput della rete possibile, per cui li consigliamo in questo caso. Per ulteriori informazioni, consulta Gruppi di collocamento.

È possibile utilizzare i frame jumbo per il traffico tra i VPC e le proprie reti locali su AWS Direct Connect. Per ulteriori informazioni e per verificare la funzionalità Jumbo Frame, consulta Impostazioni MTU di rete nella Guida per l'utente di AWS Direct Connect .

Tutti i tipi di istanze Amazon EC2 supportano 1500 MTU e tutti i tipi di istanza della generazione attuale supportano i jumbo frame. I seguenti tipi di istanza della generazione precedente supportano i jumbo frame: A1, C3, I2, M3 e R3.

Per ulteriori informazioni sulle dimensioni delle MTU supportate:

- Per configurare gateway NAT, consulta Nozioni di base di Gateway NAT nella Guida per l'utente di Amazon VPC.
- Per i gateway di transito, consulta la pagina MTU nella Guida per l'utente di Amazon VPC Transit Gateway.
- Per le zone locali, consulta Considerazioni nella Guida per l'utente delle zone locali AWS .

Rilevamento della MTU del percorso

Il rilevamento della MTU del percorso (PMTUD) è utilizzato per determinare la MTU del percorso tra due dispositivi. La MTU del percorso è la dimensione massima del pacchetto che è supportata nel percorso tra l'host di origine e quello ricevente. In presenza di una differenza della dimensione della MTU nella rete tra due host, PMTUD consente all'host ricevente di rispondere all'host di origine con un messaggio ICMP. Questo messaggio ICMP indica all'host di origine di utilizzare la dimensione della MTU più piccola sul percorso di rete per inviare nuovamente la richiesta. Senza questa negoziazione, può verificarsi la perdita del pacchetto perché la richiesta è troppo grande per l'host ricevente.

Per IPv4, se un host invia un pacchetto più grande della MTU dell'host ricevente o della MTU di un dispositivo lungo il percorso, l'host o il dispositivo ricevente rifiuta il pacchetto e restituisce il seguente messaggio ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, Codice 4). Questo indica all'host trasmittente di dividere il payload in più pacchetti più piccoli e quindi di trasmetterli di nuovo.

Il protocollo IPv6 non supporta la frammentazione nella rete. Se un host invia un pacchetto più grande della MTU dell'host ricevente o della MTU di un dispositivo lungo il percorso, l'host o il

dispositivo ricevente elimina il pacchetto e restituisce il seguente messaggio ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Questo indica all'host trasmittente di dividere il carico in più pacchetti più piccoli e quindi di trasmetterli di nuovo.

Le connessioni effettuate tramite alcuni componenti, come i gateway NAT e i sistemi di bilanciamento del carico, sono monitorati automaticamente. Ciò significa che il monitoraggio dei gruppi di sicurezza viene abilitato automaticamente per i tentativi di connessione in uscita. Se le connessioni vengono monitorate automaticamente o se le regole del gruppo di sicurezza consentono il traffico ICMP in entrata, puoi ricevere risposte PMTUD.

Tieni presente che il traffico ICMP può essere bloccato anche se è consentito a livello di gruppo di sicurezza, ad esempio se hai una voce della lista di controllo degli accessi alla rete che nega il traffico ICMP alla sottorete.

> **Important**
>
> Il rilevamento della MTU del percorso non garantisce che i frame jumbo non vengano interrotti da alcuni router. Un Internet gateway nel tuo VPC invia pacchetti fino a soli 1500 byte. Consigliamo pacchetti di 1500 MTU per il traffico Internet.

Verifica della MTU del percorso tra due host

Puoi controllare il percorso MTU tra l'istanza EC2 e un altro host. È possibile specificare un nome DNS o un indirizzo IP come destinazione. Se la destinazione è un'altra istanza EC2, verifica che il relativo gruppo di sicurezza consenta il traffico UDP in entrata.

La procedura da utilizzare dipende dal sistema operativo dell'istanza.

Istanze Linux

Esegui il tracepath comando sull'istanza per verificare il percorso MTU tra l'istanza EC2 e la destinazione specificata. Questo comando fa parte del `iputils` pacchetto, disponibile per impostazione predefinita in molte distribuzioni Linux.

Questo esempio controlla il percorso MTU tra l'istanza EC2 e. `amazon.com`

```
[ec2-user ~]$ tracepath amazon.com
```

In questo output di esempio, il percorso MTU è 1500.

```
 1?: [LOCALHOST]     pmtu 9001
 1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  100.64.16.241 (100.64.16.241)                             0.574ms
 5:  72.21.222.221 (72.21.222.221)                            84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                          79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                            96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                            79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                          91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

Istanze Windows

Per controllare il percorso MTU usando mturoute

1. Scaricalo sulla tua mturoute.exe istanza EC2 da http://www.elifulkerson.com/projects/mturoute.php.
2. Aprire una finestra del prompt dei comandi e passare alla directory in cui è stato scaricato mturoute.exe.
3. Utilizza il seguente comando per verificare il percorso MTU tra l'istanza EC2 e la destinazione specificata. Questo esempio controlla il percorso MTU tra l'istanza EC2 e. `www.elifulkerson.com`

   ```
   .\mturoute.exe www.elifulkerson.com
   ```

   In questo output di esempio, il percorso MTU è 1500.

   ```
   * ICMP Fragmentation is not permitted. *
   * Speed optimization is enabled. *
   * Maximum payload is 10000 bytes. *
   + ICMP payload of 1472 bytes succeeded.
   - ICMP payload of 1473 bytes is too big.
   Path MTU: 1500 bytes.
   ```

Controlla l'MTU per la tua istanza

Puoi controllare il valore MTU per la tua istanza. Alcune istanze sono configurate per l'utilizzo di frame jumbo, mentre altre sono configurate per l'utilizzo di dimensioni di frame standard.

La procedura da utilizzare dipende dal sistema operativo dell'istanza.

Istanze Linux

Verifica dell'impostazione della MTU su un'istanza Linux

Esegui il ip comando seguente sulla tua istanza EC2. Se l'interfaccia di rete principale non lo è`eth0`, sostituiscila `eth0` con la tua interfaccia di rete.

```
[ec2-user ~]$ ip link show eth0
```

In questo output di esempio, *`mtu 9001`* indica che l'istanza utilizza i jumbo frame.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
 DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

Istanze Windows

La procedura da utilizzare dipende dal driver dell'istanza.

ENA driver

Versione 2.1.0 e successive

Per ottenere il valore MTU, usa il seguente Get-NetAdapterAdvancedProperty comando sulla tua istanza EC2. Usa la wildcard (asterisco) per ottenere tutti i nomi Ethernet. Controllate l'output per il nome dell'interfaccia. `*JumboPacket` Un valore di 9015 indica che i frame jumbo sono abilitati. I frame jumbo sono disabilitati per impostazione predefinita.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Versione 1.5 e precedenti

Per ottenere il valore MTU, usa il seguente Get-NetAdapterAdvancedProperty comando sulla tua istanza EC2. Controlla l'output per il nome dell'interfaccia. `MTU` Un valore di 9001 indica che i frame jumbo sono abilitati. I frame jumbo sono disabilitati per impostazione predefinita.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Per ottenere il valore MTU, usa il seguente Get-NetAdapterAdvancedProperty comando sulla tua istanza EC2. Verificare la voce del nome dell'interfaccia `*JumboPacket`. Un valore di 9014 indica che i frame jumbo sono abilitati. Tieni presente che la dimensione della MTU include l'intestazione e il payload. I frame jumbo sono disabilitati per impostazione predefinita.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Per ottenere il valore MTU, usa il seguente comando sulla tua istanza EC2. Il nome dell'interfaccia può variare. Nell'output, cercare una voce denominata "Ethernet", "Ethernet 2" o "Local Area Connection". Il nome dell'interfaccia sarà necessario per abilitare o disabilitare i frame jumbo. Un valore di 9001 indica che i frame jumbo sono abilitati.

```
netsh interface ipv4 show subinterface
```

Imposta l'MTU per la tua istanza

Potresti voler utilizzare i frame jumbo per il traffico di rete all'interno del tuo VPC e i frame standard per il traffico Internet. Qualunque sia il tuo caso d'uso, ti consigliamo di verificare che l'istanza si comporti come previsto.

La procedura da utilizzare dipende dal sistema operativo dell'istanza.

Istanze Linux

Impostazione del valore della MTU su un'istanza Linux

1. Esegui il ip comando seguente sulla tua istanza. Imposta il valore MTU desiderato su 1500, ma puoi invece usare 9001.

   ```
   [ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
   ```

2. (Opzionale) Per mantenere l'impostazione della MTU della rete dopo un riavvio, modificare i file di configurazione seguenti, in base al tipo di sistema operativo.

- Nel caso di Amazon Linux 2, aggiungere la seguente riga al file `/etc/sysconfig/network-scripts/ifcfg-eth0`:

  ```
  MTU=1500
  ```

  Aggiungere la seguente riga al file `/etc/dhcp/dhclient.conf`:

  ```
  request subnet-mask, broadcast-address, time-offset, routers, domain-name,
   domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-
  servers;
  ```

- Per l'AMI Amazon Linux, aggiungi le seguenti righe al tuo `/etc/dhcp/dhclient-eth0.conf` file.

  ```
  interface "eth0" {
  supersede interface-mtu 1500;
  }
  ```

- Per altre distribuzioni di Linux, consultare la documentazione specifica.

3. (Opzionale) Riavviare l'istanza e verificare che l'impostazione della MTU sia corretta.

Istanze Windows

La procedura da utilizzare dipende dal driver dell'istanza.

ENA driver

È possibile modificare l'MTU utilizzando Device Manager o il Set-NetAdapterAdvancedProperty comando sull'istanza.

Versione 2.1.0 e successive

Utilizzate il seguente comando per abilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9015
```

Utilizzate il seguente comando per disabilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

Versione 1.5 e precedenti

Utilizzate il seguente comando per abilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 9001
```

Utilizzate il seguente comando per disabilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 1500
```

Intel SRIOV 82599 driver

È possibile modificare l'MTU utilizzando Device Manager o il Set-NetAdapterAdvancedProperty comando sull'istanza.

Utilizzate il seguente comando per abilitare i jumbo frame.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9014
```

Utilizzate il seguente comando per disabilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

AWS PV driver

È possibile modificare l'MTU utilizzando il netsh comando sulla tua istanza. Non è possibile modificare l'MTU utilizzando Device Manager.

Utilizzate il seguente comando per abilitare i jumbo frame.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Utilizzate il seguente comando per disabilitare i frame jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Risoluzione dei problemi

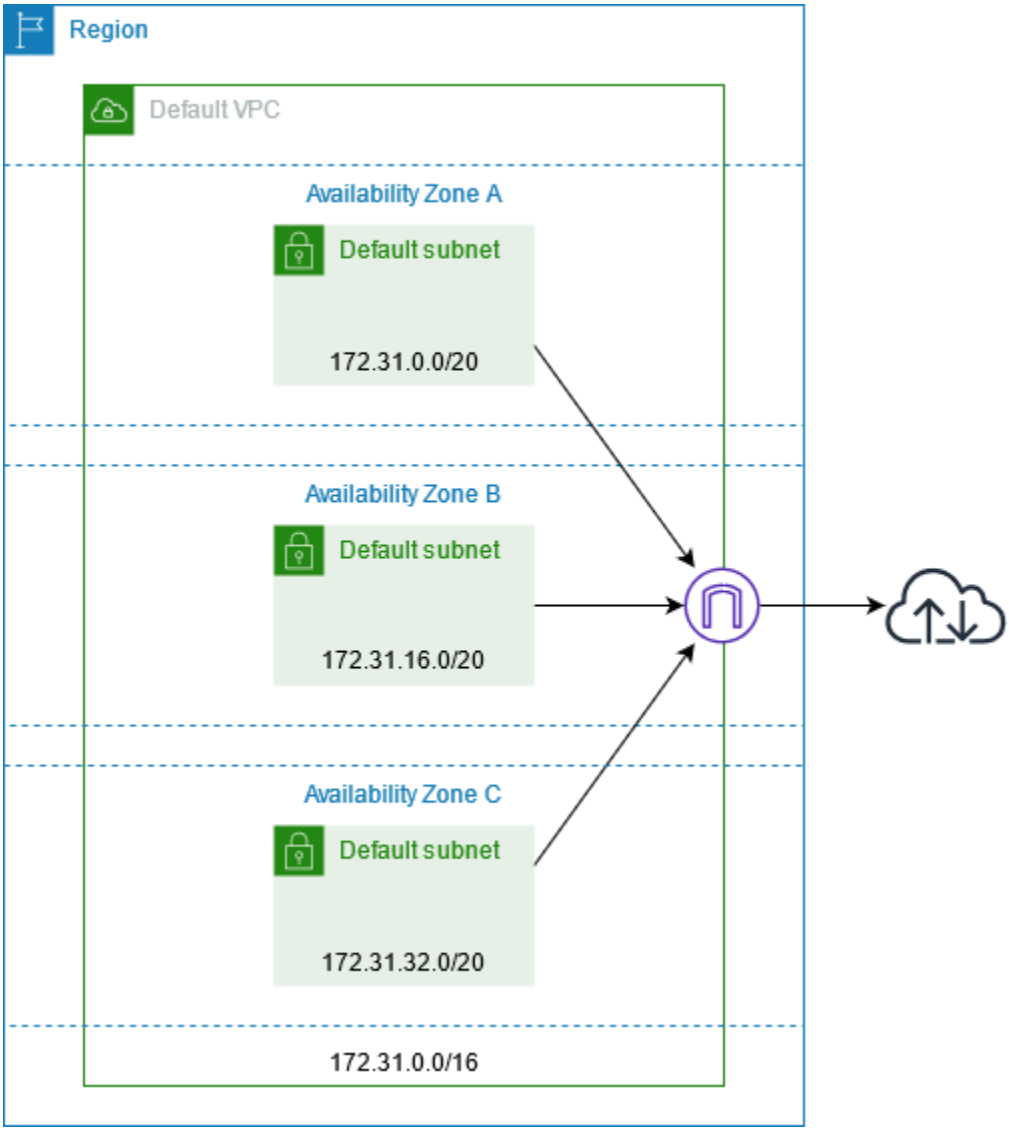
Se riscontri problemi di connettività tra la tua istanza EC2 e un cluster Amazon Redshift quando usi i jumbo frame, consulta Queries Appear to Hang nella Amazon Redshift Management Guide.

Cloud privati virtuali per le tue istanze EC2

Amazon Virtual Private Cloud (Amazon VPC) ti consente di definire una rete virtuale nella tua area logicamente isolata all'interno del AWS cloud, nota come cloud privato virtuale o VPC. Puoi creare AWS risorse, come istanze Amazon EC2, nelle sottoreti del tuo VPC. Il VPC è molto simile a una rete tradizionale gestibile nel data center locale, ma con i vantaggi legati all'utilizzo dell'infrastruttura scalabile di AWS. Puoi configurare il VPC, selezionare l'intervallo di indirizzi IP, creare sottoreti e configurare tabelle di routing, gateway di rete e impostazioni di sicurezza. È possibile connettere le istanze del VPC a Internet o al proprio data center.

I tuoi VPC predefiniti

Quando crei il tuo AWS account, creiamo un VPC predefinito in ogni regione. Un VPC predefinito è un VPC già configurato e pronto all'uso. Ad esempio, esiste una sottorete di default per ciascuna zona di disponibilità in ogni VPC predefinito, un gateway Internet allegato al VPC e nella tabella di routing principale è presente un percorso che invia tutto il traffico (0.0.0.0/0) al Gateway Internet. In alternativa, puoi creare il tuo VPC e configurarlo in base alle esigenze.



Creazione di VPC aggiuntivi

Utilizza la procedura seguente per creare un VPC con la configurazione di sottoreti, gateway e instradamenti di cui hai bisogno.

Per creare un VPC

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Seleziona Crea VPC.
3. Per Resources to create (Risorse da creare), scegli VPC and more (VPC e altro).
4. Per Name tag auto-generation (Generazione automatica di tag nome), immetti un nome per il VPC.

5. Per il blocco CIDR IPv4, mantieni il suggerimento predefinito o inserisci il blocco CIDR richiesto dall'applicazione o dalla rete.
6. Per Number of Availability Zones (Numero di zone di disponibilità), scegli 2, in modo da poter avviare le istanze in più zone di disponibilità per garantire un'elevata disponibilità.
7. Se le istanze devono essere accessibili da Internet, procedi in uno dei seguenti modi:
   - Se le tue istanze possono trovarsi in una sottorete pubblica, seleziona un valore diverso da zero per Number of public subnets (Numero di sottoreti pubbliche). Mantieni selezionate entrambe le opzioni in DNS options (Opzioni DNS). Facoltativamente, puoi aggiungere sottoreti private adesso o in seguito.
   - Se le tue istanze devono trovarsi in una sottorete privata, seleziona 0 per Number of public subnets (Numero di sottoreti pubbliche). Per Number of private subnets (Numero di sottoreti private), seleziona un numero in base alle tue esigenze (i valori possibili corrispondono a 1 o 2 sottoreti private per zona di disponibilità). Per i NAT gateways (Gateway NAT), se le istanze in entrambe le zone di disponibilità inviano o ricevono un volume significativo di traffico tra le zone di disponibilità, seleziona 1 per AZ. Altrimenti, seleziona In 1 AZ e avvia le istanze che inviano o ricevono traffico interzona nella stessa zona di disponibilità del gateway NAT.
8. Espandi Customize subnet CIDR blocks (Personalizza i blocchi CIDR della sottorete). Mantieni i suggerimenti predefiniti o inserisci un blocco CIDR per ogni sottorete. Per ulteriori informazioni, consulta Blocchi CIDR della sottorete nella Guida per l'utente di Amazon VPC.
9. Esamina il riquadro di anteprima, in cui sono visualizzate le risorse VPC che verranno create in base alle tue selezioni.
10. Seleziona Crea VPC.

Accesso a Internet dalle istanze

Le istanze avviate in una sottorete predefinita in un VPC predefinito hanno accesso a Internet, poiché i VPC predefiniti sono configurati per assegnare indirizzi IP pubblici e nomi host DNS e la tabella di routing principale è configurata con un percorso verso un gateway Internet collegato al VPC.

Per le istanze che avvii in sottoreti e VPC non predefiniti, puoi utilizzare una delle seguenti opzioni per assicurarti che le istanze che avvii in queste sottoreti abbiano accesso a Internet:

- Configurazione di un gateway Internet. Per ulteriori informazioni, consulta Collegamento delle sottoreti a Internet tramite un gateway Internet nella Guida per l'utente di Amazon VPC.

- Configurazione di un Gateway NAT pubblico. Per ulteriori informazioni, consulta Accesso a Internet da una sottorete privata nella Guida per l'utente di Amazon VPC.

Sottoreti condivise

Quando avvii istanze EC2 in sottoreti VPC condivise, tieni presente quanto segue:

- I partecipanti possono eseguire istanze in una sottorete condivisa specificando l'ID della sottorete condivisa. I partecipanti devono possedere tutti i gruppi di sicurezza o le interfacce di rete da loro specificati.
- I partecipanti possono avviare, interrompere, terminare e descrivere le istanze che hanno creato in una sottorete condivisa. I partecipanti non possono avviare, interrompere, terminare o descrivere le istanze create dal proprietario del VPC nella sottorete condivisa.
- I proprietari di VPC non possono avviare, interrompere, terminare o descrivere le istanze create dai partecipanti in una sottorete condivisa.
- I partecipanti possono connettersi a un'istanza in una sottorete condivisa utilizzando EC2 Instance Connect Endpoint. Il partecipante deve creare l'endpoint EC2 Instance Connect nella sottorete condivisa. I partecipanti non possono utilizzare un endpoint EC2 Instance Connect creato dal proprietario del VPC nella sottorete condivisa.

Per ulteriori informazioni, consulta Condivisione del VPC con altri account nella Guida per l'utente di Amazon VPC.

Sottoreti solo IPv6

Un'istanza EC2 avviata in una sottorete solo IPv6 riceve un indirizzo IPv6 ma non un indirizzo IPv4. Tutte le istanze che avvii in una sottorete solo IPv6 devono essere istanze create sul sistema Nitro. AWS

Sicurezza in Amazon EC2

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili ad Amazon EC2, consulta AWS Services in Scope by Compliance Program Program.
- Sicurezza nel cloud - La tua responsabilità include le seguenti aree.
  - Controllo dell'accesso di rete alle istanze, ad esempio mediante la configurazione del VPC e dei gruppi di sicurezza. Per ulteriori informazioni, consulta Controllo del traffico di rete.
  - Gestione delle credenziali utilizzate per connettersi alle istanze.
  - Gestione del sistema operativo guest e del software distribuiti nel sistema operativo guest, inclusi aggiornamenti e patch di sicurezza. Per ulteriori informazioni, consulta Gestione degli aggiornamenti per le istanze Windows di Amazon EC2.
  - Configurazione dei ruoli IAM collegati all'istanza e le autorizzazioni associate a tali ruoli. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Amazon EC2. Viene illustrato come configurare Amazon EC2 per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon EC2.

Indice

- Identity and Access Management per Amazon EC2
- Accesso ad Amazon EC2 utilizzando un endpoint VPC di interfaccia
- Gestione degli aggiornamenti per le istanze Windows di Amazon EC2
- Procedure consigliate di sicurezza per le istanze Windows
- Coppie di chiavi Amazon EC2 e istanze Amazon EC2
- Gruppi di sicurezza Amazon EC2 per le tue istanze EC2
- NitroTPM
- Credential Guard per istanze Windows

Protezione dei dati in Amazon EC2

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei dati in Amazon Elastic Compute Cloud. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon EC2 o altro Servizi AWS utilizzando la console, l'API o AWS gli AWS CLI SDK. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Indice

Sicurezza dei dati di Amazon EBS

I volumi di Amazon EBS sono presentati come dispositivi a blocchi non elaborati e non formattati. Sono dispositivi logici creati sull'infrastruttura EBS e il servizio Amazon EBS garantisce che siano logicamente vuoti (ovvero che i blocchi non elaborati vengano azzerati o contengano dati crittograficamente pseudocasuali) prima di qualsiasi utilizzo o riutilizzo da parte di un cliente.

Se disponi di procedure che richiedono la cancellazione di tutti i dati usando un metodo specifico, dopo o prima dell'utilizzo (o in entrambi i casi), come quelli indicati in modo dettagliato in DoD 5220.22-M (National Industrial Security Program Operating Manual, Manuale operativo del programma nazionale di sicurezza industriale) o NIST 800-88 (Guidelines for Media Sanitization, Linee guida per la sanificazione dei supporti), hai la possibilità di eseguire questa operazione su Amazon EBS. Tale attività a livello di blocco si rifletterà sui supporti di archiviazione sottostanti all'interno del servizio Amazon EBS.

Crittografia a riposo

Volumi EBS

La crittografia Amazon EBS è una soluzione di crittografia per i volumi e gli snapshot EBS che utilizza AWS KMS keys. Per ulteriori informazioni, consulta Amazon EBS encryption nella Amazon EBS User Guide.

[Istanze Windows] È inoltre possibile utilizzare le autorizzazioni Microsoft EFS e NTFS per la crittografia a livello di cartelle e file.

Volumi di archivio dell'istanza

I dati sui volumi di archivio istanza NVMe sono crittografati utilizzando una cifratura XTS-AES-256 implementata su un modulo hardware sull'istanza. Le chiavi utilizzate per crittografare i dati scritti sui dispositivi di archiviazione NVMe collegati localmente sono per cliente e per volume. Le chiavi sono generate e risiedono solo all'interno del modulo hardware, che è inaccessibile al personale AWS . Quando l'istanza viene arrestata o terminata, le chiavi crittografiche vengono distrutte e non possono essere ripristinate. Non è possibile disattivare questa cifratura e non è possibile fornire una propria chiave crittografica.

I dati sui volumi di archivio istanza HDD nelle istanze H1, D3 e D3en vengono crittografati utilizzando XTS-AES-256 e chiavi monouso.

Quando arresti, sospendi o termini un'istanza, ogni blocco di archiviazione nel volume dell'archivio istanza viene ripristinato. Pertanto, non è possibile accedere ai dati attraverso l'instance store di un'altra istanza.

Memoria

La crittografia della memoria è abilitata nelle seguenti istanze:

- Istanze con processori Graviton. AWS AWS Graviton2, AWS Graviton3 e Graviton3E supportano la crittografia della memoria sempre attiva. AWS Le chiavi di crittografia vengono generate in modo sicuro all'interno del sistema host, non lasciano il sistema host e vengono distrutte quando l'host viene riavviato o spento. Per ulteriori informazioni, consulta la pagina Processori AWS Graviton.
- Istanze con processori scalabili Intel Xeon di terza generazione (Ice Lake), come le istanze M6i, e processori scalabili Intel Xeon di quarta generazione (Sapphire Rapids), come le istanze M7i. Questi processori supportano la crittografia della memoria sempre attiva utilizzando Intel Total Memory Encryption (TME).
- Istanze con processori AMD EPYC di terza generazione (Milan), come le istanze M6a, e processori AMD EPYC di quarta generazione (Genoa), come le istanze M7a. Questi processori supportano la crittografia della memoria sempre attiva utilizzando AMD Secure Memory Encryption (SME). Le istanze con processori AMD EPYC di terza generazione (Milan) supportano anche AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP).

Crittografia in transito

Crittografia a livello fisico

Tutti i dati che fluiscono tra le AWS regioni sulla rete AWS globale vengono automaticamente crittografati a livello fisico prima di lasciare le strutture protette. AWS Tutto il traffico tra le AZ è crittografato. Ulteriori livelli di crittografia, inclusi quelli elencati in questa sezione, possono fornire ulteriore protezione.

Crittografia fornita dal peering Amazon VPC e dal peering transregionale Transit Gateway

Tutto il traffico interregionale che utilizza il peering Amazon VPC e il peering Transit Gateway viene automaticamente crittografato in blocco quando esce da una regione. Un ulteriore livello di crittografia viene fornito automaticamente a livello fisico per tutto il traffico prima che lasci le strutture AWS protette, come indicato in precedenza in questa sezione.

Crittografia tra istanze

AWS fornisce una connettività sicura e privata tra istanze EC2 di tutti i tipi. Inoltre, alcuni tipi di istanza utilizzano le funzionalità di offload dell'hardware Nitro System sottostante per crittografare automaticamente il traffico in transito tra le istanze. Questa crittografia utilizza algoritmi AEAD (Authenticated Encryption with Associated Data), con crittografia a 256 bit. Non vi è alcun impatto sulle prestazioni della rete. Per supportare questa crittografia aggiuntiva del traffico in transito tra istanze, è necessario soddisfare i seguenti requisiti:

- Le istanze utilizzano i seguenti tipi di istanza:
  - Scopo generale: M5dn, M5n, M5zn, M6a, M6i, M6iD, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-Flex
  - Elaborazione ottimizzata: C5a, C5ad, C5n, C6a, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-flex
  - Memoria ottimizzata: R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7g, R7gd, R7i, R7iZ, R8g, U-3TB1, U-6TB1, U-9TB1, U-18TB1, U7i-12 TB1, U7i-12 TB1, U7i-12 TB1, U7I-12 TB, U7 TB1 16 TB, U7 in 24 TB, U7 in 32 TB, X2IDN, X2iEDN, X2IEZn
  - Archiviazione ottimizzata: D3, D3en, I3en, i4G, i4i, Im4gn, IS4Gen
  - Elaborazione accelerata: DL1, DL2q, G4ad, G4dn, G5, G6, Gr6, Inf1, Inf2, P3dn, P4d, P4de, P5, Trn1, Trn1n, VT1
  - High Performance Computing: Hpc6a, Hpc6id, Hpc7a, Hpc7g
- Le istanze si trovano nella stessa regione.
- Le istanze si trovano nello stesso VPC o VPC con peering e il traffico non passa attraverso un dispositivo di rete virtuale, ad esempio un load balancer (load balancer) o un Transit Gateway.

Un ulteriore livello di crittografia viene fornito automaticamente a livello fisico per tutto il traffico prima che lasci le strutture protette, come indicato in precedenza in questa sezione. AWS

Per visualizzare i tipi di istanza che crittografano il traffico in transito tra istanze utilizzando la AWS CLI

Utilizza il seguente comando della describe-instance-types.

```
aws ec2 describe-instance-types \
    --filters Name=network-info.encryption-in-transit-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Crittografia da e verso AWS Outposts

Un Outpost crea connessioni di rete speciali chiamate collegamenti di servizio alla sua regione di AWS origine e, facoltativamente, connettività privata a una sottorete VPC specificata dall'utente. Tutto il traffico su tali connessioni è completamente crittografato. Per ulteriori informazioni, consulta Connettività tramite collegamenti per servizio e Crittografia in transito nella Guida per l'utente di AWS Outposts .

Crittografia dell'accesso remoto

I protocolli SSH e RDP forniscono canali di comunicazione sicuri per l'accesso remoto alle istanze, direttamente o tramite EC2 Instance Connect. L'accesso remoto alle istanze tramite AWS Systems Manager Session Manager o Run Command è crittografato utilizzando TLS 1.2 e le richieste di creazione di una connessione sono firmate utilizzando SigV4, autenticate e autorizzate da. AWS Identity and Access Management

È responsabilità dell'utente utilizzare un protocollo di crittografia quale Transport Layer Security (TLS) per eseguire la crittografia dei dati sensibili in transito tra i client e le istanze Amazon EC2.

(Istanze Windows) Assicurati di consentire solo le connessioni crittografate tra le istanze EC2 e gli endpoint AWS API o altri servizi di rete remoti sensibili. È possibile applicare questa operazione tramite un gruppo di sicurezza in uscita o regole di Windows Firewall.

Sicurezza dell'infrastruttura in Amazon EC2

In quanto servizio gestito, Amazon Elastic Compute Cloud è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura,

consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad Amazon EC2 attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Per ulteriori informazioni, vedere Infrastructure Protection in the Security Pillar — AWS Well-Architected Framework.

Isolamento della rete

Un cloud privato virtuale (VPC) è una rete virtuale nella propria area logicamente isolata nel cloud. AWS Utilizza VPC separati per isolare l'infrastruttura in base a carico di lavoro o entità dell'organizzazione.

Una sottorete è un intervallo di indirizzi IP in un VPC. Quando avvii un'istanza, questa operazione viene eseguita in una sottorete nel VPC. Utilizza sottoreti per isolare i livelli dell'applicazione (ad esempio, web, applicazione e database) all'interno di un singolo VPC. Utilizza sottoreti private per le istanze se non devono essere accessibili direttamente da Internet.

Per chiamare l'API di Amazon EC2 dal tuo VPC utilizzando indirizzi IP privati, utilizza AWS PrivateLink. Per ulteriori informazioni, consulta Accesso ad Amazon EC2 utilizzando un endpoint VPC di interfaccia.

Isolamento su host fisici

Istanze EC2 differenti sullo stesso host fisico sono tra loro isolate come se si trovassero su host fisici separati. L'hypervisor isola CPU e memoria e le istanze vengono fornite su dischi virtualizzati anziché accedere a dispositivi vergini non formattati.

Quando si interrompe o termina un'istanza, la memoria ad essa allocata viene annullata (impostata su zero) dall'hypervisor prima che venga allocata a una nuova istanza e ogni blocco di archiviazione viene ripristinato. Questo garantisce che i dati non vengano involontariamente esposti a un'altra istanza.

Gli indirizzi MAC di rete vengono assegnati dinamicamente alle istanze dall'infrastruttura di rete. AWS Gli indirizzi IP vengono assegnati dinamicamente a istanze dall'infrastruttura di rete AWS o assegnati da un amministratore EC2 tramite richiese API autenticate. La AWS rete consente alle istanze di inviare traffico solo dagli indirizzi MAC e IP loro assegnati. In caso contrario, il traffico viene interrotto.

Per impostazione predefinita, un'istanza non può ricevere traffico che non è specificatamente indirizzato ad essa. Se occorre eseguire Network Address Translation (NAT), routing o servizi firewall sull'istanza, puoi disabilitare il controllo dell'origine/della destinazione per l'interfaccia di rete.

Controllo del traffico di rete

Valuta le opzioni seguenti per il controllo del traffico di rete alle istanze EC2:

- Limita l'accesso alle istanze mediante gruppi di sicurezza. Configura regole che consentano il traffico di rete minimo richiesto. Ad esempio, è possibile consentire il traffico solo dagli intervalli di indirizzi della rete aziendale o solo per protocolli specifici, come HTTPS. Per le istanze Windows, consenti il traffico di gestione di Windows e il numero minimo di connessioni in uscita.
- Sfrutta i gruppi di sicurezza come meccanismo principale per controllare l'accesso della rete alle istanze Amazon EC2. Se necessario, utilizza liste di controllo degli accessi di rete con parsimonia per fornire un controllo di rete stateless di tipo granulare. I gruppi di sicurezza sono più versatili delle liste di controllo degli accessi di rete grazie alla loro capacità di eseguire il filtro dei pacchetti con stato e creare regole che fanno riferimento ad altri gruppi di sicurezza. Tuttavia, le liste di controllo degli accessi di rete possono essere efficaci come controllo secondario per negare un sottoinsieme specifico di traffico o fornire alla sottorete una protezione di alto livello. Inoltre, poiché gli ACL di rete si applicano a un'intera sottorete, possono essere utilizzati defense-in-depth nel caso in cui un'istanza venga avviata involontariamente senza un gruppo di sicurezza corretto.
- [Istanze Windows] Gestisci centralmente le impostazioni di Windows Firewall con Group Policy Objects (GPO) per migliorare ulteriormente i controlli di rete. I clienti utilizzano spesso Windows Firewall per un'ulteriore visibilità sul traffico di rete e per integrare i filtri dei gruppi di sicurezza, creando regole avanzate per impedire l'accesso alla rete ad applicazioni specifiche o per filtrare il traffico da un sottoinsieme di indirizzi IP. Ad esempio, Windows Firewall può limitare l'accesso all'indirizzo IP del servizio di metadati EC2 a specifici utenti o applicazioni. In alternativa, un

servizio pubblico potrebbe utilizzare gruppi di sicurezza per limitare il traffico a porte specifiche e Windows Firewall per mantenere un elenco di indirizzi IP bloccati in modo esplicito.

- Utilizza sottoreti private per le istanze se non devono essere accessibili direttamente da Internet. Utilizza un host bastione o gateway NAT per l'accesso Internet da un'istanza in una sottorete privata.
- [Istanze Windows] Utilizza protocolli di amministrazione sicuri come l'incapsulamento RDP su SSL/TLS. Il Quick Start (Avvio rapido) di Gateway Desktop remoto fornisce procedure consigliate per la distribuzione del Gateway Desktop remoto, inclusa la configurazione di RDP per l'utilizzo di SSL/TLS.
- [Istanze Windows] Usa Active Directory o AWS Directory Service per controllare e monitorare in modo rigoroso e centralizzato l'accesso interattivo di utenti e gruppi alle istanze di Windows ed evita le autorizzazioni degli utenti locali. Evita inoltre di utilizzare gli amministratori di dominio e crea account basati sui ruoli più granulari e specifici dell'applicazione. Just Enough Administration (JEA) consente di gestire le modifiche alle istanze di Windows senza accesso interattivo o amministratore. Inoltre, JEA consente alle organizzazioni di bloccare l'accesso amministrativo al sottoinsieme di comandi Windows PowerShell necessari per l'amministrazione delle istanze. Per ulteriori informazioni, consulta la sezione su "Gestione dell'accesso a livello di sistema operativo a Amazon EC2" nel whitepaper Best practice di sicurezza AWS.
- [Istanze Windows] Gli amministratori di sistema devono utilizzare account Windows con accesso limitato per eseguire attività quotidiane e aumentare l'accesso solo quando necessario per eseguire modifiche specifiche alla configurazione. Inoltre, accedi solo alle istanze di Windows direttamente quando è assolutamente necessario. Sfrutta invece sistemi di gestione della configurazione centralizzati come EC2 Run Command, Systems Center Configuration Manager (SCCM), Windows PowerShell DSC o Amazon EC2 Systems Manager (SSM) per inviare modifiche ai server Windows.
- Configura le tabelle di routing della sottorete di Amazon VPC con le route di rete minime richieste. Ad esempio, posiziona solo istanze Amazon EC2 che richiedono l'accesso diretto a Internet in sottoreti con percorsi verso un gateway Internet e posiziona solo istanze Amazon EC2 che richiedono l'accesso diretto alle reti interne in sottoreti con percorsi verso un gateway privato virtuale.
- Prendi in considerazione l'utilizzo di gruppi di sicurezza aggiuntivi per controllare e verificare il traffico di gestione delle istanze Amazon EC2 separatamente dal normale traffico delle applicazioni. Questo approccio consente ai clienti di implementare criteri IAM speciali per il controllo delle modifiche, semplificando l'audit delle modifiche apportate alle regole dei gruppi di sicurezza o agli script di verifica automatica delle regole. L'utilizzo di più interfacce di rete offre anche opzioni

aggiuntive per il controllo del traffico di rete, inclusa la possibilità di creare politiche di routing basate su host o sfruttare diverse regole di routing della sottorete VPC in base alla sottorete assegnata dell'interfaccia di rete.

- Usa AWS Virtual Private Network o AWS Direct Connect per stabilire connessioni private dalle tue reti remote ai tuoi VPC. Per ulteriori informazioni, consulta la sezione relativa alle Opzioni di connettività da rete ad Amazon VPC.
- Utilizza Log di flusso VPC per monitorare il traffico che raggiunge le istanze.
- Utilizza GuardDuty Malware Protection per identificare sulle tue istanze comportamenti sospetti indicativi della presenza di software dannoso che potrebbero compromettere il carico di lavoro, riutilizzare le risorse per usi dannosi e ottenere l'accesso non autorizzato ai tuoi dati.
- Usa GuardDuty Runtime Monitoring per identificare e rispondere a potenziali minacce alle tue istanze. Per ulteriori informazioni, consulta Come funziona il monitoraggio del runtime con le istanze Amazon EC2.
- Usa AWS Security HubReachability Analyzer o Network Access Analyzer per verificare l'accessibilità involontaria della rete dalle tue istanze.
- Utilizza Connessione all'istanza EC2 per connetterti alle istanze utilizzando Secure Shell (SSH) senza la necessità di condividere e gestire chiavi SSH.
- Utilizza AWS Systems Manager Session Manager per accedere alle istanze da remoto anziché aprire porte SSH o RDP in entrata e gestire coppie di chiavi.
- Usa AWS Systems Manager Run Command per automatizzare le attività amministrative più comuni invece di connetterti alle tue istanze.
- [Istanze Windows] Molti ruoli del sistema operativo Windows e le applicazioni aziendali Microsoft offrono anche funzionalità avanzate come le restrizioni dell'intervallo di indirizzi IP all'interno di IIS, i criteri di filtro TCP/IP in Microsoft SQL Server e i criteri di filtro delle connessioni in Microsoft Exchange. La funzionalità di restrizione di rete all'interno del livello dell'applicazione può fornire ulteriori livelli di difesa per i server applicazioni aziendali critici.

Amazon VPC supporta controlli di sicurezza di rete aggiuntivi, come gateway, server proxy e opzioni di monitoraggio della rete. Per ulteriori informazioni, consulta Controllare il traffico di rete nella Amazon VPC User Guide.

Resilienza in Amazon EC2

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente

ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

Se occorre replicare i dati o le applicazioni su distanze geografiche più ampie, utilizza AWS Local Zones. Una zona AWS locale è un'estensione di una AWS regione situata in prossimità geografica degli utenti. Le zone locali hanno le loro connessioni a Internet e supportano AWS Direct Connect. Come tutte le AWS Regioni, le AWS Local Zones sono completamente isolate dalle altre AWS Zone.

Se è necessario replicare i dati o le applicazioni in una zona AWS locale, si AWS consiglia di utilizzare una delle seguenti zone come zona di failover:

- Un'altra Local Zone
- Zona di disponibilità nella regione che non è la zona padre. È possibile utilizzare il describe-availability-zonescomando per visualizzare la zona principale.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, vedere AWS Global Infrastructure.

Oltre all'infrastruttura AWS globale, Amazon EC2 offre le seguenti funzionalità per supportare la resilienza dei dati:

- Copia di AMI tra regioni
- Copia di snapshot EBS tra regioni
- Automazione delle AMI EBS-backed tramite Amazon Data Lifecycle Manager
- Automazione degli snapshot EBS mediante Amazon Data Lifecycle Manager
- Mantenimento dell'integrità e della disponibilità del parco istanze mediante Amazon EC2 Auto Scaling
- Distribuzione del traffico in entrata tra più istanze in una singola zona di disponibilità o in più zone di disponibilità mediante Elastic Load Balancing.

Convalida della conformità per Amazon EC2

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty

può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Identity and Access Management per Amazon EC2

Le tue credenziali di sicurezza ti identificano nei servizi in AWS e ti garantiscono l'uso illimitato delle tue AWS risorse, come le risorse Amazon EC2. Puoi utilizzare le caratteristiche di Amazon EC2 e AWS Identity and Access Management (IAM) per consentire ad altri utenti, servizi e applicazioni di utilizzare le risorse Amazon EC2 senza condividere le credenziali di sicurezza. Puoi utilizzare IAM per controllare il modo in cui gli altri utenti utilizzano le risorse del tuo AWS account e puoi utilizzare i gruppi di sicurezza per controllare l'accesso alle tue istanze Amazon EC2. Puoi decidere di consentire l'uso completo o limitato delle risorse Amazon EC2.

Per le migliori pratiche per proteggere le AWS risorse utilizzando IAM, consulta Best practice di sicurezza in IAM.

Indice

Accesso di rete all'istanza

Un gruppo di sicurezza agisce come un firewall che controlla il traffico a cui è consentito raggiungere una o più istanze. Quando avvii un'istanza, assegni tale istanza a uno o più gruppi di sicurezza. Puoi aggiungere regole a ogni gruppo di sicurezza che controlla il traffico per l'istanza. Puoi modificare le regole per un gruppo di sicurezza in qualunque momento; le nuove regole vengono applicate automaticamente a tutte le istanze a cui è assegnato il gruppo di sicurezza.

Per ulteriori informazioni, consulta Regole del gruppo di sicurezza.

Attributi di autorizzazione Amazon EC2

La tua organizzazione potrebbe avere più AWS account. Amazon EC2 ti consente di specificare AWS account aggiuntivi che possono utilizzare le tue Amazon Machine Images (AMI) e gli snapshot di Amazon EBS. Queste autorizzazioni funzionano solo a livello di AWS account; non puoi limitare le autorizzazioni per utenti specifici all'interno dell'account specificato. AWS Tutti gli utenti nell'account AWS specificato possono utilizzare l'AMI o lo snapshot.

Ogni AMI dispone di un attributo `LaunchPermission` che controlla gli account AWS che possono accedere all'AMI. Per ulteriori informazioni, consulta Rendere un'AMI pubblica.

Ogni snapshot di Amazon EBS ha un `createVolumePermission` attributo che controlla quali AWS account possono utilizzare lo snapshot. Per ulteriori informazioni, consulta Share an Amazon EBS snapshot nella Amazon EBS User Guide.

IAM e Amazon EC2

IAM ti consente di:

- Crea utenti e gruppi sotto la tua Account AWS
- Assegna credenziali di sicurezza univoche a ciascun utente del Account AWS
- Controlla le autorizzazioni di ogni utente per eseguire attività utilizzando le risorse AWS
- Consenti agli utenti di un altro utente Account AWS di condividere le tue risorse AWS
- Crea ruoli per te Account AWS e definisci gli utenti o i servizi che possono assumerli
- Utilizza le identità esistenti per la tua azienda per concedere le autorizzazioni per eseguire attività utilizzando le risorse AWS

Utilizzando IAM con Amazon EC2, puoi controllare se gli utenti all'interno dell'organizzazione sono in grado di eseguire un'attività utilizzando specifiche operazioni API Amazon EC2 e se possono utilizzare risorse AWS specifiche.

Questo argomento fornisce una risposta alle seguenti domande:

- Come si creano gruppi e utenti in IAM?
- Come si crea una policy?
- Quali policy IAM sono necessarie per eseguire i task in Amazon EC2?
- Come si concedono le autorizzazioni per l'esecuzione di operazioni in Amazon EC2?

- Come si concedono le autorizzazioni per l'esecuzione di operazioni su risorse specifiche in Amazon EC2?

Creare utenti, gruppi e ruoli

Potete creare utenti e gruppi per voi Account AWS e quindi assegnare loro le autorizzazioni necessarie. Come best practice, gli utenti dovrebbero acquisire le autorizzazioni assumendo ruoli IAM.

Un ruolo IAM è un'identità IAM che puoi creare nel tuo account e che dispone di autorizzazioni specifiche. Un ruolo IAM è simile a quello di un utente IAM in quanto è un' AWS identità con politiche di autorizzazione che determinano ciò che l'identità può e non può fare. AWS Tuttavia, invece di essere associato in modo univoco a una persona, un ruolo è destinato a essere assunto da chiunque. Inoltre, un ruolo non ha credenziali a lungo termine standard associate (password o chiavi di accesso). Tuttavia, quando assumi un ruolo, vengono fornite le credenziali di sicurezza provvisorie per la sessione del ruolo. Per ulteriori informazioni su come creare ruoli IAM e concedere le relative autorizzazioni, consulta. the section called “Ruoli IAM”

Argomenti correlati

Per ulteriori informazioni su IAM, consulta:

- Policy IAM per Amazon EC2
- Ruoli IAM per Amazon EC2
- AWS Identity and Access Management (IAM)
- Guida per l'utente di IAM

Policy IAM per Amazon EC2

Per impostazione predefinita, gli utenti non sono autorizzati a creare o modificare le risorse Amazon EC2 o a eseguire attività tramite l'API Amazon EC2, la console Amazon EC2 o la CLI. Per permettere agli utenti di creare o modificare le risorse ed eseguire le attività, devi creare policy IAM che concedano agli utenti l'autorizzazione a utilizzare specifiche risorse e operazioni API e quindi collegare tali policy agli utenti, gruppi o ruoli IAM che richiedono tali autorizzazioni.

Quando si collega una policy a un utente, un gruppo di utenti o un ruolo, viene concessa o rifiutata agli utenti l'autorizzazione per eseguire attività specificate sulle risorse specificate. Per ulteriori

informazioni generali sulle policy IAM, consulta la sezione relativa a Policy e autorizzazioni in IAM nella Guida per l'utente IAM. Per ulteriori informazioni sulla gestione e la creazione di policy IAM personalizzate, consulta la sezione relativa alla gestione delle policy IAM.

Nozioni di base

Una policy IAM deve concedere o rifiutare le autorizzazioni necessarie per l'utilizzo di una o più operazioni Amazon EC2. Deve inoltre specificare le risorse che possono essere utilizzate con l'operazione, vale a dire tutte le risorse oppure, in alcuni casi, risorse specifiche. La policy può anche includere condizioni applicabili alla risorsa.

Amazon EC2 supporta parzialmente le autorizzazioni a livello di risorsa. Ciò significa che, per alcune operazioni API di EC2, non puoi specificare la risorsa che un utente può utilizzare per tale operazione. Dovrai quindi permettere agli utenti di utilizzare tutte le risorse per l'operazione.

Attività	Argomento
Introduzione alla struttura di base di una policy	Sintassi delle policy
Definizione delle operazioni nella policy	Operazioni per Amazon EC2
Definizione di risorse specifiche nella policy	Nome della risorsa Amazon (ARN) per Amazon EC2
Applicazioni di condizioni all'uso delle risorse	Chiavi di condizione per Amazon EC2
Utilizzo delle autorizzazioni disponibili a livello di risorsa per Amazon EC2	Operazioni, risorse e chiavi di condizione per Amazon EC2
Test della policy	Verificare che gli utenti dispongano delle autorizzazioni necessarie
Generazione di una policy IAM	Generazione di policy basate sull'attività di accesso
Esempi di policy per una CLI o un SDK	Politiche di esempio per lavorare con AWS CLI o un AWS SDK
Esempio di policy per la console Amazon EC2	Policy di esempio da utilizzare nella console Amazon EC2

Concedere autorizzazioni a utenti, gruppi e ruoli

Di seguito sono riportati alcuni esempi di alcune politiche AWS gestite che è possibile utilizzare se soddisfano le esigenze dell'utente:

- `PowerUserAccess`
- `ReadOnlyAccess`
- `AmazonEC2FullAccess`
- `AmazonEC2ReadOnlyAccess`

Per ulteriori informazioni, consulta the section called “AWS politiche gestite”.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Struttura delle policy

Nei seguenti argomenti viene illustrata la struttura di una policy IAM.

Indice

- Operazioni per Amazon EC2
- Autorizzazioni a livello di risorsa supportate per le operazioni API Amazon EC2
- Nome della risorsa Amazon (ARN) per Amazon EC2
- Chiavi di condizione per Amazon EC2
- Verificare che gli utenti dispongano delle autorizzazioni necessarie

Sintassi delle policy

Una policy IAM è un documento JSON costituito da una o più dichiarazioni. Ogni dichiarazione è strutturata come segue.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Una dichiarazione è costituita da diversi elementi:

- Effect (Effetto): l'elemento effect può essere `Allow` o `Deny`. Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per l'utilizzo di risorse e operazioni API, pertanto tutte le richieste vengono rifiutate. Un permesso esplicito sostituisce l'impostazione predefinita. Un rifiuto esplicito sovrascrive tutti i consensi.
- Action (Operazione): l'elemento action corrisponde all'operazione API specifica per la quale si concede o si nega l'autorizzazione. Per informazioni su come specificare l'elemento action, consulta Operazioni per Amazon EC2.
- Resource (Risorsa): la risorsa che viene modificata dall'operazione. Alcune operazioni API di Amazon EC2 ti permettono di includere nella policy risorse specifiche che possono essere create o modificate dall'operazione. Specifica una risorsa utilizzando un nome della risorsa Amazon (ARN) o il carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse. Per ulteriori

informazioni, consulta Autorizzazioni a livello di risorsa supportate per le operazioni API Amazon EC2.

- Condition: le condizioni sono facoltative. Possono essere utilizzate per controllare quando è in vigore una policy. Per ulteriori informazioni su come specificare le condizioni per Amazon EC2, consulta Chiavi di condizione per Amazon EC2.

Per ulteriori informazioni su requisiti per le policy, consulta Riferimento alle policy JSON IAM nella Guida per l'utente IAM. Per alcuni esempi di istruzioni di policy IAM per Amazon EC2, consulta Politiche di esempio per lavorare con AWS CLI o un AWS SDK.

Operazioni per Amazon EC2

In una dichiarazione di policy IAM, è possibile specificare qualsiasi operazione API per qualsiasi servizio che supporta IAM. Per Amazon EC2, utilizza il seguente prefisso con il nome dell'operazione API: `ec2:`. Ad esempio: `ec2:RunInstances` ed `ec2:CreateImage`.

Per specificare più operazioni in una sola dichiarazione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": ["ec2:action1", "ec2:action2"]
```

Puoi anche specificare più operazioni tramite caratteri jolly. Ad esempio, puoi specificare tutte le operazioni il cui nome inizia con la parola "Describe" (Descrivi) come segue:

```
"Action": "ec2:Describe*"
```

> **Note**
>
> Attualmente, le operazioni API Amazon EC2 Describe* non supportano autorizzazioni a livello di risorsa. Per ulteriori informazioni sulle autorizzazioni a livello di risorsa per Amazon EC2, consulta Policy IAM per Amazon EC2.

Per specificare tutte le operazioni API Amazon EC2, utilizza il carattere jolly * come mostrato di seguito:

```
"Action": "ec2:*"
```

Per visualizzare un elenco di operazioni di Amazon EC2, consulta Operazioni definite da Amazon EC2 nella Service Authorization Reference.

Autorizzazioni a livello di risorsa supportate per le operazioni API Amazon EC2

Il concetto di autorizzazioni a livello di risorsa indica la possibilità di specificare le risorse su cui gli utenti sono autorizzati a eseguire operazioni. Amazon EC2 supporta parzialmente le autorizzazioni a livello di risorsa. Ciò significa che per determinate operazioni di Amazon EC2, puoi controllare se gli utenti sono autorizzati a utilizzare tali operazioni in base a condizioni che devono essere soddisfatte o a specifiche risorse che gli utenti sono autorizzati a utilizzare. Ad esempio, puoi concedere agli utenti le autorizzazioni per avviare le istanze, ma solo di un determinato tipo e solo utilizzando un AMI specifico.

Per specificare una risorsa nella dichiarazione della policy IAM, si utilizza il suo nome della risorsa Amazon (ARN). Per ulteriori informazioni su come specificare il valore ARN, consulta Nome della risorsa Amazon (ARN) per Amazon EC2. Se l'operazione API non supporta gli ARN individuali, devi utilizzare il carattere jolly (*) per specificare che tutte le risorse possono essere interessate dall'operazione.

Per visualizzare le tabelle che identificano quali operazioni API Amazon EC2 supportano le autorizzazioni a livello di risorse e le chiavi di condizione e gli ARN che è possibile utilizzare in una policy, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Occorre ricordare che è possibile applicare autorizzazioni a livello di risorsa basate su tag nelle policy IAM utilizzate per la maggior parte delle operazioni API Amazon EC2. In questo modo è possibile controllare meglio le risorse che un utente può creare, modificare o utilizzare. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

Nome della risorsa Amazon (ARN) per Amazon EC2

Ogni dichiarazione di policy IAM si applica alle risorse specificate utilizzando i relativi ARN.

Un ARN presenta la seguente sintassi generale:

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

service

Il servizio (ad esempio `ec2`).

Regione

La regione per la risorsa (ad esempio `us-east-1`).

account-id

L'ID AWS dell'account, senza trattini (ad esempio,`123456789012`).

resourceType

Il tipo di risorsa (ad esempio `instance`).

resourcePath

Un percorso che identifica la risorsa. Nei percorsi puoi utilizzare il carattere jolly *.

Ad esempio, nella tua dichiarazione puoi specificare una determinata istanza (`i-1234567890abcdef0`) utilizzando il relativo ARN come segue:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Puoi specificare tutte le istanze appartenenti a un determinato account utilizzando il carattere jolly * come segue:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Puoi anche specificare tutte le risorse Amazon EC2 appartenenti a un determinato account utilizzando il carattere jolly * come segue:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Per specificare tutte le risorse o se una determinata operazione API non supporta gli ARN, utilizza il carattere jolly * nell'elemento `Resource` come segue:

```
"Resource": "*"
```

Molte operazioni API di Amazon EC2 coinvolgono più risorse. Ad esempio, `AttachVolume` collega un volume Amazon EBS a un'istanza, pertanto un utente dovrà disporre delle autorizzazioni per utilizzare il volume e l'istanza. Per specificare più risorse in una sola dichiarazione, separa i relativi ARN con una virgola come mostrato di seguito.

```
"Resource": ["arn1", "arn2"]
```

Per un elenco di ARN per le risorse Amazon EC2, consulta Tipi di risorse definiti da Amazon EC2.

Chiavi di condizione per Amazon EC2

In una dichiarazione di policy, puoi specificare facoltativamente le condizioni che controllano quando questa è in vigore. Ogni condizione contiene una o più coppie chiave/valore. Le chiavi di condizione non distinguono tra maiuscole e minuscole. Abbiamo definito chiavi di condizione AWS globali, oltre a chiavi di condizione aggiuntive specifiche del servizio.

Per un elenco di chiavi di condizione specifiche del servizio per Amazon EC2, consulta Chiavi di condizione per Amazon EC2. Amazon EC2 implementa anche le chiavi di condizione AWS globali. Per ulteriori informazioni, consulta la pagina relativa alle informazioni disponibili in tutte le richieste nella Guida per l'utente di IAM.

Tutte le operazioni Amazon EC2 supportano le chiavi di condizione `aws:RequestedRegion` e `ec2:Region`. Per ulteriori informazioni, consulta Esempio: limitazione dell'accesso a una regione specifica.

Per utilizzare una chiave di condizione nella policy IAM, utilizzare l'istruzione `Condition`. Ad esempio, la policy seguente concede agli utenti l'autorizzazione per aggiungere ed eliminare regole in entrata e in uscita per qualsiasi gruppo di sicurezza. Utilizza la chiave di condizione `ec2:Vpc` per specificare che queste azioni possono essere eseguite solo su gruppi di sicurezza in un VPC specifico.

```
{
"Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupEgress"],
     "Resource": "arn:aws:ec2:region:account:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
        }
      }
```

```
    }
  ]
}
```

Se specifichi più condizioni o più chiavi in una sola condizione le valutiamo utilizzando un'operazione AND logica. Se specifichi una sola condizione con più valori per una sola chiave, valutiamo la condizione utilizzando un'operazione OR logica. Affinché le autorizzazioni vengano concesse, tutte le condizioni devono essere soddisfatte.

Puoi anche utilizzare i segnaposto quando specifichi le condizioni. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

> **Important**
>
> Molte chiavi di condizione sono specifiche di una risorsa e alcune operazioni API utilizzano più risorse. Se scrivi una policy con una chiave di condizione, utilizza l'elemento `Resource` della dichiarazione per specificare la risorsa a cui viene applicata la chiave di condizione. In caso contrario, la policy potrebbe impedire agli utenti di eseguire operazioni perché il controllo della condizione ha esito negativo per le risorse alle quali non viene applicata la chiave di condizione. Se non vuoi specificare una risorsa oppure se hai scritto l'elemento `Action` della policy in modo da includere più operazioni API, devi utilizzare il tipo di condizione `...IfExists` per assicurarti che la chiave di condizione venga ignorata per le risorse che non la utilizzano. Per ulteriori informazioni, consulta... IfExists Condizioni nella Guida per l'utente IAM.

Chiavi di condizione

- Chiave di condizione ec2:Attribute
- Chiavi di condizione ec2:ResourceID
- Chiave di condizione ec2:SourceInstanceARN

Chiave di condizione ec2:Attribute

La chiave di condizione `ec2:Attribute` può essere utilizzata per le condizioni che filtrano l'accesso da un attributo di una risorsa.

Questa chiave condizionale supporta solo proprietà di un tipo di dati primitivo (come stringhe o numeri interi) o AttributeValueoggetti complessi che contengono solo una proprietà Value

(come la descrizione o ImdsSupportgli oggetti dell'azione ModifyImageAttributeAPI). La chiave condition non può essere utilizzata con oggetti complessi che contengono più proprietà, come l'LaunchPermissionoggetto di. ModifyImageAttribute

Ad esempio, la seguente politica utilizza la chiave `ec2:Attribute/Description` condition per filtrare l'accesso in base al complesso oggetto Description dell'azione ModifyImageAttributeAPI. La chiave di condizione consente solo le richieste che modificano la descrizione di un'immagine a `Production` o `Development`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

La politica di esempio seguente utilizza la chiave `ec2:Attribute` condition per filtrare l'accesso in base alla proprietà primitiva Attribute dell'azione ModifyImageAttributeAPI. La chiave di condizione respinge tutte le richieste che modificano la descrizione di un'immagine.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
```

```
        }
      }
    }
  ]
}
```

Chiavi di condizione ec2:ResourceID

Quando si utilizza quanto segue`ec2:`*`Resource`*`ID`chiavi di condizione con le azioni API specificate, il valore della chiave di condizione viene utilizzato per specificare la risorsa risultante creata dall'azione API.`ec2:`*`Resource`*`ID`le chiavi di condizione non possono essere utilizzate per specificare una risorsa di origine specificata nella richiesta API. Se si utilizza uno dei seguenti`ec2:`*`Resource`*`ID`condition keys con un'API specificata, quindi devi sempre specificare la wildcard (*). Se si specifica un valore diverso, la condizione si risolve sempre in * durante il runtime. Ad esempio, per utilizzare la chiave di `ec2:ImageId` condizione con l'CopyImageAPI, è necessario specificare la chiave di condizione come segue:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Ti consigliamo di evitare di utilizzare queste chiavi di condizione con queste azioni API:

- `ec2:DhcpOptionsID` – `CreateDhcpOptions`
- `ec2:ImageID`— `CopyImage``CreateImage`,`ImportImage`, e `RegisterImage`
- `ec2:InstanceID`— `RunInstances` e `ImportInstance`
- `ec2:InternetGatewayID` – `CreateInternetGateway`
- `ec2:NetworkAclID` – `CreateNetworkAcl`

- `ec2:NetworkInterfaceID` – `CreateNetworkInterface`
- `ec2:PlacementGroupName` – `CreatePlacementGroup`
- `ec2:RouteTableID` – `CreateRouteTable`
- `ec2:SecurityGroupID` – `CreateSecurityGroup`
- `ec2:SnapshotID`— `CopySnapshot`,`CreateSnapshot`, e `ImportSnapshot`
- `ec2:SubnetID` – `CreateSubnet`
- `ec2:VolumeID`— `CreateVolume` e `ImportVolume`
- `ec2:VpcID` – `CreateVpc`
- `ec2:VpcPeeringConnectionID` – `CreateVpcPeeringConnection`

Per filtrare l'accesso in base a ID di risorse specifici, si consiglia di utilizzare l'elemento di `Resource` policy come segue.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-01234567890abcdef"
    }
  ]
}
```

Chiave di condizione ec2:SourceInstanceARN

Utilizzare `ec2:SourceInstanceARN` per specificare l'ARN dell'istanza da cui viene effettuata una richiesta. Si tratta di una chiave di condizione AWS globale, il che significa che puoi utilizzarla con servizi diversi da Amazon EC2. Per un esempio di policy, consulta Esempio: consentire a un'istanza specifica di visualizzare le risorse in altri AWS servizi.

Verificare che gli utenti dispongano delle autorizzazioni necessarie

Dopo aver creato una policy IAM, prima di metterla in produzione, ti consigliamo di verificare se vengono concesse agli utenti le autorizzazioni per l'utilizzo di specifiche risorse e operazioni API necessarie.

In primo luogo, crea un utente a scopo di test e collega la policy IAM creata all'utente del test. In seguito, effettua una richiesta come utente di test.

Se l'operazione Amazon EC2 di cui stai eseguendo il test crea o modifica una risorsa, devi effettuare la richiesta utilizzando il parametro `DryRun` (o eseguire il comando della AWS CLI con l'opzione `--dry-run`). In questo caso, la chiamata completa la verifica dell'autorizzazione, ma non completa l'operazione. Ad esempio, puoi controllare se l'utente è in grado di interrompere una determinata istanza senza effettivamente terminarla. Se l'utente del test dispone delle autorizzazioni necessarie, la richiesta restituisce `DryRunOperation`, altrimenti restituisce `UnauthorizedOperation`.

Se la policy non concede all'utente le autorizzazioni previste oppure è eccessivamente permissiva, puoi modificarla in base alle esigenze e ripetere il test fino a ottenere i risultati desiderati.

> **Important**
>
> La propagazione delle modifiche alla policy e la loro validità potrebbe richiedere alcuni minuti. Ti consigliamo quindi di attendere 5 minuti prima di effettuare il test degli aggiornamenti delle policy.

Se una verifica dell'autorizzazione ha esito negativo, la richiesta restituisce un messaggio codificato con informazioni di diagnostica. Il messaggio può essere decodificato tramite l'operazione `DecodeAuthorizationMessage`. Per ulteriori informazioni, consulta DecodeAuthorizationMessagel'AWS Security Token Service API Reference e decode-authorization-messageil AWS CLI Command Reference.

Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione

Alcune operazioni API Amazon EC2 per la creazione di risorse ti consentono di specificare tag quando crei le risorse. È possibile utilizzare i tag delle risorse per implementare il controllo basato sugli attributi (ABAC). Per ulteriori informazioni, consulta Assegnazione di tag alle risorse e Controllo dell'accesso alle risorse EC2 mediante i tag delle risorse.

Per consentire agli utenti di applicare tag alle risorse durante la creazione, essi devono disporre delle autorizzazioni per utilizzare l'operazione che crea la risorsa, come `ec2:RunInstances` o `ec2:CreateVolume`. Se i tag vengono specificati nell'azione di creazione delle risorse, Amazon esegue autorizzazioni aggiuntive per l'azione `ec2:CreateTags` per verificare se gli utenti

dispongono delle autorizzazioni per creare tag. Pertanto, gli utenti devono disporre anche delle autorizzazioni esplicite per utilizzare l'operazione `ec2:CreateTags`.

Nella definizione della policy IAM per l'operazione `ec2:CreateTags`, utilizzare l'elemento `Condition` con la chiave di condizione `ec2:CreateAction` per assegnare autorizzazioni di tagging all'operazione che crea la risorsa.

Ad esempio, la seguente policy consente gli utenti di avviare istanze e applicare tag a istanze e volumi durante l'avvio. Gli utenti non sono autorizzati ad applicare tag alle risorse esistenti (non possono chiamare l'operazione `ec2:CreateTags` direttamente).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

In modo analogo, la seguente policy consente gli utenti di creare volumi e applicare tag a tali volumi durante la creazione dei volumi stessi. Gli utenti non sono autorizzati ad applicare tag alle risorse esistenti (non possono chiamare l'operazione `ec2:CreateTags` direttamente).

```
{
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "CreateVolume"
          }
       }
    }
  ]
}
```

L'operazione `ec2:CreateTags` viene valutata solo se i tag vengono applicati durante l'operazione di creazione di risorse. Pertanto, un utente con le autorizzazioni per la creazione di una risorsa (presupponendo che non siano presenti condizioni di assegnazione di tag) non necessità delle autorizzazioni per utilizzare l'operazione `ec2:CreateTags` se nella richiesta non viene specificato alcun tag. Tuttavia, se l'utente tenta di creare una risorsa con tag, la richiesta ha esito negativo se non dispone delle autorizzazioni per utilizzare l'operazione `ec2:CreateTags`.

L'operazione `ec2:CreateTags` viene valutata anche se i tag sono forniti in un modello di avvio. Per un esempio di policy, consulta Tag in un modello di avvio.

Controllo dell'accesso a tag specifici

È possibile utilizzare condizioni aggiuntive nell'elemento `Condition` delle policy IAM per controllare le chiavi dei tag e i valori che possono essere applicati alle risorse.

Le seguenti chiavi di condizione possono essere utilizzate con gli esempi nella sezione precedente:

- `aws:RequestTag`: indica che una chiave di tag o una chiave e un valore di tag sono presenti in una richiesta. Anche gli altri tag devono essere specificati nella richiesta.

  - Da utilizzare assieme all'operatore di condizione `StringEquals` per applicare una combinazione specifica di chiave e valore di tag, ad esempio per applicare il tag `cost-center=cc123`:

    ```
    "StringEquals": { "aws:RequestTag/cost-center": "cc123" }
    ```

  - Da utilizzare assieme all'operatore di condizione `StringLike` per applicare una chiave di tag specifica nella richiesta, ad esempio per applicare la chiave di tag `purpose`:

    ```
    "StringLike": { "aws:RequestTag/purpose": "*" }
    ```

- `aws:TagKeys`: applica le chiavi di tag utilizzate nella richiesta.
  - Da utilizzare assieme al modificatore `ForAllValues` per applicare chiavi di tag specifiche se vengono fornite nella richiesta (se i tag vengono specificati nella richiesta, solo le chiavi di tag specifiche sono consentite; non sono consentiti altri tag). Ad esempio, la chiave di tag `environment` o `cost-center` è consentita:

    ```
    "ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
    ```

  - Da utilizzare assieme al modificatore `ForAnyValue` per implementare la presenza di almeno una delle chiavi di tag specificate nella richiesta. Ad esempio, nella richiesta deve essere presente almeno una delle chiavi di tag `environment` o `webserver`:

    ```
    "ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
    ```

Queste chiavi di condizione possono essere applicate alle operazioni di creazione delle risorse che supportano il tagging, nonché alle operazioni `ec2:CreateTags` ed `ec2:DeleteTags`. Per sapere se un'operazione API Amazon EC2 supporta l'aggiunta di tag, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Per obbligare gli utenti a specificare i tag quando creano una risorsa, devi utilizzare la chiave di condizione `aws:RequestTag` o `aws:TagKeys` con il modificatore `ForAnyValue` nell'operazione di creazione delle risorse. L'operazione `ec2:CreateTags` non viene valutata se un utente non specifica i tag per l'operazione di creazione delle risorse.

Per le condizioni, la chiave di condizione non fa distinzione tra maiuscole e minuscole, mentre il valore della condizione fa distinzione tra maiuscole e minuscole. Pertanto, per applicare la distinzione

tra maiuscole e minuscole per una chiave di tag, utilizza la chiave di condizione `aws:TagKeys`, specificando la chiave di tag come valore nella condizione.

Per esempi di policy IAM, consulta Politiche di esempio per lavorare con AWS CLI o un AWS SDK. Per ulteriori informazioni sulle condizioni con più valori, consulta la sezione relativa alla creazione di una condizione per il test di valori di chiave multipli nella Guida per l'utente di IAM.

Controllo dell'accesso alle risorse EC2 mediante i tag delle risorse

Quando crei una policy IAM che concede agli utenti l'autorizzazione a utilizzare le risorse EC2, puoi includere informazioni sui tag nell'elemento `Condition` della policy per controllare l'accesso in base ai tag. Questo è noto come controllo degli accessi basato su attributi (ABAC). Il controllo ABAC fornisce un miglior controllo su quali risorse possono essere modificate, utilizzate o eliminate da un utente. Per ulteriori informazioni, consulta Che cos'è ABAC per AWS?

Ad esempio, è possibile creare una policy che consente agli utenti di terminare un'istanza ma che neghi l'operazione se l'istanza presenta il tag `environment=production`. A tale scopo, è possibile utilizzare la chiave di condizione `aws:ResourceTag` per consentire o negare l'accesso alla risorsa in base ai tag collegati alla risorsa.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Per sapere se un'operazione API Amazon EC2 supporta il controllo degli accessi utilizzando la chiave di condizione `aws:ResourceTag`, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2. Tieni a mente che le operazioni `Describe` non supportano le autorizzazioni a livello di risorsa, pertanto è necessario specificarle in una dichiarazione separata senza condizioni.

Per esempi di policy IAM, consulta Politiche di esempio per lavorare con AWS CLI o un AWS SDK.

Se consenti o neghi a un utente l'accesso a risorse in base ai tag, devi considerare esplicitamente di negare agli utenti la possibilità di aggiungere o rimuovere tali tag dalle stesse risorse. In caso contrario, un utente può eludere le restrizioni e ottenere l'accesso a una risorsa modificandone i tag.

Politiche di esempio per lavorare con AWS CLI o un AWS SDK

Devi concedere agli utenti le autorizzazioni necessarie per Amazon EC2 utilizzando le policy IAM. I seguenti esempi mostrano le dichiarazioni di policy che è possibile utilizzare per controllare le autorizzazioni degli utenti per Amazon EC2. Queste politiche sono progettate per le richieste effettuate con AWS CLI o con un AWS SDK. Per ulteriori informazioni, consulta Creazione di policy IAM nella Guida per l'utente IAM. Per le policy di esempio da utilizzare nella console Amazon EC2,

consultare Policy di esempio da utilizzare nella console Amazon EC2. Per esempi di policy IAM specifiche per Amazon VPC, consultare Identity and Access Management per Amazon VPC.

Negli esempi seguenti, sostituire ogni *segnaposto dell'input utente* con le proprie informazioni.

Esempi

- Esempio: accesso in sola lettura
- Esempio: limitazione dell'accesso a una regione specifica
- Utilizzo delle istanze
- Avvia istanze () RunInstances
- Utilizzo delle Istanze spot
- Esempio: utilizzo delle Istanze riservate
- Esempio: aggiunta di tag alle risorse
- Esempio: utilizzo dei ruoli IAM
- Esempio: utilizzo delle tabelle di routing
- Esempio: consentire a un'istanza specifica di visualizzare le risorse in altri AWS servizi
- Esempio: utilizzo dei modelli di avvio
- Utilizzo dei metadati delle istanze
- Lavora con volumi e snapshot di Amazon EBS

Esempio: accesso in sola lettura

La policy seguente concede agli utenti le autorizzazioni per utilizzare tutte le operazioni dell'API Amazon EC2 i cui nomi iniziano con `Describe`. L'elemento `Resource` utilizza un carattere jolly per indicare che tutti gli utenti possono specificare tutte le risorse con queste operazioni dell'API. Il carattere jolly * è necessario inoltre nei casi in cui l'operazione dell'API non supporta le autorizzazioni a livello di risorsa. Per ulteriori informazioni sugli ARN che è possibile utilizzare con le operazioni API Amazon EC2, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Per impostazione predefinita, agli utenti non viene concessa l'autorizzazione per eseguire le operazioni dell'API sulle risorse (a meno che un'altra istruzione non conceda loro l'autorizzazione corrispondente).

```
{
   "Version": "2012-10-17",
```

```
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

Esempio: limitazione dell'accesso a una regione specifica

La policy seguente nega agli utenti le autorizzazioni per utilizzare tutte le operazioni dell'API Amazon EC2, a meno che la regione sia Europa (Francoforte). Utilizza la chiave di condizione globale `aws:RequestedRegion`, che è supportato da tutte le operazioni API di Amazon EC2.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
}
```

In alternativa, è possibile utilizzare la chiave di condizione `ec2:Region`, specifica per Amazon EC2 ed è supportata da tutte le operazioni API di Amazon EC2.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
```

```
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

Utilizzo delle istanze

Esempi

- Esempio: descrizione, avvio, arresto e terminazione di tutte le istanze
- Esempio: descrizione di tutte le istanze e arresto, avvio e terminazione soltanto di determinate istanze

Esempio: descrizione, avvio, arresto e terminazione di tutte le istanze

La policy seguente concede agli utenti le autorizzazioni per utilizzare le operazioni dell'API specificate nell'elemento `Action`. L'elemento `Resource` utilizza un carattere jolly * per indicare che tutti gli utenti possono specificare tutte le risorse con queste operazioni dell'API. Il carattere jolly * è necessario inoltre nei casi in cui l'operazione dell'API non supporta le autorizzazioni a livello di risorsa. Per ulteriori informazioni sugli ARN che è possibile utilizzare con le operazioni API Amazon EC2, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Gli utenti non dispongono dell'autorizzazione per utilizzare altre operazioni dell'API (a meno che un'altra istruzione non conceda loro l'autorizzazione corrispondente) perché, per impostazione predefinita, agli utenti non viene concessa l'autorizzazione per utilizzare le operazioni dell'API.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
```

```
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
   ]
}
```

Esempio: descrizione di tutte le istanze e arresto, avvio e terminazione soltanto di determinate istanze

La policy seguente consente agli utenti di descrivere tutte le istanze, di avviare e arrestare soltanto le istanze i-1234567890abcdef0 e i-0598c7d356eba48d7 e di terminare soltanto le istanze in della regione Stati Uniti orientali (Virginia settentrionale), (`us-east-1`) con il tag di risorsa "`purpose=test`".

La prima istruzione utilizza il carattere jolly * per l'elemento `Resource` per indicare che gli utenti possono specificare tutte le risorse con questa operazione; in questo caso, possono elencare tutte le istanze. Il carattere jolly * è necessario inoltre nei casi in cui l'operazione dell'API non supporta le autorizzazioni a livello di risorsa (in questo caso, `ec2:DescribeInstances`). Per ulteriori informazioni sugli ARN che è possibile utilizzare con le operazioni API Amazon EC2, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

La seconda istruzione utilizza le autorizzazioni a livello di risorsa per le operazioni `StopInstances` e `StartInstances`. Le istanze specifiche sono indicate dai relativi ARN nell'elemento `Resource`.

La terza istruzione consente agli utenti di chiudere tutte le istanze nella regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`) che appartengono all' AWS account specificato, ma solo se l'istanza ha il tag. "`purpose=test`" L'elemento `Condition` qualifica l'istruzione della policy applicata.

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
```

```
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:account-id:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:account-id:instance/i-0598c7d356eba48d7"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
      }
   }

   ]
}
```

Avvia istanze () RunInstances

L'azione RunInstancesAPI avvia una o più istanze On-Demand o una o più istanze Spot. `RunInstances`richiede un AMI e crea un'istanza. Gli utenti possono specificare nella richiesta una coppia di chiavi e un gruppo di sicurezza. L'avvio in un VPC richiede una sottorete e crea un'interfaccia di rete. L'avvio da un'AMI Amazon EBS-backed implica la creazione di un volume. Pertanto, gli utenti devono disporre delle autorizzazioni per utilizzare queste risorse Amazon EC2. Puoi creare un'istruzione della policy che richiede agli utenti di specificare un parametro facoltativo su `RunInstances` o limitare l'accesso degli utenti a determinati valori dei parametri.

Per ulteriori informazioni sulle autorizzazioni a livello di risorse richieste per avviare un'istanza, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Per impostazione predefinita, gli utenti non dispongono delle autorizzazioni per descrivere, avviare, arrestare o terminare le istanze risultanti. Un modo per concedere agli utenti l'autorizzazione per gestire le istanze risultanti, consiste nel creare un tag specifico per ciascuna istanza e nel creare quindi un'istruzione che consenta loro di gestire le istanze con tale tag. Per ulteriori informazioni, consulta Utilizzo delle istanze.

Risorse

- AMI
- Tipi di istanza
- Sottoreti
- Volumi EBS
- Tag
- Tag in un modello di avvio
- GPU elastiche
- Modelli di lancio

AMI

La policy seguente consente gli utenti di avviare le istanze soltanto tramite le AMI specificate, `ami-9e1670f7` e `ami-45cf5c3c`. Gli utenti non possono avviare un'istanza con altre AMI (a meno che un'altra istruzione non conceda loro l'autorizzazione corrispondente).

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-9e1670f7",
        "arn:aws:ec2:region::image/ami-45cf5c3c",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:network-interface/*"
      ]
    }
   ]
}
```

In alternativa, la policy seguente consente agli utenti di avviare le istanze da tutte le AMI di proprietà di Amazon o di determinati partner sicuri e verificati. L'elemento `Condition` della prima istruzione

verifica se `ec2:Owner` è `amazon`. Gli utenti non possono avviare un'istanza con altre AMI (a meno che un'altra istruzione non conceda loro l'autorizzazione corrispondente).

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Tipi di istanza

La policy seguente consente agli utenti di avviare le istanze soltanto tramite il tipo di istanza `t2.micro` o `t2.small` per consentire di tenere sotto controllo i costi. Gli utenti non possono avviare istanze di dimensioni maggiori perché l'elemento `Condition` della prima istruzione verifica se `ec2:InstanceType` è `t2.micro` o `t2.small`.

```
{
   "Version": "2012-10-17",
```

```
   "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

In alternativa, puoi creare una policy che nega agli utenti le autorizzazioni per avviare le istanze a eccezione dei tipi di istanza `t2.micro` e `t2.small`.

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
```

```
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Sottoreti

La policy seguente consente agli utenti di avviare le istanze soltanto tramite la sottorete `subnet-12345678` specificata. Il gruppo non può avviare le istanze in altre sottoreti (a meno che un'altra istruzione non conceda agli utenti l'autorizzazione corrispondente).

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region:account-id:subnet/subnet-12345678",
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*"
      ]
    }
   ]
}
```

In alternativa, puoi creare una policy che rifiuti agli utenti le autorizzazioni per avviare le istanze nelle altre sottoreti. Questa istruzione rifiuta l'autorizzazione per la creazione di un'interfaccia di rete, tranne se viene specificata la sottorete `subnet-12345678`. Questa negazione sostituisce le altre policy create per consentire l'avvio delle istanze in altre sottoreti.

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:network-interface/*"
      ],
      "Condition": {
         "ArnNotEquals": {
            "ec2:Subnet": "arn:aws:ec2:region:account-id:subnet/subnet-12345678"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Volumi EBS

La policy seguente consente agli utenti di avviare le istanze soltanto se i volumi EBS dell'istanza sono crittografati. Per assicurarsi che il volume root sia crittografato, gli utenti devono avviare un'istanza da un'AMI creata con snapshot crittografate. Anche gli altri eventuali volumi collegati dagli utenti all'istanza durante l'avvio devono essere crittografati.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        }
    ]
}
```

Tag

Tag di istanze durante la creazione

La policy seguente consente agli utenti di avviare le istanze e di aggiungervi dei tag durante la creazione. Per le operazioni di creazione delle risorse in cui vengono applicati i tag, gli utenti devono disporre delle autorizzazioni per utilizzare l'operazione `CreateTags`. La seconda istruzione utilizza la chiave di condizione `ec2:CreateAction` per consentire agli utenti di creare i tag soltanto nel contesto di `RunInstances` e soltanto per le istanze. Tramite la richiesta `RunInstances`, gli utenti non possono aggiungere tag alle risorse esistenti e ai volumi.

Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Tag di istanze e volumi durante la creazione con tag specifici

La policy seguente include la chiave di condizione `aws:RequestTag` che richiede agli utenti di applicare tag alle istanze e ai volumi creati da `RunInstances` con i tag `environment=production` e `purpose=webserver`. Se gli utenti non indicano questi tag specifici, o se non specificano nessun tag, la richiesta non riesce.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
```

```
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:security-group/*",
         "arn:aws:ec2:region:account-id:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:region:account-id:volume/*",
          "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/environment": "production" ,
             "aws:RequestTag/purpose": "webserver"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Tag di istanze e volumi durante la creazione con almeno un tag specifico

La policy seguente utilizza il modificatore `ForAnyValue` sulla condizione `aws:TagKeys` per indicare che occorre specificare almeno un tag nella richiesta e che deve contenere la chiave `environment` o `webserver`. I tag devono essere applicati alle istanze e ai volumi. È possibile specificare nella richiesta qualsiasi valore di tag.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:security-group/*",
         "arn:aws:ec2:region:account-id:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:region:account-id:volume/*",
          "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
          "ForAnyValue:StringEquals": {
              "aws:TagKeys": ["environment","webserver"]
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
```

```
          "StringEquals": {
              "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Se vengono applicati tag alle istanze durante la creazione, è necessario applicare un tag specifico

Nella policy seguente non è necessario che gli utenti specifichino i tag nella richiesta, ma se lo fanno, i tag devono essere di tipo `purpose=test`. Non sono consentiti altri tag. Gli utenti possono applicare i tag alle risorse compatibili con l'applicazione dei tag nella richiesta `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
          },
          "ForAllValues:StringEquals": {
              "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Per impedire a chiunque si chiami tag su create for RunInstances

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Consenti solo tag specifici per spot-instances-request. L'incoerenza numero 2 entra in gioco qui. In circostanze normali, se non si specifica alcun tag, il risultato è che non viene autenticato. Nel caso di spot-instances-request, questa politica non verrà valutata in assenza di spot-instances-request tag, pertanto una richiesta Spot on Run senza tag avrà esito positivo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

Tag in un modello di avvio

Nell'esempio seguente, gli utenti possono avviare le istanze, ma solo tramite un modello di avvio specifico (`lt-09477bcd97b0d310e`). La chiave di condizione `ec2:IsLaunchTemplateResource` impedisce agli utenti di sovrascrivere le risorse specificate nel modello di avvio. La seconda parte dell'istruzione consente agli utenti di assegnare tag alle istanze al momento della creazione; questa parte dell'istruzione è necessaria se sono stati specificati dei tag per l'istanza nel modello di avvio.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
```

```
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:instance/*",
      "Condition": {
         "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

GPU elastiche

Nella policy seguente, gli utenti possono avviare un'istanza e specificare una GPU elastica da collegare all'istanza. Gli utenti possono avviare le istanze in qualsiasi regione, ma possono collegare una GPU elastica durante l'avvio soltanto nella regione `us-east-2`.

La chiave di condizione `ec2:ElasticGpuType` garantisce che le istanze utilizzino il tipo di GPU elastica `eg1.medium` o `eg1.large`.

```
{
    "Version": "2012-10-17",
    "Statement": [
             {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:*:account-id:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2",
                    "ec2:ElasticGpuType": [
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:instance/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:volume/*",
                "arn:aws:ec2:*:account-id:key-pair/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        }
    ]
}
```

Modelli di lancio

Nell'esempio seguente, gli utenti possono avviare le istanze, ma solo tramite un modello di avvio specifico (`lt-09477bcd97b0d310e`). Gli utenti possono sovrascrivere i parametri nel modello di avvio specificandolo nell'operazione `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
```

```
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          }
       }
    }
  ]
}
```

In questo esempio, gli utenti possono avviare le istanze solo se utilizzano un modello di avvio specifico. La policy utilizza la chiave di condizione `ec2:IsLaunchTemplateResource` per impedire agli utenti di sovrascrivere qualsiasi ARN preesistente del modello di avvio.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
            "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

La policy di esempio seguente consente agli utenti di avviare le istanze, ma solo tramite un modello di avvio. Gli utenti non possono sovrascrivere i parametri di sottorete e interfaccia di rete della richiesta; tali parametri possono essere specificati soltanto nel modello di avvio. La prima parte dell'istruzione utilizza l'NotResourceelemento per consentire tutte le altre risorse tranne le sottoreti e le interfacce di rete. La seconda parte dell'istruzione consente le risorse di sottorete e interfaccia di rete, ma soltanto se provenienti dal modello di avvio.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
```

```
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:region:account-id:subnet/*",
                      "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          }
       }
    },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:region:account-id:subnet/*",
                   "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

L'esempio seguente consente agli utenti di avviare le istanze solo tramite un modello di avvio e solo se quest'ultimo dispone del tag `Purpose=Webservers`. Gli utenti non possono sovrascrivere nessuno dei parametri del modello di avvio nell'operazione `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
         "Bool": {
```

```
            "ec2:IsLaunchTemplateResource": "true"
          }
        }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
       }
     }
  ]
}
```

Utilizzo delle Istanze spot

È possibile utilizzare l' RunInstances azione per creare richieste di istanze Spot e contrassegnare le richieste di istanze Spot al momento della creazione. La risorsa da specificare RunInstances è`spot-instances-request`.

La risorsa `spot-instances-request` viene valutata nella policy IAM come segue:

- Se non tagghi una richiesta di istanza Spot al momento della creazione, Amazon EC2 non valuta la `spot-instances-request` risorsa nell' RunInstancesistruzione.
- Se tagghi una richiesta di istanza Spot al momento della creazione, Amazon EC2 valuta la `spot-instances-request` risorsa nell'istruzione. RunInstances

Pertanto, per la risorsa `spot-instances-request`, alla policy IAM si applicano le seguenti regole:

- Se utilizzi RunInstances per creare una richiesta di istanza Spot e non intendi taggare la richiesta di istanza Spot al momento della creazione, non è necessario consentire esplicitamente la `spot-instances-request` risorsa; la chiamata avrà esito positivo.
- Se utilizzi RunInstances per creare una richiesta di istanza Spot e intendi taggare la richiesta di istanza Spot al momento della creazione, devi includere la `spot-instances-request` risorsa nell'istruzione RunInstances allow, altrimenti la chiamata avrà esito negativo.
- Se utilizzi RunInstances per creare una richiesta di istanza Spot e intendi contrassegnare la richiesta di istanza Spot al momento della creazione, devi specificare la `spot-instances-`

`request` risorsa o il * carattere jolly nell'istruzione CreateTags allow, altrimenti la chiamata avrà esito negativo.

Puoi richiedere istanze Spot utilizzando RunInstances o. RequestSpotInstances I seguenti esempi di policy IAM si applicano solo quando si richiedono istanze Spot utilizzando. RunInstances

Esempio: richiedi istanze Spot utilizzando RunInstances

La seguente politica consente agli utenti di richiedere istanze Spot utilizzando l'azione RunInstances . La `spot-instances-request` risorsa, creata da RunInstances, richiede istanze Spot.

> **Note**
>
> Da utilizzare RunInstances per creare richieste di istanze Spot, puoi ometterle `spot-instances-request` dall'`Resource`elenco se non intendi taggare le richieste di istanze Spot al momento della creazione. Questo perché Amazon EC2 non valuta la `spot-instances-request` risorsa nell' RunInstancesistruzione se la richiesta dell'istanza Spot non è contrassegnata al momento della creazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
```

```
}
```

Warning

NON SUPPORTATO — Esempio: nega agli utenti l'autorizzazione a richiedere istanze Spot utilizzando RunInstances
La seguente policy non è supportata per la risorsa `spot-instances-request`.
La seguente policy intende concedere agli utenti l'autorizzazione per l'avvio di Istanze on demand, ma nega agli utenti l'autorizzazione a richiedere Istanze spot. La `spot-instances-request` risorsa, creata da RunInstances, è la risorsa che richiede le istanze Spot. La seconda affermazione ha lo scopo di negare l' RunInstances azione per la `spot-instances-request` risorsa. Tuttavia, questa condizione non è supportata perché Amazon EC2 non valuta la `spot-instances-request` risorsa nell' RunInstances istruzione se la richiesta dell'istanza Spot non è contrassegnata al momento della creazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests - NOT SUPPORTED - DO NOT USE!",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
        }
    ]
```

```
}
```

Esempio: tag di richieste di istanze spot durante la creazione

La seguente policy consente agli utenti di applicare un tag a tutte le risorse create durante l'avvio dell'istanza. La prima istruzione consente di RunInstances creare le risorse elencate. La `spot-instances-request` risorsa, creata da RunInstances, è la risorsa che richiede le istanze Spot. La seconda istruzione include il carattere jolly * per consentire a tutte le risorse l'applicazione di tag quando vengono create all'avvio dell'istanza.

> **Note**
>
> Se tagghi una richiesta di istanza Spot al momento della creazione, Amazon EC2 valuta la `spot-instances-request` risorsa nell'istruzione. RunInstances Pertanto, è necessario consentire esplicitamente alla `spot-instances-request` risorsa di eseguire l' RunInstances azione, altrimenti la chiamata avrà esito negativo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
```

```
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Esempio: assegnazione di tag di diniego durante la creazione per richieste di istanze spot

La seguente policy nega agli utenti l'autorizzazione di applicare un tag alle risorse create durante l'avvio dell'istanza.

La prima istruzione consente di RunInstances creare le risorse elencate. La `spot-instances-request` risorsa, creata da RunInstances, è la risorsa che richiede le istanze Spot. La seconda istruzione include il carattere jolly * per negare a tutte le risorse l'applicazione di tag quando vengono create all'avvio dell'istanza. Se `spot-instances-request` o qualsiasi altra risorsa viene taggata in fase di creazione, la RunInstances chiamata avrà esito negativo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
```

```
            "Resource": "*"
        }
    ]
}
```

Warning

NON SUPPORTATO - Esempio: autorizzazione per la creazione di una richiesta di istanza spot solo se è stato applicato un tag specifico
La seguente policy non è supportata per la risorsa `spot-instances-request`.
La seguente politica ha lo scopo di concedere RunInstances l'autorizzazione a creare una richiesta di istanza Spot solo se la richiesta è contrassegnata con un tag specifico.
La prima istruzione consente RunInstances di creare le risorse elencate.
La seconda istruzione intende concedere agli utenti l'autorizzazione a creare una richiesta di istanza spot solo se alla richiesta è applicato il tag `environment=production`. Se questa condizione viene applicata ad altre risorse create da RunInstances, l'indicazione di nessun tag genera un `Unauthenticated` errore. Tuttavia, se non viene specificato alcun tag per la richiesta dell'istanza Spot, Amazon EC2 non valuta la `spot-instances-request` risorsa nell' RunInstances istruzione, il che comporta la creazione di richieste di istanze Spot senza tag da. RunInstances
Tieni presente che specificare un altro tag diverso da 1 `environment=production` genera un `Unauthenticated` errore, perché se un utente tagga una richiesta di istanza Spot, Amazon EC2 valuta `spot-instances-request` la risorsa nell'istruzione. RunInstances

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
```

```
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "RequestSpotInstancesOnlyIfTagIs_environment=production - NOT
 SUPPORTED - DO NOT USE!",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }

    ]
}
```

Esempio: diniego della creazione di una richiesta di istanza spot se ha un tag specifico applicato

La seguente politica nega RunInstances l'autorizzazione a creare una richiesta di istanza Spot se la richiesta è contrassegnata con. `environment=production`

La prima istruzione consente di RunInstances creare le risorse elencate.

La seconda istruzione nega agli utenti l'autorizzazione per creare una richiesta di istanza spot se la richiesta ha il tag `environment=production`. Se si specifica `environment=production` come tag, viene generato un errore `Unauthenticated`. Se si specificano altri tag o se non si specifica alcun tag, verrà creata una richiesta di istanza spot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Esempio: utilizzo delle Istanze riservate

La policy seguente fornisce agli utenti l'autorizzazione per visualizzare, modificare e acquistare le Istanze riservate nell'account.

Non è possibile impostare le autorizzazioni a livello di risorsa per singole Istanze riservate. Questa policy significa che gli utenti hanno accesso a tutte le Istanze riservate dell'account.

L'elemento `Resource` utilizza il carattere jolly * per indicare che gli utenti possono specificare tutte le risorse tramite questa operazione; in questo caso, possono elencare e modificare tutte le Istanze riservate nell'account. Possono inoltre acquistare le Istanze riservate con le credenziali dell'account. Il carattere jolly * è necessario inoltre nei casi in cui l'operazione dell'API non supporta le autorizzazioni a livello di risorsa.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
    }
   ]
}
```

Per consentire agli utenti di visualizzare e modificare le Istanze riservate nell'account, ma non di acquistare nuove Istanze riservate.

```
{
  "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

Esempio: aggiunta di tag alle risorse

La policy seguente consente agli utenti di utilizzare l'operazione `CreateTags` per applicare tag a un'istanza soltanto se il tag contiene la chiave `environment` e il valore `production`. Non sono consentiti altri tag e l'utente non può aggiungere tag ad altri tipi di risorse.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

La policy seguente consente agli utenti di assegnare tag a tutte le risorse compatibili con l'assegnazione di tag e che dispongono già di un tag con una chiave `owner` e un valore corrispondente al nome utente. Inoltre, gli utenti devono specificare nella richiesta un tag con la chiave `anycompany:environment-type` e un valore `test` o `prod`. Gli utenti possono specificare altri tag nella richiesta.

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:*/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:RequestTag/anycompany:environment-type": ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

Puoi creare una policy IAM che consenta agli utenti di eliminare tag specifici per una risorsa. Ad esempio, la policy seguente consente agli utenti di eliminare i tag di un volume se le chiavi di tag specificate nella richiesta sono `environment` o `cost-center`. È possibile specificare qualsiasi valore per il tag, ma la chiave di tag deve corrispondere a una delle chiavi specificate.

> **Note**
>
> Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa. Gli utenti non necessitano delle autorizzazioni per utilizzare l'operazione `ec2:DeleteTags` per eliminare una risorsa con tag; necessitano soltanto delle autorizzazioni per effettuare l'operazione di eliminazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment","cost-center"]
        }
      }
    }
  ]
}
```

Questa policy consente agli utenti di eliminare soltanto il tag `environment=prod` su qualsiasi risorsa e soltanto se la risorsa dispone già di un tag con una chiave `owner` e di un valore corrispondente al nome utente. Gli utenti non possono eliminare nessun altro tag di una risorsa.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

Esempio: utilizzo dei ruoli IAM

La policy seguente consente agli utenti di collegare, sostituire e scollegare un ruolo IAM dalle istanze che includono il tag `department=test`. Per la sostituzione o lo scollegamento di un ruolo IAM è necessario un ID di associazione, pertanto la policy concede agli utenti anche l'autorizzazione per utilizzare l'operazione `ec2:DescribeIamInstanceProfileAssociations`.

Per trasferire il ruolo all'istanza, gli utenti devono disporre dell'autorizzazione per utilizzare l'operazione `iam:PassRole`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
```

```
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/DevTeam*"
    }
  ]
}
```

La policy seguente consente agli utenti di collegare o sostituire un ruolo IAM per qualsiasi istanza. Gli utenti possono collegare o sostituire soltanto i ruoli IAM il cui nome inizia con `TestRole-`. Per l'operazione `iam:PassRole`, assicurarsi di specificare il nome del ruolo IAM e non il profilo dell'istanza (se i nomi sono diversi). Per ulteriori informazioni, consulta Profili delle istanze.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/TestRole-*"
        }
    ]
}
```

Esempio: utilizzo delle tabelle di routing

La policy seguente consente agli utenti di aggiungere, rimuovere e sostituire gli instradamenti delle tabelle di routing associate soltanto al VPC `vpc-ec43eb89`. Per specificare un VPC per la chiave di condizione `ec2:Vpc`, devi specificare l'ARN completo del VPC.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-ec43eb89"
                }
            }
        }
    ]
}
```

Esempio: consentire a un'istanza specifica di visualizzare le risorse in altri AWS servizi

Di seguito è riportato un esempio di policy che è possibile collegare a un ruolo IAM. La policy consente a un'istanza di visualizzare le risorse in vari AWS servizi. Utilizza la chiave `ec2:SourceInstanceARN` global condition per specificare che l'istanza da cui viene effettuata la richiesta deve essere un'istanza`i-093452212644b0dd6`. Se lo stesso ruolo IAM è associato a un'altra istanza, l'altra istanza non può effettuare nessuna di queste operazioni.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:region:account-id:instance/
i-093452212644b0dd6"
                }
            }
        }
    ]
}
```

Esempio: utilizzo dei modelli di avvio

La policy seguente consente agli utenti di creare una versione del modello di avvio e di modificarne uno, ma solo nel caso di un modello di avvio specifico (`lt-09477bcd97b0d3abc`). Gli utenti non possono utilizzare altri modelli di lancio.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d3abc"
    }
  ]
```

```
}
```

La policy seguente consente agli utenti di eliminare i modelli di avvio e la relativa versione, purché il modello di avvio disponga del tag `Purpose=Testing`.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Action": [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Utilizzo dei metadati delle istanze

Le policy seguenti assicurano che gli utenti possano recuperare i metadati delle istanze solo utilizzando Servizio di metadati dell'istanza Versione 2 (IMDSv2). Puoi combinare le quattro policy seguenti in un'unica policy con quattro istruzioni. Se vengono combinate in un'unica policy, questa può essere utilizzata come policy di controllo dei servizi (SCP). Può funzionare altrettanto bene come policy deny applicata a una policy IAM esistente (togliendo e limitando le autorizzazioni esistenti) o come policy di controllo dei servizi (SCP) applicata a livello globale a un account, a un'unità organizzativa o a un'intera organizzazione.

> **Note**
>
> Le seguenti politiche relative alle opzioni di RunInstances metadati devono essere utilizzate insieme a una politica che fornisca le autorizzazioni principali con cui avviare un'istanza. RunInstances Se il principale non dispone anche RunInstances delle autorizzazioni, non

sarà in grado di avviare un'istanza. Per ulteriori informazioni, consulta le policy Utilizzo delle istanze e Avvia istanze () RunInstances.

Important

Se si utilizzano gruppi Auto Scaling e si deve richiedere l'uso di IMDSv2 su tutte le nuove istanze, i gruppi Auto Scaling devono utilizzare i modelli di avvio.
Quando un gruppo Auto Scaling utilizza un modello di avvio, le `ec2:RunInstances` autorizzazioni del principal IAM vengono controllate quando viene creato un nuovo gruppo Auto Scaling. Vengono inoltre controllati quando un gruppo Auto Scaling esistente viene aggiornato per utilizzare un nuovo modello di avvio o una nuova versione di un modello di avvio.
Le restrizioni sull'uso di IMDSv1 su principal IAM per `RunInstances` vengono verificate solo quando viene creato o aggiornato un gruppo Auto Scaling che utilizza un modello di avvio. Per un gruppo Auto Scaling configurato per l'utilizzo del modello di avvio `Latest` o `Default`, le autorizzazioni non vengono controllate quando viene creata una nuova versione del modello di avvio. Per controllare le autorizzazioni, è necessario configurare il gruppo Auto Scaling in modo da utilizzare una versione specifica del modello di avvio.

Per applicare l'uso di IMDSv2 su istanze lanciate dai gruppi Auto Scaling, sono necessari i seguenti passaggi aggiuntivi:

1. Disabilitare l'utilizzo delle configurazioni di avvio per tutti gli account dell'organizzazione utilizzando i limiti delle autorizzazioni IAM o le policy di controllo del servizio (SCP) per i nuovi principal creati. Per i principal IAM esistenti con autorizzazioni di gruppo Auto Scaling, aggiornare le policy associate con questa chiave di condizione. Per disabilitare l'utilizzo delle configurazioni di avvio, creare o modificare la policy IAM, il limite delle autorizzazioni o la relativa policy di controllo del servizio con la chiave di condizione `"autoscaling:LaunchConfigurationName"` con il valore specificato come `null`.
2. Per i nuovi modelli di avvio, configurare le opzioni dei metadati dell'istanza nel modello di avvio. Per i modelli di avvio esistenti, creare una nuova versione del modello di avvio e configurare le opzioni dei metadati dell'istanza nella nuova versione.
3. Nella policy che concede a qualsiasi principal l'autorizzazione per utilizzare un modello di avvio, limitare l'associazione di `$latest` e `$default` specificando `"autoscaling:LaunchTemplateVersionSpecified": "true"`. Limitando l'utilizzo a una versione specifica di un modello di avvio, è possibile assicurarsi che

vengano avviate nuove istanze utilizzando la versione in cui sono configurate le opzioni dei metadati dell'istanza. Per ulteriori informazioni, consulta il riferimento LaunchTemplateSpecificationall'API Amazon EC2 Auto Scaling, in particolare il parametro. `Version`

4. Per un gruppo Auto Scaling che utilizza una configurazione di avvio, sostituire la configurazione di avvio con un modello di avvio. Per ulteriori informazioni, consulta Sostituzione di una configurazione di avvio con un modello di avvio nella Guida per l'utente di Amazon EC2 Auto Scaling.
5. Per un gruppo Auto Scaling che utilizza un modello di avvio, assicurarsi che utilizzi un nuovo modello di avvio con le opzioni di metadati dell'istanza configurate oppure utilizzi una nuova versione del modello di avvio corrente con le opzioni dei metadati dell'istanza configurate. Per ulteriori informazioni, consulta la sezione AWS CLI Command update-auto-scaling-group Reference.

Esempi

- Richiesta dell'uso di IMDSv2
- Come negare l'esclusione da IMDSv2
- Specificare limite massimo di hop
- Limitazione di chi può modificare le opzioni dei metadati dell'istanza
- Richiesta delle credenziali del ruolo da recuperare da IMDSv2

Richiesta dell'uso di IMDSv2

La seguente politica specifica che non è possibile chiamare l' RunInstances API a meno che l'istanza non abbia anche scelto di richiedere l'uso di IMDSv2 (indicato da). `"ec2:MetadataHttpTokens": "required"` Se non si specifica che l'istanza richiede IMDSv2, viene visualizzato un errore quando si chiama l'API. `UnauthorizedOperation` RunInstances

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
```

```
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

Come negare l'esclusione da IMDSv2

La seguente policy specifica che non puoi chiamare l'API `ModifyInstanceMetadataOptions` e consentire l'opzione IMDSv1 o IMDSv2. Se chiami l'API `ModifyInstanceMetadataOptions`, l'attributo `HttpTokens` deve essere impostato su `required`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DenyIMDSv1HttpTokensModification",
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Attribute/HttpTokens": "required"
            },
            "Null": {
                "ec2:Attribute/HttpTokens": false
            }
        }
    }]
}
```

Specificare limite massimo di hop

La seguente politica specifica che non è possibile chiamare l' RunInstances API a meno che non si specifichi anche un limite di hop e il limite di hop non può essere superiore a 3. Se non lo fai, ricevi un `UnauthorizedOperation` errore quando chiami l' RunInstances API.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
               {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

Limitazione di chi può modificare le opzioni dei metadati dell'istanza

Con la policy seguente, gli utenti con il ruolo `ec2-imds-admins` potranno apportare modifiche alle opzioni di metadati dell'istanza. Se un principale diverso dal `ec2-imds-admins` ruolo tenta di chiamare l' ModifyInstanceMetadataOptions API, riceverà un `UnauthorizedOperation` errore. Questa istruzione potrebbe essere utilizzata per controllare l'uso dell' ModifyInstanceMetadataOptions API; attualmente non esistono controlli di accesso (condizioni) dettagliati per l'API. ModifyInstanceMetadataOptions

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "AllowOnlyImdsAdminsToModifySettings",
            "Effect": "Deny",
            "Action": "ec2:ModifyInstanceMetadataOptions",
            "Resource": "*",
            "Condition": {
                "StringNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/ec2-imds-admins"
                }
            }
        }
    ]
}
```

Richiesta delle credenziali del ruolo da recuperare da IMDSv2

La policy seguente specifica che se questa policy viene applicata a un ruolo e il ruolo viene assunto dal servizio EC2 e le credenziali risultanti vengono utilizzate per firmare una richiesta, la richiesta deve essere firmata dalle credenziali del ruolo EC2 recuperate da IMDSv2. In caso contrario, per tutte le relative chiamate all'API si verifica un errore `Unauthorized0peration`. Questa istruzione/policy può essere applicata a livello generale perché, se la richiesta non è firmata dalle credenziali del ruolo EC2, non ha alcun effetto.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Lavora con volumi e snapshot di Amazon EBS

Ad esempio, le politiche per l'utilizzo di volumi e snapshot di Amazon EBS, consulta Esempi di policy basate sull'identità per Amazon EBS.

Policy di esempio da utilizzare nella console Amazon EC2

Devi concedere agli utenti le autorizzazioni necessarie per Amazon EC2 utilizzando le policy IAM. È possibile utilizzare le policy IAM per concedere agli utenti le autorizzazioni per visualizzare e utilizzare risorse specifiche nella console Amazon EC2. È possibile utilizzare le politiche di esempio nella sezione precedente; tuttavia, sono progettate per le richieste effettuate con AWS CLI o un AWS SDK. Per ulteriori informazioni, consulta Politiche di esempio per lavorare con AWS CLI o un AWS SDK e Creazione di policy IAM nella Guida per l'utente IAM.

La console utilizza operazioni API aggiuntive per le relative caratteristiche. Pertanto, queste policy potrebbero non funzionare come previsto. Ad esempio, un utente con l'autorizzazione per l'utilizzo solo dell'operazione API `DescribeVolumes` riscontrerà errori quando cerca di visualizzare i volumi nella console. In questa sezione sono descritte le policy che consentono agli utenti di utilizzare parti specifiche della console. Per ulteriori informazioni sulla creazione di politiche per la console Amazon EC2, consulta il seguente post sul blog sulla AWS sicurezza: Granting Users Permission to Work in the Amazon EC2 Console.

> **Tip**
>
> Per individuare le operazioni API necessarie per eseguire le attività nella console, puoi utilizzare un servizio, ad esempio AWS CloudTrail. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail. Se la policy non concede l'autorizzazione per creare o modificare una risorse specifica, nella console viene visualizzato un messaggio codificato con informazioni di diagnostica. Puoi decodificare il messaggio utilizzando l'azione DecodeAuthorizationMessageAPI for o AWS STS il decode-authorization-messagecomando in. AWS CLI

Esempi

- Esempio: accesso in sola lettura
- Esempio: utilizzo della procedura guidata per l'avvio dell'istanza EC2
- Esempio: utilizzo dei gruppi di sicurezza
- Esempio: utilizzo degli indirizzi IP elastici
- Esempio: utilizzo delle Istanze riservate

Esempio: accesso in sola lettura

Per consentire agli utenti di visualizzare tutte le risorse nella console Amazon EC2, è possibile utilizzare la stessa policy impiegata nel seguente esempio: Esempio: accesso in sola lettura. Gli utenti non possono eseguire operazioni su queste risorse o creare nuove risorse a meno che un'altra istruzione conceda loro l'autorizzazione corrispondente.

Visualizzazione di istanze, AMI e snapshot

In alternativa, puoi concedere l'accesso in sola lettura a un sottoinsieme di risorse. A tale scopo, sostituisci il carattere jolly * nell'operazione API `ec2:Describe` con operazioni `ec2:Describe`

specifiche per ciascuna risorsa. La seguente policy consente agli utenti di visualizzare tutte le istanze, AMI e snapshot nella console Amazon EC2. L'operazione `ec2:DescribeTags` consente agli utenti di visualizzare le AMI pubbliche. La console richiede le informazioni di tagging per visualizzare le AMI pubbliche. Tuttavia, puoi rimuovere questa operazione per consentire agli utenti di visualizzare solo le AMI private.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeTags",
         "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
   }
   ]
}
```

> **Note**
>
> Le operazioni API di Amazon EC2 `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa, pertanto non è possibile controllare le singole risorse che gli utenti possono visualizzare nella console. Il carattere jolly * è quindi necessario nell'elemento `Resource` dell'istruzione precedente. Per ulteriori informazioni sugli ARN che è possibile utilizzare con le operazioni API Amazon EC2, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Visualizza istanze e metriche CloudWatch

La seguente policy consente agli utenti di visualizzare le istanze nella console Amazon EC2, CloudWatch nonché gli allarmi e i parametri nella scheda Monitoraggio della pagina Istanze. La console Amazon EC2 utilizza l' CloudWatch API per visualizzare gli allarmi e le metriche, quindi è necessario concedere agli utenti l'autorizzazione a utilizzare le azioni`cloudwatch:DescribeAlarms`,,

`cloudwatch:DescribeAlarmsForMetric`cloudwatch:ListMetrics, `cloudwatch:GetMetricStatistics` e. `cloudwatch:GetMetricData`

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:DescribeAlarmsForMetric",
         "cloudwatch:ListMetrics",
         "cloudwatch:GetMetricStatistics",
         "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
   }
   ]
}
```

Esempio: utilizzo della procedura guidata per l'avvio dell'istanza EC2

La procedura guidata per l'avvio dell'istanza Amazon EC2 è una schermata contenente opzioni per la configurazione e l'avvio di un'istanza. La policy deve includere l'autorizzazione per l'utilizzo delle operazioni API che consentono agli utenti di utilizzare le opzioni della procedura guidata. Se la policy non include l'autorizzazione per l'utilizzo di tali operazioni, alcuni elementi della procedura guidata potrebbero non venire caricati correttamente e gli utenti potrebbero non essere in grado di completare il processo di avvio.

Accesso di base alla procedura guidata per l'avvio dell'istanza

Per completare un processo di avvio correttamente, gli utenti devono disporre dell'autorizzazione per l'uso dell'operazione API `ec2:RunInstances` e almeno delle seguenti operazioni API:

- `ec2:DescribeImages`: per visualizzare e selezionare un'AMI.
- `ec2:DescribeInstanceTypes`: per visualizzare e selezionare un tipo di istanza.
- `ec2:DescribeVpcs`: Per visualizzare le opzioni di rete disponibili.
- `ec2:DescribeSubnets`: Per visualizzare tutte le sottoreti disponibili per il VPC scelto.

- `ec2:DescribeSecurityGroups` o `ec2:CreateSecurityGroup`: per visualizzare e selezionare un gruppo di sicurezza esistente o crearne uno nuovo.
- `ec2:DescribeKeyPairs` o `ec2:CreateKeyPair`: per selezionare una coppia di chiavi esistente o per crearne una nuova.
- `ec2:AuthorizeSecurityGroupIngress`: per aggiungere le regole in entrata.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

Puoi aggiungere operazioni API alla policy per mettere a disposizione opzioni aggiuntive per gli utenti, ad esempio:

- `ec2:DescribeAvailabilityZones`: Per visualizzare e selezionare una zona di disponibilità specifica.
- `ec2:DescribeNetworkInterfaces`: Per visualizzare e selezionare le interfacce di rete esistenti per la sottorete selezionata.

- Per aggiungere regole in uscita ai gruppi di sicurezza VPC, è necessario concedere agli utenti l'autorizzazione per utilizzare l'operazione API `ec2:AuthorizeSecurityGroupEgress`. Per modificare o eliminare le regole esistenti, è necessario concedere agli utenti l'autorizzazione per utilizzare l'operazione API `ec2:RevokeSecurityGroup*` corrispondente.
- `ec2:CreateTags`: per applicare tag alle risorse create da `RunInstances`. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione. Se gli utenti non dispongono dell'autorizzazione per utilizzare questa operazione e tentano di applicare tag nella pagina relativa al tagging della procedura guidata per l'avvio dell'istanza, l'avvio ha esito negativo.

  > **Important**
  >
  > Se si specifica un Name (Nome) durante l'avvio di un'istanza viene creato un tag e viene richiesta l'operazione `ec2:CreateTags`. Prestare particolare attenzione quando si concede agli utenti l'autorizzazione per l'uso dell'operazione `ec2:CreateTags`, perché questo limita la possibilità di utilizzare la chiave di condizione `aws:ResourceTag` per limitare l'utilizzo di altre risorse. Se si concede agli utenti l'autorizzazione a utilizzare l'operazione `ec2:CreateTags`, è possibile modificare il tag di una risorsa per ignorare tali restrizioni. Per ulteriori informazioni, consulta Controllo dell'accesso alle risorse EC2 mediante i tag delle risorse.

- Per utilizzare parametri Systems Manager durante la selezione di un'AMI, è necessario aggiungere `ssm:DescribeParameters` e `ssm:GetParameters` alla policy. `ssm:DescribeParameters` concede agli utenti l'autorizzazione per visualizzare e selezionare i parametri Systems Manager. `ssm:GetParameters` concede agli utenti l'autorizzazione per ottenere i valori dei parametri Systems Manager. Puoi inoltre limitare l'accesso a parametri Systems Manager specifici. Per ulteriori informazioni, consulta Limitare l'accesso a parametri Systems Manager specifici in seguito in questa sezione.

Attualmente, le operazioni API `Describe*` di Amazon EC2 non supportano le autorizzazioni a livello di risorsa, pertanto non è possibile limitare le singole risorse che gli utenti possono visualizzare nella procedura guidata per l'avvio dell'istanza. Puoi tuttavia applicare autorizzazioni a livello di risorsa nell'operazione API `ec2:RunInstances` per limitare le risorse che gli utenti possono utilizzare per avviare un'istanza. L'avvio ha esito negativo se gli utenti selezionano opzioni che non sono autorizzati a usare.

Limitazione dell'accesso a un tipo di istanza, sottorete e regione specifici

La seguente policy consente gli utenti di avviare istanze `t2.micro` tramite le AMI di proprietà di Amazon e solo in una sottorete specifica (`subnet-1a2b3c4d`). Gli utenti possono eseguire l'avvio solo nella regione `sa-east-1`. Se gli utenti selezionano una regione diversa oppure se selezionano un tipo di istanza, un'AMI o una sottorete diversa nella procedura guidata per l'avvio dell'istanza, l'avvio avrà esito negativo.

La prima istruzione concede agli utenti l'autorizzazione per visualizzare le opzioni nella procedura guidata per l'avvio dell'istanza o di crearne di nuove, come illustrato nell'esempio precedente. La seconda istruzione concede agli utente l'autorizzazione per utilizzare l'interfaccia di rete, il volume, la coppia di chiavi, il gruppo di sicurezza e le risorse della sottorete per l'operazione `ec2:RunInstances`. Questi elementi sono obbligatori per l'avvio di un'istanza in un VPC. Per ulteriori informazioni sull'uso dell'operazione `ec2:RunInstances`, consulta Avvia istanze () RunInstances. La terza e la quarta istruzione concedono agli utenti l'autorizzazione per utilizzare rispettivamente le risorse dell'istanza e le risorse dell'AMI, ma solo se l'istanza è un'istanza `t2.micro` e solo se l'AMI è di proprietà di Amazon o di determinati partner sicuri e verificati.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeKeyPairs",
         "ec2:CreateKeyPair",
         "ec2:DescribeVpcs",
         "ec2:DescribeSubnets",
         "ec2:DescribeSecurityGroups",
         "ec2:CreateSecurityGroup",
         "ec2:AuthorizeSecurityGroupIngress"
   ],
   "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action":"ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:sa-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:sa-east-1:111122223333:volume/*",
         "arn:aws:ec2:sa-east-1:111122223333:key-pair/*",
```

```
            "arn:aws:ec2:sa-east-1:111122223333:security-group/*",
            "arn:aws:ec2:sa-east-1:111122223333:subnet/subnet-1a2b3c4d"
        ]
    },
    {
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": [
            "arn:aws:ec2:sa-east-1:111122223333:instance/*"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": [
              "arn:aws:ec2:sa-east-1::image/ami-*"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:Owner": "amazon"
            }
        }
    }
    ]
}
```

Limitazione dell'accesso a parametri Systems Manager specifici

La policy seguente concede l'accesso all'utilizzo di parametri Systems Manager con un nome specifico.

La prima istruzione concede agli utenti l'autorizzazione per visualizzare parametri Systems Manager quando si seleziona un'AMI nella procedura guidata per l'avvio dell'istanza. La seconda istruzione concede agli utenti l'autorizzazione a utilizzare solo i parametri denominati `prod-*`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
```

```
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:us-east-2:123456123:parameter/prod-*"
   }
   ]
}
```

Esempio: utilizzo dei gruppi di sicurezza

Visualizzazione dei gruppi di sicurezza e aggiunta e rimozione delle regole

La seguente policy concede agli utenti l'autorizzazione per visualizzare i gruppi di sicurezza nella console Amazon EC2 e per aggiungere e rimuovere le regole in entrata e in uscita e per elencare e modificare le descrizioni delle regole per i gruppi di sicurezza esistenti associati al tag `Department=Test`.

Nella prima istruzione, l'operazione `ec2:DescribeTags` consente agli utenti di visualizzare i tag nella console e ciò semplifica l'identificazione dei gruppi di sicurezza che gli utenti possono modificare.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
         "ec2:DescribeSecurityGroupRules",
         "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:ModifySecurityGroupRules",
            "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
            "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
        ],
        "Resource": [
            "arn:aws:ec2:region:111122223333:security-group/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/Department": "Test"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:ModifySecurityGroupRules"
        ],
        "Resource": [
            "arn:aws:ec2:region:111122223333:security-group-rule/*"
        ]
    }
]}
```

Utilizzo della finestra di dialogo Create Security Group (Crea un gruppo di sicurezza)

È possibile creare una policy che consenta agli utenti di utilizzare la finestra di dialogo Create Security Group (Crea un gruppo di sicurezza) nella console Amazon EC2. Per utilizzare questa finestra di dialogo, gli utenti devono disporre dell'autorizzazione per l'uso almeno delle seguenti operazioni API:

- `ec2:CreateSecurityGroup`: per creare un nuovo gruppo di sicurezza.
- `ec2:DescribeVpcs`: Per visualizzare un elenco di VPC esistenti nell'elenco VPC.

Con queste autorizzazioni, gli utenti possono creare un nuovo gruppo di sicurezza, ma non possono aggiungervi regole. Per utilizzare regole nella finestra di dialogo Create Security Group (Crea un gruppo di sicurezza), è possibile aggiungere le seguenti operazioni API alla policy:

- `ec2:AuthorizeSecurityGroupIngress`: per aggiungere le regole in entrata.
- `ec2:AuthorizeSecurityGroupEgress`: per aggiungere le regole in uscita al gruppo di sicurezza VPC.
- `ec2:RevokeSecurityGroupIngress`: per modificare o eliminare le regole in uscita esistenti. Ciò risulta utile per consentire agli utenti di utilizzare la caratteristica Copy to new (Copia su nuovo) nella console. Questa caratteristica consente di aprire la finestra di dialogo Create Security Group (Crea un gruppo di sicurezza) e popolarlo con le stesse regole del gruppo di sicurezza selezionato.
- `ec2:RevokeSecurityGroupEgress`: per modificare o eliminare le regole in uscita per i gruppi di sicurezza VPC. Ciò risulta utile per consentire agli utenti di modificare o eliminare la regola in uscita di default che autorizza tutto il traffico in uscita.
- `ec2:DeleteSecurityGroup`: da specificare quando non è possibile salvare regole non valide. La console crea innanzitutto il gruppo di sicurezza e quindi aggiunge le regole specificate. Se le regole non sono valide, l'operazione ha esito negativo e la console cerca di eliminare il gruppo di sicurezza. L'utente rimane nella finestra di dialogo Create Security Group (Crea un gruppo di sicurezza) in modo da consentirgli di correggere la regola non valida e provare a creare di nuovo il gruppo di sicurezza. Questa operazione API non è obbligatoria, ma se un utente non riceve l'autorizzazione per utilizzarla e tenta di creare un gruppo di sicurezza con regole non valide, il gruppo di sicurezza viene creato senza regole. L'utente dovrà quindi aggiungere le regole in un secondo momento.
- `ec2:UpdateSecurityGroupRuleDescriptionsIngress`: per aggiungere o aggiornare le descrizioni delle regole dei gruppi di sicurezza in entrata (inbound).
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress`: per aggiungere o aggiornare le descrizioni delle regole del gruppo di sicurezza in uscita (outbound).
- `ec2:ModifySecurityGroupRules`: per modificare modify-security-group-rules.
- `ec2:DescribeSecurityGroupRules`: per elencare le regole dei gruppi di sicurezza.

La seguente policy concede agli utenti l'autorizzazione per utilizzare la finestra di dialogo Create Security Group (Crea un gruppo di sicurezza) e per creare le regole in entrata e in uscita per i gruppi di sicurezza associati a un VPC specifico (`vpc-1a2b3c4d`). Gli utenti possono creare i gruppi di sicurezza per EC2-Classic o un altro VPC, ma non possono aggiungervi regole. In modo analogo, gli utenti non possono aggiungere regole ai gruppi di sicurezza esistenti che non sono associati al VPC `vpc-1a2b3c4d`. Agli utenti viene inoltre concesso l'autorizzazione per visualizzare tutti i gruppi di sicurezza nella console. Ciò aiuta gli utenti a identificare i gruppi di sicurezza a cui possono

aggiungere regole in entrata. Inoltre, questa policy concede agli utenti l'autorizzazione per eliminare i gruppi di sicurezza associati al VPC `vpc-1a2b3c4d`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:111122223333:vpc/vpc-1a2b3c4d"
         }
      }
    }
   ]
}
```

Esempio: utilizzo degli indirizzi IP elastici

Per consentire agli utenti di visualizzare gli indirizzi IP elastici nella console Amazon EC2, è necessario concedergli l'autorizzazione per utilizzare l'operazione `ec2:DescribeAddresses`.

Per consentire agli utenti di utilizzare gli indirizzi IP elastici, puoi aggiungere le seguenti operazioni alla policy.

- `ec2:AllocateAddress`: Per allocare un indirizzo IP elastico.
- `ec2:ReleaseAddress`: per rilasciare un indirizzo IP elastico.

- `ec2:AssociateAddress`: per associare un indirizzo IP elastico a un'istanza o un'interfaccia di rete.
- `ec2:DescribeNetworkInterfaces` ed `ec2:DescribeInstances`: Per utilizzare la schermata Associate address (Associa indirizzo). Nella schermata sono visualizzate le istanze disponibili o le interfacce di rete a cui puoi associare un indirizzo IP elastico.
- `ec2:DisassociateAddress`: per annullare l'associazione di un indirizzo IP elastico a un'istanza o un'interfaccia di rete.

La seguente policy consente agli utenti di visualizzare, allocare e associare indirizzi IP elastici alle istanze. Gli utenti non possono associare gli indirizzi IP elastici alle interfacce di rete, annullare l'associazione degli indirizzi IP elastici o rilasciarli.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

Esempio: utilizzo delle Istanze riservate

La seguente policy consente agli utenti di visualizzare e modificare le istanze riservate nell'account, nonché acquistare nuove istanze riservate nella AWS Management Console.

Questa policy consente agli utenti di visualizzare tutte le Istanze riservate, così come Istanze on demand, nell'account. Non è possibile impostare le autorizzazioni a livello di risorsa per singole Istanze riservate.

```
{
   "Version": "2012-10-17",
```

```
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
         "ec2:ModifyReservedInstances",
         "ec2:PurchaseReservedInstancesOffering",
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeAvailabilityZones",
         "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
   }
   ]
}
```

L'operazione `ec2:DescribeAvailabilityZones` è necessaria affinché la console Amazon EC2 sia in grado di visualizzare le informazioni sulle zone di disponibilità in cui è possibile acquistare le Istanze riservate. L'operazione `ec2:DescribeInstances` non è obbligatoria, ma fa sì che l'utente possa visualizzare le istanze nell'account e possa acquistare prenotazioni conformi alle specifiche corrette.

Puoi modificare le operazioni API per limitare l'accesso utente, ad esempio la rimozione di `ec2:DescribeInstances` ed `ec2:DescribeAvailabilityZones` indica che l'utente dispone dell'accesso in sola lettura.

AWS politiche gestite per Amazon EC2

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le policy AWS gestite che scriverle autonomamente. Creare policy gestite dal cliente IAM per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando

diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: AmazonEC2FullAccess

Puoi collegare la policy `AmazonEC2FullAccess` alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso completo ad Amazon EC2.

Per visualizzare le autorizzazioni relative a questa politica, consulta il Managed Policy AmazonEC2FullAccessReference.AWS

AWS politica gestita: AmazonEC2ReadOnlyAccess

Puoi collegare la policy `AmazonEC2ReadOnlyAccess` alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso in sola lettura ad Amazon EC2.

Per visualizzare le autorizzazioni per questa policy, consulta AmazonEC2ReadOnlyAccessil AWS Managed Policy Reference.

AWS politica gestita: AWSEC2CapacityReservationFleetRolePolicy

Questa policy è collegata al ruolo collegato ai servizi denominato AWSServiceRoleForEC2CapacityReservationFleet per consentire alle prenotazioni della capacità di creare, modificare e annullare le prenotazioni di capacità per il proprio conto. Per ulteriori informazioni, consulta Ruolo collegato ai servizi per il parco istanze di prenotazione della capacità.

Per visualizzare le autorizzazioni per questa policy, consulta AWSEC2CapacityReservationFleetRolePolicyil AWS Managed Policy Reference.

AWS politica gestita: AWSEC2FleetServiceRolePolicy

Questa policy è collegato al ruolo collegato ai servizi denominato AWSServiceRoleForEC2Fleet per consentire al parco istanze EC2 di richiedere, avviare, terminare e taggare le istanze per il proprio conto. Per ulteriori informazioni, consulta Ruolo collegato al servizio per parco istanze EC2.

Per visualizzare le autorizzazioni per questa politica, consulta AWSEC2FleetServiceRolePolicyil AWS Managed Policy Reference.

AWS politica gestita: AWSEC2SpotFleetServiceRolePolicy

Questa policy è collegata al ruolo collegato ai servizi denominato AWSServiceRoleForEC2SpotFleet per consentire al parco istanze spot di avviare e gestire le istanze per il proprio conto. Per ulteriori informazioni, consulta Ruolo collegato al servizio per il parco istanze spot.

Per visualizzare le autorizzazioni per questa politica, consulta AWSEC2SpotFleetServiceRolePolicyil AWS Managed Policy Reference.

AWS politica gestita: AWSEC2SpotServiceRolePolicy

Questa policy è collegata al ruolo collegato ai servizi denominato AWSServiceRoleForEC2Spot per consentire ad Amazon EC2 di avviare e gestire le istanze spot per il proprio conto. Per ulteriori informazioni, consulta Ruolo collegato ai servizi per le richieste di istanza spot.

Per visualizzare le autorizzazioni per questa politica, consulta AWSEC2SpotServiceRolePolicyil AWS Managed Policy Reference.

AWS politica gestita: AWSEC2VssSnapshotPolicy

Puoi collegare questa policy gestita al ruolo del profilo dell'istanza IAM che usi per le tue istanze Amazon EC2 Windows. La policy concede le autorizzazioni per consentire ad Amazon EC2 di creare e gestire istantanee VSS per tuo conto.

Per visualizzare le autorizzazioni per questa policy, consulta AWSEC2VssSnapshotPolicyil Managed Policy Reference.AWS

AWS politica gestita: EC2FastLaunchFullAccess

Puoi allegare la `EC2FastLaunchFullAccess` policy al tuo profilo di istanza o a un altro ruolo IAM. Questa policy garantisce l'accesso completo alle azioni di EC2 Fast Launch e autorizzazioni mirate come segue.

Dettagli dell'autorizzazione

- EC2 Fast Launch: viene concesso l'accesso amministrativo, in modo che il ruolo possa abilitare o disabilitare EC2 Fast Launch e descrivere le immagini di EC2 Fast Launch.

- Amazon EC2: l'accesso è concesso per Amazon RunInstances EC2 CreateTags e descrivi le azioni necessarie per verificare le autorizzazioni delle risorse.
- IAM: viene concesso l'accesso per ottenere e utilizzare profili di istanza il cui nome contiene la creazione del EC2FastLaunchServiceRolePolicy ruolo `ec2fastlaunch` collegato al servizio.

Per visualizzare le autorizzazioni relative a questa policy, consulta il AWS Managed Policy EC2FastLaunchFullAccessReference.

AWS politica gestita: EC2FastLaunchServiceRolePolicy

Questa policy è associata al ruolo collegato al servizio denominato per consentire AWSServiceRoleForEC2FastLaunchad Amazon EC2 di creare e gestire una serie di snapshot preimpostate che riducono il tempo necessario per avviare le istanze dall'AMI abilitata per EC2 Fast Launch. Per ulteriori informazioni, consulta the section called “Ruolo collegato al servizio”.

Per visualizzare le autorizzazioni relative a questa policy, consulta il Managed Policy Reference. EC2FastLaunchServiceRolePolicyAWS

AWS politica gestita: Ec2InstanceConnectEndpoint

Questa policy è associata a un ruolo collegato al servizio denominato AWSServiceRoleForEC2InstanceConnectper consentire a EC2 Instance Connect Endpoint di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Ruolo collegato ai servizi per l'endpoint EC2 Instance Connect.

Per visualizzare le autorizzazioni relative a questa policy, consulta il Managed Policy Reference Ec2InstanceConnectEndpoint.AWS

Amazon EC2 si aggiorna alle AWS politiche gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon EC2 da quando questo servizio ha iniziato a tracciare queste modifiche.

Modifica	Descrizione	Data
EC2FastLaunchFullAccess: nuova policy	Amazon EC2 ha aggiunto questa policy per eseguire azioni API relative alla	14 maggio 2024

Modifica	Descrizione	Data
	funzionalità EC2 Fast Launch da un'istanza. La policy può essere allegata al profilo dell'istanza per un'istanza lanciata da un'AMI abilitata per EC2 Fast Launch.	
AWSEC2VssSnapshotPolicy: nuova policy	Amazon EC2 ha aggiunto la `AWSEC2VssSnapshotPolicy` policy che contiene le autorizzazioni per creare e aggiungere tag alle Amazon Machine Images (AMI) e agli snapshot EBS.	28 marzo 2024
EC2FastLaunchServiceRolePolicy: nuova policy	Amazon EC2 ha aggiunto la funzionalità EC2 Fast Launch per consentire alle AMI Windows di avviare le istanze più velocemente creando una serie di snapshot preimpostate.	26 novembre 2021
Amazon EC2 ha iniziato a monitorare le modifiche	Amazon EC2 ha iniziato a tracciare le modifiche alle sue AWS politiche gestite	1 marzo 2021

Ruoli IAM per Amazon EC2

Le applicazioni devono firmare le proprie richieste API con AWS credenziali. Pertanto, se sei uno sviluppatore di applicazioni, avrai bisogno di una strategia per gestire le credenziali per le applicazioni eseguite su istanze EC2. Ad esempio, puoi distribuire in modo sicuro le credenziali AWS alle istanze, consentendo alle applicazioni eseguite su tali istanze di utilizzare le credenziali per firmare le richieste, e contemporaneamente proteggere le credenziali da altri utenti. Tuttavia, è difficile distribuire in modo sicuro le credenziali a ciascuna istanza, specialmente a quelle AWS create per

tuo conto, come le istanze Spot o le istanze nei gruppi di Auto Scaling. Inoltre, devi essere in grado di aggiornare le credenziali su ogni istanza quando ruoti le credenziali. AWS

> **Note**
>
> Per i tuoi carichi di lavoro Amazon EC2, ti consigliamo di recuperare le credenziali di sessione utilizzando il metodo descritto di seguito. Queste credenziali dovrebbero consentire al carico di lavoro di effettuare richieste di API AWS , senza dover utilizzare `sts:AssumeRole` per assumere lo stesso ruolo già associato all'istanza. A meno che non sia necessario passare i tag di sessione per il controllo degli accessi basato sugli attributi (ABAC) o passare una policy di sessione per limitare ulteriormente le autorizzazioni del ruolo, tali chiamate di assunzione del ruolo non sono necessarie in quanto creano un nuovo set delle stesse credenziali di sessione del ruolo temporaneo.
> Se il carico di lavoro utilizza un ruolo per assumere se stesso, devi creare una policy di attendibilità che consenta esplicitamente a tale ruolo di assumere se stesso. Se non crei la policy di attendibilità, ricevi l'errore `AccessDenied`. Per ulteriori informazioni, consulta Modifica di una policy di attendibilità di un ruolo nella Guida per l'utente di IAM.

Abbiamo sviluppato i ruoli IAM in modo da consentire alle applicazioni di eseguire in modo sicuro le richieste API dalle istanze senza la necessità di gestire le credenziali di sicurezza utilizzate dalle applicazioni stesse. Invece di creare e distribuire AWS le tue credenziali, puoi delegare l'autorizzazione a effettuare richieste API utilizzando i ruoli IAM nel modo seguente:

1. Crea un ruolo IAM.
2. Definisci quali account o AWS servizi possono assumere il ruolo.
3. Definire le operazioni e le risorse API che l'applicazione può utilizzare dopo l'assunzione del ruolo.
4. Specificare il ruolo quando avvii l'istanza o quando associ il ruolo a un'istanza esistente.
5. Impostare l'applicazione in modo che recuperi un set di credenziali temporanee e le utilizzi.

Ad esempio, puoi utilizzare i ruoli IAM per concedere le autorizzazioni alle applicazioni eseguite su istanze che devono utilizzare un bucket in Amazon S3. Puoi specificare le autorizzazioni per i ruoli IAM mediante la creazione di una policy in formato JSON. Si tratta di policy simili a quelle create per gli utenti . Se modifichi un ruolo, la modifica verrà propagata a tutte le istanze.

> **Note**
>
> Le credenziali del ruolo IAM di Amazon EC2 non sono soggette alla durata massima delle sessioni configurata nel ruolo. Per ulteriori informazioni, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

Durante la creazione di ruoli IAM, associa policy IAM con privilegi minimi che limitano l'accesso alle chiamate API specifiche richieste dall'applicazione. Per la comunicazione Windows-to-Windows, utilizza gruppi e ruoli Windows ben definiti e ben documentati per concedere l'accesso a livello di applicazione tra istanze di Windows. Gruppi e ruoli consentono ai clienti di definire le autorizzazioni a livello di cartella NTFS con privilegi minimi per l'applicazione e le autorizzazioni a livello di cartella NTFS per limitare l'accesso ai requisiti specifici dell'applicazione.

È possibile associare un solo ruolo IAM a un'istanza, ma è possibile associare lo stesso ruolo a molte istanze. Per ulteriori informazioni sulla creazione e sull'utilizzo dei ruoli IAM, consulta la sezione relativa ai ruoli nella Guida per l'utente di IAM.

Puoi applicare le autorizzazioni a livello di risorsa alle policy IAM per controllare la capacità degli utenti di collegare, sostituire o scollegare i ruoli IAM per un'istanza. Per ulteriori informazioni, consulta Autorizzazioni a livello di risorsa supportate per le operazioni API Amazon EC2 e l'esempio seguente: Esempio: utilizzo dei ruoli IAM.

Indice

Profili delle istanze

Amazon EC2 utilizza un profilo dell'istanza come container per un ruolo IAM. Quando crei un ruolo IAM utilizzando la console IAM, la console crea automaticamente un profilo dell'istanza e le assegna lo stesso nome del ruolo a cui corrisponde. Se utilizzi la console Amazon EC2 per avviare un'istanza con un ruolo IAM o per collegare un ruolo IAM a un'istanza, scegli il ruolo in base all'elenco di nomi di profilo delle istanze.

Se utilizzi l' AWS CLI API o un AWS SDK per creare un ruolo, crei il ruolo e il profilo dell'istanza come azioni separate, con nomi potenzialmente diversi. Se poi utilizzi l' AWS CLI API o un AWS SDK per avviare un'istanza con un ruolo IAM o per associare un ruolo IAM a un'istanza, specifica il nome del profilo dell'istanza.

Un profilo dell'istanza può contenere solo un ruolo IAM. Questo limite non può essere aumentato.

Per ulteriori informazioni, consulta la sezione relativa ai profili delle istanze nella Guida per l'utente di IAM.

Recupero delle credenziali di sicurezza dai metadati delle istanze

Un'applicazione in un'istanza recupera le credenziali di sicurezza fornite dal ruolo dalla voce `iam/security-credentials/role-name` nei metadati dell'istanza. All'applicazione vengono concesse le autorizzazioni per le operazioni e le risorse definite per il ruolo tramite le credenziali di sicurezza associate al ruolo. Queste credenziali di sicurezza sono temporanee e sono caratterizzate da un piano di rotazione automatica. Ciò significa che rendiamo disponibili nuove credenziali almeno cinque minuti prima della scadenza delle vecchie credenziali.

> **Warning**
>
> Se utilizzi servizi che usano metadati delle istanze con i ruoli IAM, assicurati di non esporre le credenziali quando i servizi effettuano chiamate HTTP per tuo conto. I tipi di servizi che possono esporre le credenziali includono i proxy HTTP, i servizi validatore HTML/CSS e i processori XML che supportano l'inclusione XML.

Il comando seguente recupera le credenziali di sicurezza per un ruolo IAM denominato `s3access`.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/
s3access
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/s3access
```

Di seguito è riportato un output di esempio.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
}
```

Per le applicazioni e PowerShell i comandi Tools for Windows eseguiti sull'istanza, non è necessario ottenere in modo esplicito le credenziali di sicurezza temporanee: gli AWS SDK e Tools for Windows ottengono PowerShell automaticamente le credenziali dal servizio di metadati dell'istanza EC2 e le utilizzano. AWS CLI AWS CLI Per eseguire una chiamata esternamente all'istanza utilizzando le credenziali di sicurezza temporanee, ad esempio per testare le policy IAM, è necessario fornire la chiave di accesso, la chiave segreta e il token di sessione. Per ulteriori informazioni, consulta Utilizzo

delle credenziali di sicurezza temporanee per richiedere l'accesso alle risorse nella Guida per l'utente IAM. AWS

Per ulteriori informazioni sui metadati delle istanze, consulta Utilizzo dei metadati delle istanze. Per informazioni sull'indirizzo IP dei metadati dell'istanza, consulta Recupero dei metadati dell'istanza.

Concessione a un utente dell'autorizzazione a trasferire un ruolo IAM a un'istanza

Per consentire a un utente di avviare un'istanza con un ruolo IAM o per collegare o sostituire un ruolo IAM per un'istanza esistente, devi concedere all'utente l'autorizzazione a utilizzare le seguenti operazioni API:

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

Ad esempio, la policy IAM seguente concede agli utenti l'autorizzazione ad avviare istanze con un ruolo IAM o a collegare o sostituire un ruolo IAM per un'istanza esistente tramite la AWS CLI.

> **Note**
>
> Questa policy concede agli utenti l'accesso a tutti i ruoli specificando la risorsa come * nella policy. Tuttavia, si prega di tenere conto del principio del privilegio minimo come best practice.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
         "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

Per concedere agli utenti l'autorizzazione per avviare le istanze con un ruolo IAM o per collegare o sostituire un ruolo IAM per un'istanza esistente tramite la console Amazon EC2, devi concedere loro l'autorizzazione ad utilizzare `iam:ListInstanceProfiles`, `iam:PassRole`,`ec2:AssociateIamInstanceProfile` e `ec2:ReplaceIamInstanceProfileAssociation` oltre a qualsiasi altra autorizzazione di cui potrebbero aver bisogno. Per esempi di policy, consulta Policy di esempio da utilizzare nella console Amazon EC2.

Utilizzo dei ruoli IAM

Puoi creare un ruolo IAM e collegarlo a un'istanza durante o dopo l'avvio. Puoi inoltre sostituire o scollegare un ruolo IAM per un'istanza.

Indice

Creare un ruolo IAM.

Devi creare un ruolo IAM prima di poter avviare un'istanza utilizzando tale ruolo o di collegarlo a un'istanza.

Console

Per creare un ruolo IAM utilizzando la console IAM

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione seleziona Ruoli, quindi scegli Crea ruolo.

3. Nella pagina Seleziona entità attendibile scegli Servizio AWS, quindi seleziona il caso d'uso EC2. Seleziona Successivo.
4. Nella pagina Aggiungi autorizzazioni seleziona una policy che concede alle istanze l'accesso alle risorse necessarie. Seleziona Successivo.
5. Nella pagina Nomina, verifica e crea, immetti un nome e una descrizione per il ruolo. Facoltativamente, aggiungi i tag al ruolo. Scegli Crea ruolo.

Command line

Nell'esempio seguente viene creato un ruolo IAM con una policy che consente al ruolo di utilizzare un bucket Amazon S3.

Come creare un ruolo e il profilo dell'istanza IAM (AWS CLI)

1. Creare la seguente policy di attendibilità e salvarla in un file di testo denominato `ec2-role-trust-policy.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Creare il ruolo `s3access` e specificare la policy di attendibilità creata utilizzando il comando create-role.

```
aws iam create-role \
    --role-name s3access \
    --assume-role-policy-document file://ec2-role-trust-policy.json
```

Example response

```
{
    "Role": {
        "AssumeRolePolicyDocument": {
```

```
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    }
                }
            ]
        },
        "RoleId": "AROAIIZKPBKS2LEXAMPLE",
        "CreateDate": "2013-12-12T23:46:37.247Z",
        "RoleName": "s3access",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/s3access"
    }
}
```

3. Creare una policy di accesso e salvarla in un file di testo denominato `ec2-role-access-policy.json`. Ad esempio, questa policy concede autorizzazioni amministrative per Amazon S3 ad applicazioni eseguite nell'istanza.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:*"],
      "Resource": ["*"]
    }
  ]
}
```

4. Allega la politica di accesso al ruolo utilizzando il put-role-policycomando.

```
aws iam put-role-policy \
    --role-name s3access \
    --policy-name S3-Permissions \
    --policy-document file://ec2-role-access-policy.json
```

5. Crea un profilo di istanza denominato `s3access-profile` utilizzando il create-instance-profilecomando.

```
aws iam create-instance-profile --instance-profile-name s3access-profile
```

Example response

```
{
    "InstanceProfile": {
        "InstanceProfileId": "AIPAJTLBPJLEGREXAMPLE",
        "Roles": [],
        "CreateDate": "2013-12-12T23:53:34.093Z",
        "InstanceProfileName": "s3access-profile",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:instance-profile/s3access-profile"
    }
}
```

6. Aggiungi il ruolo `s3access` al profilo dell'istanza `s3access-profile`.

```
aws iam add-role-to-instance-profile \
    --instance-profile-name s3access-profile \
    --role-name s3access
```

In alternativa, è possibile utilizzare i seguenti AWS Tools for Windows PowerShell comandi:

- New-IAMRole
- Registrati - IAM RolePolicy
- Nuovo-IAM InstanceProfile

Avvio di un'istanza con un ruolo IAM

Dopo aver creato un ruolo IAM, puoi avviare un'istanza e associare tale ruolo all'istanza durante l'avvio.

> **Important**
>
> Dopo aver creato un ruolo IAM, potrebbero essere necessari alcuni secondi per la propagazione delle autorizzazioni. Se il primo tentativo di avviare un'istanza con un ruolo ha

esito negativo, attendi alcuni secondi prima di riprovare. Per ulteriori informazioni, consulta la sezione Risoluzione dei problemi dei ruoli IAM nella Guida per l'utente di IAM.

New console

Per avviare un'istanza con un ruolo IAM (console)

1. Segui la procedura per avviare un'istanza.
2. Espandi Advanced details (Dettagli avanzati) e per IAM instance profile (Profilo dell'istanza IAM) seleziona il ruolo IAM creato.

   > **Note**
   >
   > Nell'elenco IAM instance profile (Profilo dell'istanza IAM) viene visualizzato il nome del profilo dell'istanza creato contemporaneamente al ruolo IAM. Se hai creato il ruolo IAM utilizzando la console, il profilo dell'istanza creato automaticamente avrà lo stesso nome del ruolo. Se hai creato il tuo ruolo IAM utilizzando l' AWS CLI API o un AWS SDK, potresti aver denominato il profilo dell'istanza in modo diverso.

3. Configura tutti gli altri dettagli richiesti per la tua istanza o accetta i valori predefiniti e seleziona una coppia di chiavi. Per informazioni sui campi della procedura guidata di avvio istanza, consulta Avvio di un'istanza utilizzando parametri definiti.
4. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).
5. Se utilizzi le azioni dell'API Amazon EC2 nella tua applicazione, recupera le credenziali di AWS sicurezza rese disponibili sull'istanza e usale per firmare le richieste. L' AWS SDK lo fa per te.

   IMDSv2

   Per le istanze Linux, vedi l'esempio seguente:

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/iam/security-credentials/role_name
   ```

Per le istanze Windows, vedi l'esempio seguente:

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-
ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

IMDSv1

Per le istanze Linux, vedi l'esempio seguente:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

Per le istanze Windows, vedi l'esempio seguente:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/
security-credentials/role_name
```

Old console

Per avviare un'istanza con un ruolo IAM (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di controllo scegliere Avvia istanza.
3. Selezionare un'AMI e un tipo di istanza, quindi scegliere Next: Configure Instance Details (Successivo: configura dettagli dell'istanza).
4. Nella pagina Configure Instance Details (Configura dettagli dell'istanza), in IAM role (Ruolo IAM), selezionare il ruolo IAM creato.

> **Note**
>
> Nell'elenco IAM role (Ruolo IAM) viene visualizzato il nome del profilo dell'istanza creato quando è stato creato il ruolo IAM. Se hai creato il ruolo IAM utilizzando la console, il profilo dell'istanza creato automaticamente avrà lo stesso nome del ruolo.

Se hai creato il tuo ruolo IAM utilizzando l' AWS CLI API o un AWS SDK, potresti aver denominato il profilo dell'istanza in modo diverso.

5. Configurare qualsiasi altro dettaglio, quindi seguire le istruzioni visualizzate nella procedura guidata e scegliere Review and Launch (Analizza e avvia) per accettare le impostazioni di default e passare direttamente alla pagina Review Instance Launch (Rivedi l'avvio dell'istanza).
6. Rivedere le impostazioni, quindi scegliere Launch (Avvia) per scegliere la coppia di chiavi e avviare l'istanza.
7. Se utilizzi le azioni dell'API Amazon EC2 nella tua applicazione, recupera le credenziali di AWS sicurezza rese disponibili sull'istanza e usale per firmare le richieste. L' AWS SDK lo fa per te.

   IMDSv2

   Per le istanze Linux, vedi l'esempio seguente:

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/iam/security-credentials/role_name
   ```

   Per le istanze Windows, vedi l'esempio seguente:

   ```
   PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-
   ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
   ```

   ```
   PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
    -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
   credentials/role_name
   ```

   IMDSv1

   Per le istanze Linux, vedi l'esempio seguente:

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
   credentials/role_name
   ```

Per le istanze Windows, vedi l'esempio seguente:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/
security-credentials/role_name
```

Command line

È possibile utilizzare il AWS CLI per associare un ruolo a un'istanza durante l'avvio. Devi specificare il profilo dell'istanza nel comando.

Come avviare un'istanza con un ruolo IAM (AWS CLI)

1. Utilizzare il comando run-instances per avviare un'istanza utilizzando il profilo dell'istanza. L'esempio seguente illustra come avviare un'istanza con il profilo dell'istanza.

   ```
   aws ec2 run-instances \
       --image-id ami-11aa22bb \
       --iam-instance-profile Name="s3access-profile" \
       --key-name my-key-pair \
       --security-groups my-security-group \
       --subnet-id subnet-1a2b3c4d
   ```

   In alternativa, utilizzate il PowerShell comando New-EC2InstanceTools for Windows.

2. Se utilizzi le azioni dell'API Amazon EC2 nella tua applicazione, recupera le credenziali di AWS sicurezza rese disponibili sull'istanza e usale per firmare le richieste. L' AWS SDK lo fa per te.

   ```
   curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
   ```

Collegamento di un ruolo IAM all'istanza

Per collegare un ruolo IAM a un'istanza senza ruolo, l'istanza può essere nello stato `stopped` o `running`.

Console

Per collegare un ruolo IAM a un'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza e scegliere Actions (Operazioni), Security (Sicurezza), Modify IAM role (Modifica ruolo IAM).
4. Selezionare il ruolo IAM da collegare all'istanza e scegliere Save (Salva).

Command line

Come collegare un ruolo IAM a un'istanza (AWS CLI)

1. Se necessario, descrivere le istanze per ottenere l'ID dell'istanza a cui collegare il ruolo.

```
aws ec2 describe-instances
```

2. Utilizza il associate-iam-instance-profilecomando per associare il ruolo IAM all'istanza specificando il profilo dell'istanza. Puoi utilizzare il nome della risorsa Amazon (ARN) del profilo dell'istanza oppure il relativo nome.

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

Example response

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-1234567890abcdef0",
        "State": "associating",
        "AssociationId": "iip-assoc-0dbd8529a48294120",
        "IamInstanceProfile": {
            "Id": "AIPAJLNLDX3AMYZNWYYAY",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-1"
        }
    }
}
```

In alternativa, utilizzate i seguenti PowerShell comandi Tools for Windows:

- Get-EC2Instance
- Register-EC2IamInstanceProfile

Sostituire un ruolo IAM

Per sostituire il ruolo IAM su un'istanza che ha già un ruolo IAM collegato, l'istanza deve essere nello stato `running`. È possibile eseguire questa operazione se si desidera modificare il ruolo IAM per un'istanza senza scollegare prima quella esistente. Ad esempio, è possibile eseguire questa operazione per verificare che le operazioni API eseguite dalle applicazioni in esecuzione sull'istanza non siano interrotte.

Console

Per sostituire un ruolo IAM per un'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza e scegliere Actions (Operazioni), Security (Sicurezza), Modify IAM role (Modifica ruolo IAM).
4. Selezionare il ruolo IAM da collegare all'istanza e scegliere Save (Salva).

Command line

Come sostituire un ruolo IAM per un'istanza (AWS CLI)

1. Se necessario, descrivere le associazioni del profilo dell'istanza IAM per recuperare l'ID associazione per il profilo dell'istanza IAM da sostituire.

```
aws ec2 describe-iam-instance-profile-associations
```

2. Utilizza il comando replace-iam-instance-profile-association per sostituire il profilo dell'istanza IAM specificando l'ID di associazione per il profilo di istanza esistente e l'ARN o il nome del profilo di istanza che dovrebbe sostituirlo.

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
```

```
    --iam-instance-profile Name="TestRole-2"
```

Example response

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "associating",
        "AssociationId": "iip-assoc-09654be48e33b91e0",
        "IamInstanceProfile": {
            "Id": "AIPAJCJEDKX7QYHWYK7GS",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

In alternativa, utilizza i seguenti comandi Tools for Windows: PowerShell

- Get-EC2IamInstanceProfileAssociation
- Set-EC2IamInstanceProfileAssociation

Scollegare un ruolo IAM

Puoi scollegare un ruolo IAM da un'istanza in esecuzione o arrestata.

Console

Per scollegare un ruolo IAM da un'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza e scegliere Actions (Operazioni), Security (Sicurezza), Modify IAM role (Modifica ruolo IAM).
4. Per IAM role (Ruolo IAM), scegliere No IAM Role (Nessun ruolo IAM). Seleziona Salva.
5. Nella finestra di dialogo di conferma, immettere Detach (Scollega), quindi scegliere Detach (Scollega).

Command line

Come scollegare un ruolo IAM da un'istanza (AWS CLI)

1. Se necessario, usa describe-iam-instance-profile-associations per descrivere le associazioni dei profili di istanza IAM e ottenere l'ID di associazione per il profilo dell'istanza IAM da scollegare.

```
aws ec2 describe-iam-instance-profile-associations
```

Example response

```
{
    "IamInstanceProfileAssociations": [
        {
            "InstanceId": "i-088ce778fbfeb4361",
            "State": "associated",
            "AssociationId": "iip-assoc-0044d817db6c0a4ba",
            "IamInstanceProfile": {
                "Id": "AIPAJEDNCAA64SSD265D6",
                "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
            }
        }
    ]
}
```

2. Utilizza il disassociate-iam-instance-profilecomando per scollegare il profilo dell'istanza IAM utilizzando il relativo ID di associazione.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

Example response

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "disassociating",
        "AssociationId": "iip-assoc-0044d817db6c0a4ba",
        "IamInstanceProfile": {
            "Id": "AIPAJEDNCAA64SSD265D6",
```

```
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

In alternativa, utilizza i seguenti PowerShell comandi Tools for Windows:

- Get-EC2IamInstanceProfileAssociation
- Unregister-EC2IamInstanceProfile

Generazione di una policy per il ruolo IAM in base all'attività di accesso

Quando si crea per la prima volta un ruolo IAM per le applicazioni, a volte è possibile concedere altre autorizzazioni oltre a quanto richiesto. Prima di avviare l'applicazione nell'ambiente di produzione, è possibile generare una policy IAM basata sull'attività di accesso per un ruolo IAM. IAM Access Analyzer esamina AWS CloudTrail i log e genera un modello di policy che contiene le autorizzazioni utilizzate dal ruolo nell'intervallo di date specificato. È possibile utilizzare il modello per creare una policy gestita con autorizzazioni granulari e quindi collegarla al ruolo IAM. In questo modo, concedi solo le autorizzazioni necessarie al ruolo per interagire con le AWS risorse per il tuo caso d'uso specifico. In questo modo è possibile rispettare la best practice per concedere il minimo privilegio. Per ulteriori informazioni, consulta Generazione di policy basate sull'attività di accesso nella Guida per l'utente di IAM.

Accesso ad Amazon EC2 utilizzando un endpoint VPC di interfaccia

Puoi migliorare la posizione di sicurezza del VPC creando una connessione privata tra il VPC e Amazon EC2. Puoi accedere ad Amazon EC2 come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze presenti nel VPC non richiedono indirizzi IP pubblici per accedere ad Amazon EC2.

Per ulteriori informazioni, consulta Access Servizi AWS through AWS PrivateLink nella Guida.AWS PrivateLink

Indice

Creazione di un endpoint VPC dell'interfaccia

Crea un endpoint di interfaccia per Amazon EC2 utilizzando uno dei seguenti nomi di servizi:

- com.amazonaws.***region***.ec2: crea un endpoint per le operazioni dell'API Amazon EC2.

Per ulteriori informazioni, consulta Accedere a un endpoint VPC Servizio AWS con interfaccia nella Guida.AWS PrivateLink

Creazione di una policy di endpoint

Una policy di endpoint è una risorsa IAM che è possibile allegare all'endpoint di interfaccia. La policy di endpoint di default permette l'accesso completo all'API Amazon EC2 tramite l'endpoint di interfaccia. Per controllare l'accesso consentito all'API Amazon EC2 dal VPC, allegare una policy di endpoint personalizzata all'endpoint di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire operazioni.
- Le operazioni che possono essere eseguite.
- La risorsa su cui è possibile eseguire le operazioni.

> **Important**
>
> Quando viene applicata una policy non predefinita a un endpoint VPC di interfaccia per Amazon EC2, alcune richieste API non riuscite, ad esempio quelle `RequestLimitExceeded` provenienti da, potrebbero non essere registrate su Amazon o Amazon. AWS CloudTrail CloudWatch

Per ulteriori informazioni, consulta la sezione Controllo dell'accesso ai servizi con policy di endpoint nella Guida di AWS PrivateLink .

Nell'esempio seguente viene illustrata una policy endpoint VPC che nega l'autorizzazione per creare volumi non crittografati o per lanciare istanze con volumi non crittografati. Inoltre, la policy di esempio concede a chiunque l'autorizzazione per eseguire tutte le altre operazioni Amazon EC2.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
}
```

Gestione degli aggiornamenti per le istanze Windows di Amazon EC2

Ti consigliamo di applicare patch, aggiornare e proteggere regolarmente il sistema operativo e le applicazioni sulle istanze EC2. Puoi utilizzare Gestione patch di AWS Systems Manager per

automatizzare il processo di installazione degli aggiornamenti correlati alla sicurezza per il sistema operativo e le applicazioni.

Per le istanze EC2 in un gruppo con scalabilità automatica, puoi utilizzare il runbook AWS-PatchAsgInstance per evitare che le istanze sottoposte a patch vengano sostituite. In alternativa, puoi utilizzare qualsiasi servizio di aggiornamento automatico o processi consigliati per installare gli aggiornamenti che sono forniti dal fornitore dell'applicazione.

Risorse

- AL2023 — Aggiornamento di AL2023 nella Guida per l'utente di Amazon Linux 2023.
- AL2: gestisci il software sulla tua istanza Amazon Linux 2 nella Guida per l'utente di Amazon Linux 2.
- Istanze Windows —. the section called “Gestione degli aggiornamenti”

Procedure consigliate di sicurezza per le istanze Windows

Ti consigliamo di seguire queste best practice di sicurezza per le tue istanze di Windows.

Indice

Best practice di sicurezza di alto livello

È necessario attenersi alle seguenti best practice di sicurezza di alto livello per le istanze di Windows:

- Accesso minimo: concedi l'accesso solo a sistemi e posizioni attendibili e attesi. Questo vale per tutti i prodotti Microsoft, ad esempio Active Directory, server di produttività aziendale Microsoft e servizi infrastrutturali quali Servizi di desktop remoto, server proxy inverso, server Web IIS e altri. Utilizza AWS funzionalità come i gruppi di sicurezza delle istanze Amazon EC2, le liste di controllo degli accessi alla rete (ACL) e le sottoreti pubbliche/private di Amazon VPC per stratificare la sicurezza in più posizioni in un'architettura. All'interno di un'istanza Windows, i clienti

possono utilizzare Windows Firewall per ampliare ulteriormente la strategia all'interno della loro distribuzione. defense-in-depth Installare solo i componenti e le applicazioni del sistema operativo necessari per il funzionamento del sistema come progettato. Configurare i servizi infrastrutturali, ad esempio IIS, per l'esecuzione con account di servizio o per l'utilizzo di funzionalità quali le identità del pool di applicazioni per accedere alle risorse localmente e in remoto all'intera infrastruttura.

- Privilegi minimi: determina il set minimo di privilegi necessari alle istanze e agli account per svolgere le proprie funzioni. Limita tali server e utenti in modo da consentire solo queste autorizzazioni definite. Utilizza tecniche quali i controlli di accesso basati sui ruoli per ridurre l'area di superficie degli account amministrativi e creare i ruoli più limitati per eseguire un'attività. Utilizza le funzionalità del sistema operativo, ad esempio Encrypting File System (EFS) all'interno di NTFS per crittografare i dati sensibili inattivi e controllare l'accesso dell'applicazione e dell'utente ad esso.
- Gestione della configurazione: crea una configurazione server di base che incorpori patch di up-to-date sicurezza e suite di protezione basate su host che includono antivirus, antimalware, rilevamento/prevenzione delle intrusioni e monitoraggio dell'integrità dei file. Valuta ogni server rispetto alla linea di base registrata corrente per identificare e contrassegnare eventuali deviazioni. Assicura che ogni server sia configurato per generare e archiviare in modo sicuro i dati di log e di controllo appropriati.
- Gestione delle modifiche: crea processi per controllare le modifiche alle linee di base di configurazione del server e adotta processi di modifica completamente automatizzati. Inoltre, sfrutta Just Enough Administration (JEA) con Windows PowerShell DSC per limitare l'accesso amministrativo alle funzioni minime richieste.
- Gestione delle patch: implementa processi che applichino, aggiornino e proteggano regolarmente il sistema operativo e le applicazioni sulle istanze EC2.
- Registri di controllo: verifica l'accesso e tutte le modifiche alle istanze Amazon EC2 per verificare l'integrità del server e garantire che vengano apportate solo modifiche autorizzate. Sfrutta funzionalità come Enhanced Logging for IIS per migliorare le funzionalità di registrazione predefinite. AWS funzionalità come VPC Flow Logs e AWS CloudTrail sono disponibili anche per controllare l'accesso alla rete, incluse rispettivamente le richieste consentite/negate e le chiamate API.

Gestione degli aggiornamenti

Per garantire i migliori risultati quando esegui Windows Server su Amazon EC2, ti consigliamo di implementare le seguenti best practice:

- Configure Windows Update

- Update drivers
- Use the latest Windows AMIs
- Test performance before migration
- Update launch agents
- Riavvia l'istanza di Windows dopo aver installato gli aggiornamenti. Per ulteriori informazioni, consulta Riavvio dell'istanza.

Per informazioni su come aggiornare o migrare un'istanza Windows a una nuova versione di Windows Server, consultare Aggiornamento di un'istanza Amazon EC2 Windows a una versione più recente di Windows Server.

Configura Windows Update

Per impostazione predefinita, le istanze avviate dalle AMI di AWS Windows Server non ricevono aggiornamenti tramite Windows Update.

Aggiornamento dei driver Windows

Mantieni aggiornati i driver su tutte le istanze di Windows EC2 per accertarti che le correzioni più recenti e i miglioramenti di prestazioni siano applicati a tutta la tua serie di istanze. A seconda del tipo di istanza, è necessario aggiornare i driver AWS PV, Amazon ENA e AWS NVMe.

- Utilizza gli argomenti su SNS per ottenere gli aggiornamenti per le ultime versioni dei driver.
- Usa l' AWS Systems Manager Automation runbook AWSSupport per applicare facilmente gli aggiornamenti UpgradeWindows AWSDrivers a tutte le tue istanze.

Avvia le istanze utilizzando le AMI Windows più recenti

AWS rilascia nuove AMI Windows ogni mese, che contengono le patch, i driver e gli agenti di avvio più recenti del sistema operativo. Quando avvii nuove istanze o quando crei immagini personalizzate, devi utilizzare le AMI più recenti.

- Per visualizzare gli aggiornamenti di ogni versione delle AMI AWS Windows, consulta Cronologia delle versioni di AWS Windows AMI.
- Per compilare con le AMI più recenti disponibili, consulta Query per l'AMI Windows più recente tramite Systems Manager Parameter Store.

- Per ulteriori informazioni sulle AMI Windows specializzate che è possibile utilizzare per avviare istanze per il database e sui casi d'uso relativi al rafforzamento della conformità, vedere AMI Windows specializzate nel Windows AMI Reference.AWS

Test delle prestazioni del sistema/delle applicazioni prima di eseguire la migrazione

La migrazione delle applicazioni aziendali a AWS può comportare molte variabili e configurazioni. È opportuno testare sempre le prestazioni della soluzione EC2 per assicurarsi di quanto segue:

- I tipi di istanza sono configurati correttamente, incluse la dimensione dell'istanza, le reti migliorate e la tenancy (condivisa o dedicata).
- La topologia dell'istanza è idonea per il carico di lavoro e, laddove necessario, impiega caratteristiche ad alte prestazioni (tenancy dedicata, gruppi di collocamento, volumi archivio dell'istanza, bare metal).

Aggiornamento degli agenti di avvio

Esegui l'aggiornamento all'agente EC2Launch v2 più recente per assicurarti che le ultime correzioni vengano applicate a tutto il parco istanze. Per ulteriori informazioni, consulta the section called “Migrazione”.

Se si utilizza un parco istanze misto o si desidera continuare a utilizzare gli agenti EC2Launch (Windows Server 2016 e 2019) o EC2 Config (solo sistemi operativi legacy), eseguire l'aggiornamento alle versioni più recenti dei rispettivi agenti.

Gli aggiornamenti automatici sono supportati nelle seguenti combinazioni di versioni di Windows Server e agenti di avvio. Puoi attivare gli aggiornamenti automatici nella console SSM Quick Setup Host Management in Agenti di avvio Amazon EC2.

Versione Windows	EC2Launch v1	EC2Launch v2
2016	✓	✓
2019	✓	✓
2022		✓

- Per ulteriori informazioni sull'aggiornamento a EC2Launch v2, consulta. the section called “Installa”

- Per informazioni sull'aggiornamento manuale di EC2Config, consulta. the section called “Installazione di EC2Config”
- Per informazioni sull'aggiornamento manuale di EC2Launch, consulta. the section called “Installazione di EC2Launch”

Gestione della configurazione

Amazon Machine Images (AMI) fornisce una configurazione iniziale per un'istanza Amazon EC2, che include il sistema operativo Windows e personalizzazioni facoltative specifiche del cliente, come applicazioni e controlli di sicurezza. Crea un catalogo AMI contenente linee di base di configurazione di sicurezza personalizzate per garantire che tutte le istanze di Windows vengano avviate con controlli di sicurezza standard. Le linee di base di sicurezza possono essere inserite in un'AMI, avviate dinamicamente all'avvio di un'istanza EC2 o impacchettate come prodotto per una distribuzione uniforme attraverso i portafogli di Service Catalog. AWS Per ulteriori informazioni sulla protezione di un'AMI, consulta Best Practices for Building an AMI.

Ogni istanza Amazon EC2 deve rispettare gli standard di sicurezza organizzativa. Non installare ruoli e funzionalità di Windows che non sono necessari e installa software per la protezione da codice dannoso (antivirus, antimalware, attenuazione degli exploit), monitora l'integrità dell'host ed esegui il rilevamento delle intrusioni. Configura il software di sicurezza per monitorare e mantenere le impostazioni di sicurezza del sistema operativo, proteggere l'integrità dei file operativi critici e avvisare eventuali deviazioni dalla linea di base di sicurezza. Considera di implementare i benchmark della configurazione di sicurezza pubblicati da Microsoft, dal Center for Internet Security (CIS) o dal National Institute of Standards and Technology (NIST). Prendi in considerazione l'utilizzo di altri strumenti Microsoft per server di applicazioni particolari, ad esempio il Best Practice Analyzer per SQL Server.

AWS i clienti possono anche eseguire valutazioni Amazon Inspector per migliorare la sicurezza e la conformità delle applicazioni distribuite su istanze Amazon EC2. Amazon Inspector valuta automaticamente le applicazioni per individuare vulnerabilità o deviazioni dalle procedure consigliate e include una base di conoscenze di centinaia di regole mappate a standard di conformità di sicurezza comuni (ad esempio, PCI DSS) e definizioni di vulnerabilità. Esempi di regole incorporate includono la verifica se l'accesso remoto root è abilitato o se sono installate versioni software vulnerabili. Queste regole vengono aggiornate regolarmente dai ricercatori di sicurezza. AWS

Quando si proteggono le istanze di Windows, si consiglia di implementare Servizi di dominio Active Directory per abilitare un'infrastruttura scalabile, sicura e gestibile per i percorsi distribuiti. Inoltre,

dopo aver avviato le istanze dalla console Amazon EC2 o utilizzando uno strumento di provisioning Amazon EC2, ad esempio, è buona norma utilizzare le funzionalità native del sistema operativo, AWS CloudFormation come Microsoft PowerShell Windows DSC, per mantenere lo stato della configurazione nel caso in cui si verifichi una variazione della configurazione.

Gestione delle modifiche

Dopo aver applicato le basi di sicurezza iniziali alle istanze Amazon EC2 all'avvio, controlla le modifiche in corso su Amazon EC2 per mantenere la sicurezza delle macchine virtuali. Stabilisci un processo di gestione delle modifiche per autorizzare e incorporare le modifiche alle AWS risorse (come gruppi di sicurezza, tabelle di routing e ACL di rete) nonché alle configurazioni del sistema operativo e delle applicazioni (come Windows o patch delle applicazioni, aggiornamenti software o aggiornamenti dei file di configurazione).

AWS fornisce diversi strumenti per aiutare a gestire le modifiche alle AWS risorse, tra cui AWS CloudTrail, AWS Config AWS CloudFormation AWS Elastic Beanstalk AWS OpsWorks, e pacchetti di gestione per Systems Center Operations Manager e System Center Virtual Machine Manager. Tieni presente che Microsoft rilascia le patch di Windows il secondo martedì di ogni mese (o secondo necessità) e AWS aggiorna tutte le AMI Windows gestite da AWS entro cinque giorni dal rilascio di una patch da parte di Microsoft. Pertanto è importante applicare continuamente patch a tutte le AMI di base, aggiornare i AWS CloudFormation modelli e le configurazioni dei gruppi Auto Scaling con gli ID AMI più recenti e implementare strumenti per automatizzare la gestione delle patch delle istanze in esecuzione.

Microsoft fornisce diverse opzioni per la gestione delle modifiche al sistema operativo Windows e alle applicazioni. SCCM, ad esempio, fornisce una copertura completa del ciclo di vita delle modifiche dell'ambiente. Seleziona gli strumenti che rispondono ai requisiti aziendali e controlla in che modo le modifiche influenzeranno i contratti di servizio delle applicazioni, la capacità, la sicurezza e le procedure di ripristino di emergenza. Evita le modifiche manuali e sfrutta invece software di gestione automatizzata della configurazione o strumenti a riga di comando come EC2 Run Command o Windows PowerShell per implementare processi di modifica ripetibili e basati su script. Per rispondere a questo requisito, utilizza bastion host con logging avanzato per tutte le interazioni con le istanze di Windows per garantire che tutti gli eventi e le attività vengano registrati automaticamente.

Controllo e responsabilità per le istanze Windows di Amazon EC2

AWS CloudTrail e Regole di AWS Config forniscono funzionalità di controllo e tracciamento delle modifiche per controllare le modifiche alle risorse. AWS Config AWS Configura i log di eventi di

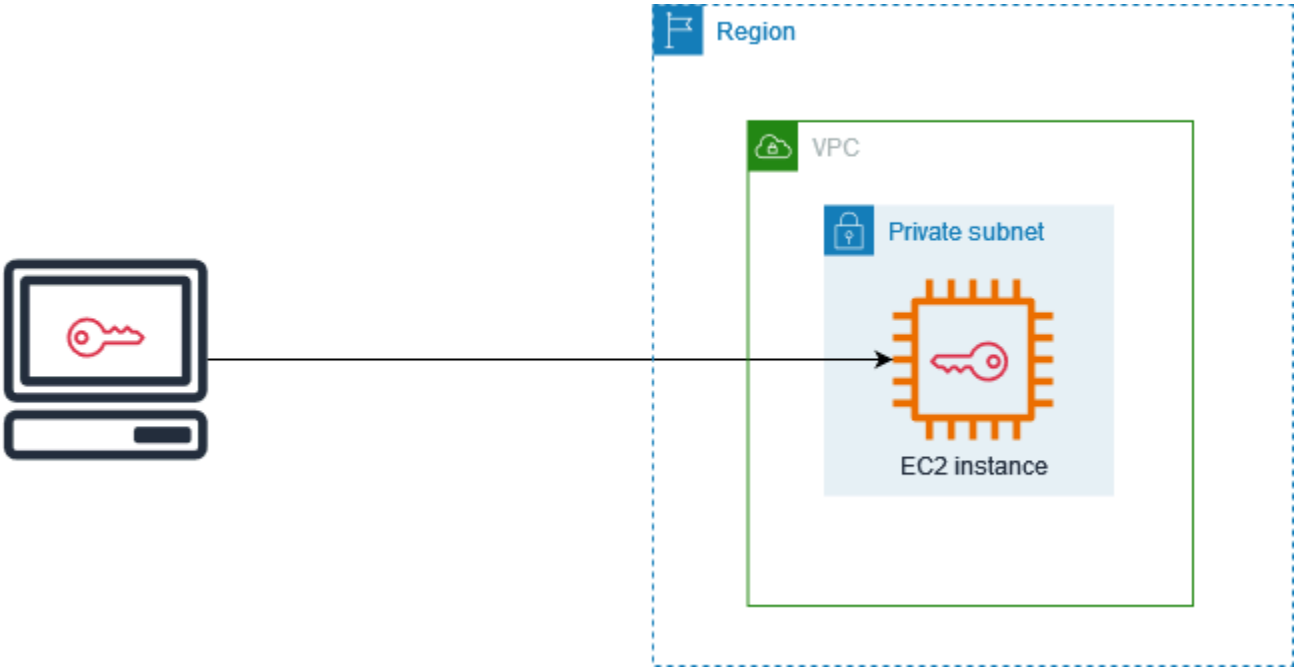
Windows per inviare file di log locali a un sistema centralizzato di gestione dei log per conservare i dati di log per l'analisi del comportamento operativo e di sicurezza. Microsoft System Center Operations Manager (SCOM) aggrega informazioni sulle applicazioni Microsoft distribuite nelle istanze Windows e applica set di regole preconfigurati e personalizzati in base ai ruoli e ai servizi dell'applicazione. I System Center Management Pack si basano su SCOM per fornire indicazioni sulla configurazione e monitoraggio specifiche delle applicazioni. Questi Management Pack supportano Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014 e molti altri server e tecnologie.

Oltre agli strumenti di gestione dei sistemi Microsoft, i clienti possono utilizzare Amazon CloudWatch per monitorare l'utilizzo della CPU dell'istanza, le prestazioni del disco, l'I/O di rete ed eseguire controlli dello stato di host e istanze. Gli agenti di lancio EC2Config, EC2Launch ed EC2Launch v2 forniscono l'accesso a funzionalità aggiuntive e avanzate per le istanze Windows. Ad esempio, possono esportare i log di sistema, sicurezza, applicazioni e Internet Information Services (IIS) di Windows in CloudWatch log che possono quindi essere integrati con i CloudWatch parametri e gli allarmi di Amazon. I clienti possono anche creare script che esportano i contatori delle prestazioni di Windows in metriche CloudWatch personalizzate di Amazon.

Coppie di chiavi Amazon EC2 e istanze Amazon EC2

Una coppia di chiavi, costituita da una chiave privata e una chiave pubblica, è un insieme di credenziali di sicurezza utilizzate per dimostrare l'identità durante la connessione a un'istanza Amazon EC2. Per le istanze Linux, la chiave privata consente di accedere in modo sicuro tramite SSH all'istanza. Per le istanze Windows, è necessaria la chiave privata per decrittografare la password dell'amministratore, che viene quindi utilizzata per connettersi all'istanza.

Amazon EC2 memorizza la chiave pubblica sulla tua istanza e tu memorizzi la chiave privata, come mostrato nel diagramma seguente. È importante archiviare la chiave privata in un luogo sicuro perché chiunque possieda la chiave privata può connettersi alle istanze che utilizzano la coppia di chiavi.



Quando avvii un'istanza, puoi specificare una coppia di chiavi, in modo da poterti connettere all'istanza utilizzando un metodo che richiede una coppia di chiavi. A seconda di come gestisci la sicurezza, puoi specificare la stessa coppia di chiavi per tutte le istanze oppure puoi specificare coppie di chiavi diverse.

Per le istanze Linux, quando l'istanza si avvia per la prima volta, la chiave pubblica specificata all'avvio viene inserita nell'istanza Linux in una voce all'interno`~/.ssh/authorized_keys`. Quando ti connetti all'istanza Linux usando SSH, per accedere devi specificare la chiave privata che corrisponde alla chiave pubblica.

Per ulteriori informazioni sulla connessione alla tua istanza EC2, consulta. Connect alla tua istanza EC2

> **Important**
>
> Poiché Amazon EC2 non conserva una copia della chiave privata, se si perde una chiave privata non è possibile recuperarla. Tuttavia, può ancora esserci un modo per connettersi a istanze per cui hai perso la chiave privata. Per ulteriori informazioni, consulta Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Linux?.

In alternativa alle coppie di chiavi, puoi utilizzarle AWS Systems Manager Session Managerper connetterti alla tua istanza con una shell interattiva basata su browser con un solo clic o il (). AWS Command Line Interface AWS CLI

Indice

Crea una coppia di key pair per la tua istanza Amazon EC2

Puoi usare Amazon EC2 per creare le tue coppie di chiavi oppure puoi utilizzare uno strumento di terze parti per creare le tue coppie di chiavi e poi importarle in Amazon EC2.

Amazon EC2 supporta chiavi RSA SSH-2 a 2048 bit per istanze Linux e Windows. Amazon EC2 supporta anche le chiavi ED25519 per le istanze Linux.

Per i passaggi per connettersi alla propria istanza Linux utilizzando SSH dopo aver creato una key pair, vederethe section called “Connessione all'istanza di Linux”.

Per la procedura di connessione all'istanza di Windows tramite RDP dopo aver creato una key pair, consultathe section called “Connettiti all'istanza Windows ”.

Indice

Creazione di una coppia di chiavi utilizzando Amazon EC2

Quando crei una coppia di chiavi utilizzando Amazon EC2, la chiave pubblica viene archiviata in Amazon EC2 e tu archivi la chiave privata.

Puoi creare fino a 5.000 coppie di chiavi per regione. Per richiedere un aumento, crea una richiesta di supporto. Per ulteriori informazioni, consulta Creazione di una richiesta di assistenza nella Guida per l'utente di AWS Support .

Console

Come creare una coppia di chiavi utilizzando Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, sotto Network & Security (Rete e sicurezza), scegliere Key Pairs (Coppie di chiavi).
3. Scegliere Create key pair (Crea coppia di chiavi).
4. Per Name (Nome), immettere un nome descrittivo per la coppia di chiavi. Amazon EC2 associa la chiave pubblica con il nome specificato come nome della chiave. Il nome può includere fino a 255 caratteri ASCII. Non può includere spazi iniziali o finali.
5. Seleziona un tipo di key pair appropriato per il tuo sistema operativo:

   (istanze Linux) Per il tipo di coppia di chiavi, scegli RSA o ED25519.

   (Istanze Windows) Per il tipo di coppia di chiavi, scegli RSA. Le chiavi ED25519 non sono supportate per le istanze Windows.
6. Per Private key file format (Formato file chiave privata), scegliere il formato in cui salvare la chiave privata. Per salvare la chiave privata in un formato che può essere utilizzato con OpenSSH, scegliere pem. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegliere ppk.
7. Per aggiungere un tag, scegli Add tag (Aggiungi tag) e immetti la chiave e il valore per il tag. Ripetere per ogni tag.
8. Scegliere Create key pair (Crea coppia di chiavi).
9. Il file della chiave privata viene automaticamente scaricato dal browser. Il nome del file di base è il nome specificato come nome della coppia di chiavi e l'estensione del nome del file è determinata dal formato di file scelto. Salvare il file della chiave privata in un luogo sicuro.

   > **Important**
   >
   > Questo è l'unico momento in cui salvare il file della chiave privata.

10. (Istanze Linux) Se prevedi di utilizzare un client SSH su un computer macOS o Linux per connetterti alla tua istanza Linux, usa il comando seguente per impostare le autorizzazioni del tuo file di chiave privata in modo che solo tu possa leggerlo.

```
chmod 400 key-pair-name.pem
```

Se non imposti queste autorizzazioni, allora non puoi connetterti alle tue istanze usando questa coppia di chiavi. Per ulteriori informazioni, consulta Errore: Unprotected Private Key File (File della chiave privata non protetto).

AWS CLI

Come creare una coppia di chiavi utilizzando Amazon EC2

1. Utilizza il comando create-key-pair come segue per generare la coppia di chiavi e salvare la chiave privata in un file `.pem`.

   Per `--key-name`, specifica un nome per la chiave pubblica. Il nome può essere composto da un massimo di 255 caratteri ASCII.

   Per `--key-type`, specifica `rsa` o `ed25519`. Se non includi i parametri `--key-type`, una chiave `rsa` viene creata per impostazione predefinita. Le chiavi ED25519 non sono supportate per le istanze Windows.

   Per `--key-format`, specifica `pem` o `ppk`. Se non viene incluso il parametro `--key-format`, per impostazione di default viene creato un file `pem`.

   `--query "KeyMaterial"` stampa il materiale della chiave privata nell'output.

   `--output text > my-key-pair.pem` salva il materiale della chiave privata in un file con estensione specificata. L'estensione può essere `.pem` o `.ppk`. La chiave privata può avere un nome diverso dalla chiave pubblica ma, per facilità d'uso, utilizzare lo stesso nome.

```
aws ec2 create-key-pair \
    --key-name my-key-pair \
    --key-type rsa \
    --key-format pem \
    --query "KeyMaterial" \
    --output text > my-key-pair.pem
```

2. (Istanze Linux) Se prevedi di utilizzare un client SSH su un computer macOS o Linux per connetterti alla tua istanza Linux, usa il comando seguente per impostare le autorizzazioni del tuo file di chiave privata in modo che solo tu possa leggerlo.

```
chmod 400 key-pair-name.pem
```

Se non imposti queste autorizzazioni, allora non puoi connetterti alle tue istanze usando questa coppia di chiavi. Per ulteriori informazioni, consulta Errore: Unprotected Private Key File (File della chiave privata non protetto).

PowerShell

Come creare una coppia di chiavi utilizzando Amazon EC2

Utilizzate il New-EC2KeyPair AWS Tools for Windows PowerShell comando seguente per generare la chiave e salvarla in un file or. `.pem` `.ppk`

Per `-KeyName`, specifica un nome per la chiave pubblica. Il nome può essere composto da un massimo di 255 caratteri ASCII.

Per `-KeyType`, specifica `rsa` o `ed25519`. Se non includi i parametri `-KeyType`, una chiave `rsa` viene creata per impostazione predefinita. Le chiavi ED25519 non sono supportate per le istanze Windows.

Per `-KeyFormat`, specifica `pem` o `ppk`. Se non viene incluso il parametro `-KeyFormat`, per impostazione di default viene creato un file `pem`.

`KeyMaterial` stampa il materiale della chiave privata nell'output.

`Out-File -Encoding ascii -FilePath` *`C:\path\my-key-pair`*`.pem` salva il materiale della chiave privata in un file con estensione specificata. L'estensione può essere `.pem` o `.ppk`. La chiave privata può avere un nome diverso dalla chiave pubblica ma, per facilità d'uso, utilizzare lo stesso nome.

```
PS C:\> (New-EC2KeyPair -KeyName "my-key-pair" -KeyType "rsa" -KeyFormat
 "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Crea una key pair usando AWS CloudFormation

Quando si crea una nuova coppia di chiavi utilizzando AWS CloudFormation, la chiave privata viene salvata in AWS Systems Manager Parameter Store. Il nome del parametro ha il formato seguente:

```
/ec2/keypair/key_pair_id
```

Per ulteriori informazioni, consulta Archivio dei parametri AWS Systems Manager nella Guida per l'utente di AWS Systems Manager .

Per creare una key pair usando AWS CloudFormation

1. Specificate la AWS::EC2::KeyPairrisorsa nel modello.

   ```
   Resources:
     NewKeyPair:
       Type: 'AWS::EC2::KeyPair'
       Properties:
         KeyName: new-key-pair
   ```

2. Utilizza il comando describe-key-pairs come segue per ottenere l'ID della coppia di chiavi.

   ```
   aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
    KeyPairs[*].KeyPairId --output text
   ```

   Di seguito è riportato un output di esempio.

   ```
   key-05abb699beEXAMPLE
   ```

3. Utilizza il comando get-parameter come segue per ottenere il parametro per la tua chiave e salvare il materiale della chiave in un file `.pem`.

   ```
   aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
    --query Parameter.Value --output text > new-key-pair.pem
   ```

Autorizzazioni IAM richieste

AWS CloudFormation Per consentire la gestione dei parametri di Parameter Store per tuo conto, il ruolo IAM assunto dal AWS CloudFormation o dal tuo utente deve disporre delle seguenti autorizzazioni:

- `ssm:PutParameter`: concede l'autorizzazione per creare un parametro per il materiale della chiave privata.
- `ssm:DeleteParameter`: concede l'autorizzazione a eliminare il parametro che ha archiviato il materiale della chiave privata. Questa autorizzazione è necessaria indipendentemente dal fatto che la coppia di chiavi sia stata importata o creata da AWS CloudFormation.

Quando si AWS CloudFormation elimina una coppia di chiavi creata o importata da uno stack, esegue un controllo delle autorizzazioni per determinare se si dispone dell'autorizzazione per eliminare i parametri, anche se AWS CloudFormation crea un parametro solo quando crea una coppia di chiavi, non quando importa una coppia di chiavi. AWS CloudFormation verifica l'autorizzazione richiesta utilizzando un nome di parametro fabbricato che non corrisponde a nessun parametro del tuo account. Pertanto, è possibile che nel messaggio di errore `AccessDeniedException` venga visualizzato un nome di parametro fittizio.

Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2

Istanze Linux

Invece di creare la coppia di chiavi tramite Amazon EC2, è possibile creare una coppia di chiavi RSA o ED25519 utilizzando una strumento di terze parti e importare la chiave pubblica in Amazon EC2.

Requisiti delle coppie di chiavi

- Tipi supportati: RSA ed ED25519. Amazon EC2 non accetta chiavi DSA.
- Formati supportati:
  - Formato della chiave pubblica OpenSSH (il formato in). `~/.ssh/authorized_keys` Se effettui la connessione mediante SSH mentre stai utilizzando l'API EC2 Instance Connect, è supportato anche il formato SSH.
  - Il formato del file della chiave privata SSH deve essere PEM o PPK
  - (Solo RSA) Il formato DER con codifica Base64
  - (Solo RSA) Il formato file della chiave pubblica SSH come specificato in RFC4716
- Le lunghezze supportate sono 1024, 2048 e 4096. Se effettui la connessione mediante SSH mentre stai utilizzando l'API EC2 Instance Connect, le lunghezze supportate sono 2048 e 4096.

Per creare una coppia di chiavi tramite uno strumento di terza parte

1. Generare una coppia di chiavi con lo strumento di terza parte preferito. Ad esempio, per creare una coppia di chiavi è possibile utilizzare ssh-keygen (uno strumento fornito con l'installazione standard di OpenSSH). In alternativa, Java, Ruby, Python e molti altri linguaggi di programmazione forniscono librerie standard utilizzabili per creare una coppia di chiavi RSA o ED25519.

   > **Important**
   >
   > La chiave privata deve essere nel formato PEM o PPK. Ad esempio, utilizzare `ssh-keygen -m PEM` per generare la chiave OpenSSH nel formato PEM.

2. Salvare la chiave pubblica in un file locale. Ad esempio, `~/.ssh/my-key-pair.pub`. L'estensione del nome del file non è importante.
3. Salvare la chiave privata in un file locale con estensione `.pem` o `.ppk`. Ad esempio `~/.ssh/my-key-pair.pem` o `~/.ssh/my-key-pair.ppk`.

   > **Important**
   >
   > Salvare il file della chiave privata in un luogo sicuro. Dovrai fornire il nome della chiave pubblica quando avvii un'istanza e la chiave privata corrispondente ogni volta che ti connetti all'istanza.

Istanze Windows

Invece di creare la coppia di chiavi tramite Amazon EC2, puoi creare una coppia di chiavi RSA utilizzando un tool di terze parti e importare la chiave pubblica in Amazon EC2.

Requisiti delle coppie di chiavi

- Tipi supportati: RSA. Amazon EC2 non accetta chiavi DSA.

  > **Note**
  >
  > Le chiavi ED25519 non sono supportate per le istanze Windows.

- Formati supportati:

- Formato a chiave pubblica OpenSSH
- Il formato del file della chiave privata SSH deve essere PEM o PPK
- (Solo RSA) Il formato DER con codifica Base64
- (Solo RSA) Il formato file della chiave pubblica SSH come specificato in RFC4716

- Le lunghezze supportate sono 1024, 2048 e 4096.

Per creare una coppia di chiavi tramite uno strumento di terza parte

1. Generare una coppia di chiavi con lo strumento di terza parte preferito. Ad esempio, per creare una coppia di chiavi è possibile utilizzare ssh-keygen (uno strumento fornito con l'installazione standard di OpenSSH). In alternativa, Java, Ruby, Python e molti altri linguaggi di programmazione forniscono librerie standard che è possibile utilizzare per creare una coppia di chiavi RSA.

   > **Important**
   >
   > La chiave privata deve essere nel formato PEM o PPK. Ad esempio, utilizzare `ssh-keygen -m PEM` per generare la chiave OpenSSH nel formato PEM.

2. Salvare la chiave pubblica in un file locale. Ad esempio, `C:\keys\my-key-pair.pub`. L'estensione del nome del file non è importante.
3. Salvare la chiave privata in un file locale con estensione `.pem` o `.ppk`. Ad esempio `C:\keys\my-key-pair.pem` o `C:\keys\my-key-pair.ppk`. L'estensione del nome di file di questo file è importante perché solo `.pem` i file possono essere selezionati quando ci si connette all'istanza di Windows dalla console EC2.

   > **Important**
   >
   > Salvare il file della chiave privata in un luogo sicuro. Dovrai fornire il nome della chiave pubblica quando avvii un'istanza e la chiave privata corrispondente ogni volta che ti connetti all'istanza.

Dopo avere creato la coppia di chiavi, utilizzare uno dei seguenti metodi per importare la chiave pubblica in Amazon EC2.

Console

Come importare la chiave pubblica in Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Key Pairs (Coppie di chiavi).
3. Scegliere Import key pair (Importa coppia di chiavi).
4. Per Name (Nome), immettere un nome descrittivo per la chiave pubblica. Il nome può includere fino a 255 caratteri ASCII. Non può includere spazi iniziali o finali.

   > **Note**
   >
   > Quando ci si connette all'istanza dalla console EC2, la console suggerisce questo nome per il nome file della chiave privata.

5. Scegliere Browse (Sfoglia) per navigare e selezionare la chiave pubblica oppure incollare il contenuto della chiave pubblica nel campo Public key contents (Contenuto chiave pubblica).
6. Scegliere Import key pair (Importa coppia di chiavi).
7. Verificare che la chiave pubblica importata venga visualizzata nell'elenco delle coppie di chiavi.

AWS CLI

Come importare la chiave pubblica in Amazon EC2

Utilizza il comando import-key-pair AWS CLI .

Per verificare che la coppia di chiavi sia stata importata correttamente

Utilizza il comando describe-key-pairs AWS CLI .

PowerShell

Come importare la chiave pubblica in Amazon EC2

Utilizza il comando Import-EC2KeyPair AWS Tools for Windows PowerShell .

Per verificare che la coppia di chiavi sia stata importata correttamente

Utilizza il comando Get-EC2KeyPair AWS Tools for Windows PowerShell .

Assegnazione di tag a una coppia di chiavi

Per aiutarti a classificare e gestire le coppie di chiavi che hai creato utilizzando Amazon EC2 o importate in Amazon EC2, puoi etichettarle con metadati personalizzati. Per ulteriori informazioni sul funzionamento dei tag, consultare Tagging delle risorse Amazon EC2..

Console

Per visualizzare, aggiungere o eliminare un tag per una coppia di key pair

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Key Pairs (Coppie di chiavi).
3. Seleziona una chiave pubblica, quindi scegli Operazioni, Gestisci tag.
4. La pagina Gestisci tag visualizza tutti i tag assegnati alla chiave pubblica.
   - Per aggiungere un tag, scegliere Add tag (Aggiungi tag), quindi immettere la chiave e il valore del tag. Puoi aggiungere fino a 50 tag per chiave. Per ulteriori informazioni, consulta Limitazioni applicate ai tag.
   - Per eliminare un tag, scegliere Remove (Rimuovi) accanto al tag da eliminare.
5. Scegliere Save (Salva).

AWS CLI

Per visualizzare i tag delle tue coppie di chiavi

Utilizza il comando describe-tags AWS CLI . Nell'esempio seguente vengono descritti i tag per tutte le chiavi pubbliche.

```
aws ec2 describe-tags --filters "Name=resource-type,Values=key-pair"
```

```
{
    "Tags": [
    {
        "Key": "Environment",
        "ResourceId": "key-0123456789EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    },
```

```
    {
        "Key": "Environment",
        "ResourceId": "key-9876543210EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    }]
}
```

Per descrivere i tag di una key pair

Utilizza il comando describe-key-pairs AWS CLI .

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789EXAMPLE
```

```
{
    "KeyPairs": [
    {
        "KeyName": "MyKeyPair",
        "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "KeyPairId": "key-0123456789EXAMPLE",
        "Tags": [
        {
            "Key": "Environment",
            "Value": "Production"
        }]
    }]
}
```

Per etichettare una coppia di key pair

Utilizza il comando create-tags AWS CLI . Nell'esempio seguente, la chiave pubblica è contrassegnata con `Key=Cost-Center` e `Value=CC-123`.

```
aws ec2 create-tags --resources key-0123456789EXAMPLE --tags Key=Cost-
Center,Value=CC-123
```

Come eliminare un tag da una coppia di chiavi

Utilizza il comando delete-tags AWS CLI . Per degli esempi, consulta Esempi in Riferimento ai comandi AWS CLI .

PowerShell

Per visualizzare i tag delle tue coppie di chiavi

Utilizza il comando Get-EC2Tag.

Per descrivere i tag di una key pair

Utilizza il comando Get-EC2KeyPair.

Per etichettare una coppia di key pair

Utilizza il comando New-EC2Tag.

Come eliminare un tag da una coppia di chiavi

Utilizza il comando Remove-EC2Tag.

Descrivi le tue coppie di chiavi

Puoi descrivere le coppie di chiavi archiviate in Amazon EC2. È inoltre possibile recuperare il materiale della chiave pubblica e identificare la chiave pubblica specificata all'avvio.

Argomenti

Descrivi le tue coppie di chiavi

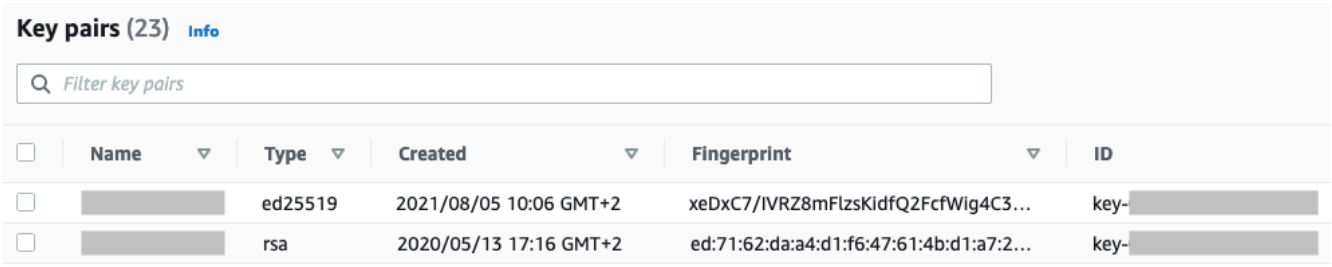
È possibile visualizzare le seguenti informazioni sulle chiavi pubbliche archiviate in Amazon EC2: nome della chiave pubblica, ID, tipo di chiave, impronta digitale, materiale chiave pubblica, data e ora (nel fuso orario UTC) in cui la chiave è stata creata da Amazon EC2 (se la chiave è stata creata da uno strumento di terze parti, la data e l'ora si riferiscono al momento in cui la chiave è stata importata in Amazon EC2) e tutti i tag associati alla chiave pubblica.

Puoi utilizzare la console Amazon EC2 o AWS CLI visualizzare informazioni sulle tue chiavi pubbliche.

Console

Come visualizzare le informazioni sulle chiavi pubbliche

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione sinistro, scegli Key Pairs (Coppie di chiavi).
3. È possibile visualizzare le informazioni su ciascuna chiave pubblica nella tabella Key pairs (Coppie di chiavi).



4. Per visualizzare i tag di una chiave pubblica, seleziona la casella di controllo accanto alla chiave e quindi scegli Actions (Operazioni), Manage tags (Gestisci tag).

AWS CLI

Come descrivere una chiave pubblica

Utilizza il comando describe-key-pairs e specifica il parametro `--key-names`.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

Output di esempio

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
```

```
}
```

In alternativa, invece di `--key-names`, è possibile specificare il parametro `--key-pair-ids` per identificare la chiave pubblica.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example
```

Per visualizzare il materiale della chiave pubblica nell'output, è necessario specificare il parametro `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Esempio di output: nell'output, il campo `PublicKey` contiene il materiale della chiave pubblica.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Recupero del materiale delle chiavi pubbliche

Si possono utilizzare vari metodi per accedere al materiale della chiave pubblica. Puoi recuperare il materiale relativo alla chiave pubblica dalla chiave privata corrispondente sul tuo computer locale, dai metadati dell'istanza sull'istanza che è stata avviata con la chiave pubblica o utilizzando il comando. `describe-key-pairs` AWS CLI Per le istanze Linux, il materiale della chiave pubblica può essere recuperato anche dal `authorized_keys` file sull'istanza.

Utilizza uno dei metodi descritti di seguito per recuperare il materiale della chiave pubblica.

Istanze Linux

From the private key

Come recuperare il materiale della chiave pubblica dalla chiave privata

Sul computer locale macOS, è possibile utilizzare il comando ssh-keygen per recuperare la chiave pubblica per la coppia di chiavi. Specificare il percorso in cui è stata scaricata la chiave privata (il file `.pem`).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

Il comando restituisce la chiave pubblica, come illustrato nell'esempio seguente.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Se il comando non riesce, assicurati di aver modificato le autorizzazioni sul file della coppia di chiavi private in modo che solo l'utente possa visualizzarlo:

```
chmod 400 key-pair-name.pem
```

From the instance metadata

È possibile utilizzare Instance Metadata Service Version 2 o Instance Metadata Service Version 1 per recuperare la chiave pubblica dai metadati dell'istanza.

> **Note**
>
> Se si modifica la coppia di chiavi utilizzata per connettersi all'istanza, Amazon EC2 non aggiorna i metadati dell'istanza per mostrare la nuova chiave pubblica. I metadati dell'istanza continuano a mostrare la chiave pubblica per la coppia di chiavi specificata al momento dell'avvio dell'istanza.

Come recuperare il materiale della chiave pubblica dai metadati dell'istanza

Usa uno dei comandi seguenti dalla tua istanza.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Output di esempio

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Per ulteriori informazioni sui metadati delle istanze, consulta Recupero dei metadati dell'istanza.

From the instance

Se si specifica una coppia di chiavi durante l'avvio di un'istanza Linux, quando l'istanza viene avviata per la prima volta, il contenuto della chiave pubblica viene inserito nell'istanza in una voce in `~/.ssh/authorized_keys`.

Come recuperare il materiale della chiave pubblica da un'istanza

1. Connettiti alla tua istanza.
2. Nella finestra del terminale, aprire il file `authorized_keys` utilizzando l'editor di testo preferito (ad esempio vim o nano).

   ```
   [ec2-user ~]$ nano ~/.ssh/authorized_keys
   ```

   Il file `authorized_keys` viene aperto, visualizzando la chiave pubblica seguita dal nome della coppia di chiavi. La seguente voce è un esempio di coppia di chiavi denominata *key-pair-name*.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

From describe-key-pairs

Come recuperare il materiale della chiave pubblica dal comando **`describe-key-pairs`** della AWS CLI

Utilizza il comando describe-key-pairs e specifica il parametro `--key-names` per identificare la chiave pubblica. Per includere il materiale della chiave pubblica nell'output, specificare il parametro `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Esempio di output: nell'output, il campo `PublicKey` contiene il materiale della chiave pubblica.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

In alternativa, invece di `--key-names`, è possibile specificare il parametro `--key-pair-ids` per identificare la chiave pubblic.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

Istanze Windows

From the private key

Come recuperare il materiale della chiave pubblica dalla chiave privata

Sul computer locale Windows, è possibile utilizzare PuTTYgen per ottenere la chiave pubblica per la coppia di chiavi.

Avvia PuTTYgen e scegli Load (Carica). Seleziona il file della chiave privata `.ppk` o `.pem`. PuTTYgen visualizza la chiave pubblica in Public key for pasting into OpenSSH authorized_keys file (Chiave pubblica da incollare nel file OpenSSH authorized_keys). È anche possibile visualizzare la chiave pubblica scegliendo Save public key (Salva chiave pubblica), specificando un nome del file, salvando il file e quindi aprendolo.

From the instance metadata

È possibile utilizzare Instance Metadata Service Version 2 o Instance Metadata Service Version 1 per recuperare la chiave pubblica dai metadati dell'istanza.

> **Note**
>
> Se si modifica la coppia di chiavi utilizzata per connettersi all'istanza, Amazon EC2 non aggiorna i metadati dell'istanza per mostrare la nuova chiave pubblica. I metadati dell'istanza continuano a mostrare la chiave pubblica per la coppia di chiavi specificata al momento dell'avvio dell'istanza.

Come recuperare il materiale della chiave pubblica dai metadati dell'istanza

Usa uno dei comandi seguenti dalla tua istanza.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri  http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Output di esempio

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Per ulteriori informazioni sui metadati delle istanze, consulta Recupero dei metadati dell'istanza.

From describe-key-pairs

Come recuperare il materiale della chiave pubblica dal comando **`describe-key-pairs`** della AWS CLI

Utilizza il comando describe-key-pairs e specifica il parametro `--key-names` per identificare la chiave pubblica. Per includere il materiale della chiave pubblica nell'output, specificare il parametro `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Esempio di output: nell'output, il campo `PublicKey` contiene il materiale della chiave pubblica.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
```

```
    ]
}
```

In alternativa, invece di `--key-names`, è possibile specificare il parametro `--key-pair-ids` per identificare la chiave pubblic.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

Identificazione della chiave pubblica specificata al momento dell'avvio

Se specifichi una chiave pubblica quando avvii un'istanza, il nome della chiave pubblica viene registrato dall'istanza.

Come identificare la chiave pubblica specificata all'avvio

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e seleziona l'istanza desiderata.
3. Nella scheda Dettagli, sotto Dettagli istanza, nel campo Coppia di chiavi assegnata all'avvio viene visualizzato il nome della chiave pubblica specificata all'avvio dell'istanza.

> **Note**
>
> Il valore del campo Coppia di chiavi assegnata all'avvio non cambia anche se si modifica la chiave pubblica sull'istanza o si aggiungono chiavi pubbliche.

Eliminazione della coppia di chiavi

Puoi eliminare una coppia di chiavi, che rimuove la chiave pubblica archiviata in Amazon EC2. L'eliminazione di una coppia di chiavi non elimina la chiave privata corrispondente.

Quando elimini una chiave pubblica utilizzando i metodi seguenti, elimini la chiave pubblica archiviata in Amazon EC2 solo quando la coppia di chiavi è stata creata o importata. L'eliminazione di una chiave pubblica non rimuove la chiave pubblica dalle istanze a cui è stata aggiunta, né quando è stata avviata l'istanza né successivamente. Inoltre, la chiave privata non viene eliminata dal computer locale. È possibile continuare a connettersi alle istanze avviate tramite una chiave pubblica che è stata eliminata da Amazon EC2, purché si disponga ancora del file della chiave privata (`.pem`).

> **Important**
>
> Se si sta utilizzando un gruppo Auto Scaling (ad esempio, in un ambiente Elastic Beanstalk), assicurarsi che la chiave pubblica che si sta cancellando non sia specificata in un modello di avvio o in una configurazione di avvio associati. Se Amazon EC2 Auto Scaling rileva un'istanza non integra, avvia un'istanza sostitutiva. Tuttavia, l'avvio dell'istanza non riesce se non è possibile trovare la chiave pubblica. Per ulteriori informazioni, consulta Modelli di avvio nella Guida per l'utente di Amazon EC2 Auto Scaling.

Console

Come eliminare la chiave pubblica su Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Key Pairs (Coppie di chiavi).
3. Seleziona la coppia di chiavi da eliminare e scegli Actions (Operazioni), Delete (Elimina).
4. Nel campo di conferma immettere `Delete` e quindi scegliere Delete (Elimina).

AWS CLI

Come eliminare la chiave pubblica su Amazon EC2

Utilizza il comando delete-key-pair AWS CLI .

PowerShell

Come eliminare la chiave pubblica su Amazon EC2

Utilizza il comando Remove-EC2KeyPair AWS Tools for Windows PowerShell .

Aggiungi o rimuovi una chiave pubblica sulla tua istanza Linux

Se si perde una chiave privata, si perde l'accesso a tutte le istanze che utilizzano la coppia di chiavi. Per ulteriori informazioni sulla connessione a un'istanza utilizzando una coppia di chiavi diversa da quella specificata all'avvio, vedi Ho perso la mia chiave privata.

Quando avvii un'istanza, puoi specificare una coppia di chiavi. Se si specifica una coppia di chiavi all'avvio, quando l'istanza viene avviata per la prima volta il materiale della chiave pubblica viene inserito nell'istanza Linux in una voce in `~/.ssh/authorized_keys`.

È possibile modificare la coppia di chiavi utilizzata per accedere all'account di sistema predefinito dell'istanza aggiungendo una nuova chiave pubblica nell'istanza o sostituendo la chiave pubblica (eliminando la chiave pubblica esistente e aggiungendone una nuova) nell'istanza. È inoltre possibile rimuovere tutte le chiavi pubbliche da un'istanza. Per aggiungere o sostituire una coppia di chiavi, è necessario essere in grado di connettersi all'istanza.

È possibile aggiungere o sostituire una key pair per i seguenti motivi:

- Se un utente dell'organizzazione richiede l'accesso all'utente di sistema utilizzando una coppia di chiavi separata, è possibile aggiungere tale coppia di chiavi all'istanza.
- Se si vuole impedire che qualcuno in possesso di una copia della chiave privata (file `.pem`) si colleghi alla propria istanza (ad esempio, se ha lasciato l'organizzazione), è possibile eliminare la chiave pubblica sull'istanza e sostituirla con una nuova.
- Se si crea un'AMI Linux da un'istanza, il materiale sulla chiave pubblica viene copiato dall'istanza all'AMI. Se si avvia un'istanza dall'AMI, la nuova istanza include la chiave pubblica dell'istanza originale. Per impedire a un utente che dispone della chiave privata di connettersi alla nuova istanza, è possibile rimuovere la chiave pubblica dall'istanza originale prima di creare l'AMI.

Utilizzare le seguenti procedure per modificare la coppia di key pair per l'utente predefinito, ad esempio`ec2-user`. Per informazioni sull'aggiunta di utenti all'istanza, consulta la documentazione relativa al sistema operativo dell'istanza.

Per aggiungere o sostituire una coppia di chiavi

1. Creare una nuova coppia di chiavi tramite la console Amazon EC2 o uno strumento di terze parti.
2. Recuperare la chiave pubblica da una nuova coppia di chiavi. Per ulteriori informazioni, consulta Recupero del materiale delle chiavi pubbliche.
3. Connettersi all'istanza tramite un file di chiave privata esistente.
4. Utilizzare l'editor di testo preferito, aprire il file `.ssh/authorized_keys` nell'istanza. Incollare le informazioni sulla chiave pubblica dalla nuova coppia di chiavi sotto le informazioni sulla chiave pubblica esistenti. Salva il file.
5. Disconnettersi dalla nuova istanza e verificare che sia possibile connettersi all'istanza tramite il nuovo file di chiave privata.

6. (Facoltativo) Se si sostituisce una coppia di chiavi esistente, connettersi all'istanza ed eliminare le informazioni sulla chiave pubblica per la coppia di chiavi originale dal file `.ssh/authorized_keys`.

> **Important**
>
> Se si sta utilizzando un gruppo Auto Scaling, assicurarsi che la coppia di chiavi che si sta sostituendo non sia specificata nel modello o nella configurazione di avvio. Se Amazon EC2 Auto Scaling rileva un'istanza non integra, avvia un'istanza sostitutiva. Tuttavia, l'avvio dell'istanza non riesce se non è possibile trovare la coppia di chiavi. Per ulteriori informazioni, consulta Modelli di avvio nella Guida per l'utente di Amazon EC2 Auto Scaling.

Come rimuovere una chiave pubblica da un'istanza

1. Connettiti alla tua istanza.
2. Utilizzare l'editor di testo preferito, aprire il file `.ssh/authorized_keys` nell'istanza. Eliminare le informazioni sulla chiave pubblica e quindi salvare il file.

> **Warning**
>
> Dopo aver rimosso tutte le chiavi pubbliche da un'istanza ed effettuato la disconnessione dall'istanza, non è possibile connettersi nuovamente ad essa a meno che l'AMI non fornisca un altro modo di accedere.

Verifica dell'impronta digitale della coppia di chiavi

Per verificare l'impronta digitale della tua coppia di chiavi, confronta l'impronta digitale visualizzata nella pagina Coppie di chiavi nella console Amazon EC2, o restituita dal comando, con describe-key-pairsl'impronta digitale generata utilizzando la chiave privata sul tuo computer locale. Queste impronte digitali devono corrispondere.

Quando Amazon EC2 calcola un'impronta digitale, potrebbe accodare un padding all'impronta digitale con caratteri =. Altri strumenti, ad esempio ssh-keygen, potrebbero omettere questo padding.

Se stai cercando di verificare l'impronta digitale della tua istanza Linux EC2, non l'impronta digitale della tua coppia di chiavi, vedi Ottenere l'impronta digitale dell'istanza.

Come vengono calcolate le impronte digitali

Amazon EC2 utilizza diverse funzioni hash per calcolare le impronte digitali per le coppie di chiavi RSA e ED25519. Inoltre, per le coppie di chiavi RSA, Amazon EC2 calcola le impronte digitali in modo diverso utilizzando diverse funzioni hash a seconda che la coppia di chiavi sia stata creata da Amazon EC2 o importata in Amazon EC2.

Nella tabella seguente sono elencate le funzioni hash utilizzate per calcolare le impronte digitali per le coppie di chiavi RSA e ED25519 create da Amazon EC2 e importate in Amazon EC2.

(Istanze Linux) Funzioni hash utilizzate per calcolare le impronte digitali

Fonte di coppia di chiavi	Coppie di chiavi RSA (Windows e Linux)	Coppie di chiavi ED25519 (Linux)
Create da Amazon EC2	SHA-1	SHA-256
Importate in Amazon EC2	MD5[1]	SHA-256

[1] Se importi una chiave RSA pubblica in Amazon EC2, l'impronta digitale viene calcolata utilizzando una funzione hash MD5. Ciò è vero indipendentemente da come è stata creata la coppia di chiavi, ad esempio utilizzando uno strumento di terze parti o generando una nuova chiave pubblica da una chiave privata esistente creata con Amazon EC2.

Utilizzare la stessa coppia di chiavi in diverse regioni

Se prevedi di utilizzare la stessa coppia di chiavi per connetterti a istanze diverse Regioni AWS, devi importare la chiave pubblica in tutte le regioni in cui la utilizzerai. Se utilizzi Amazon EC2 per creare la coppia di chiavi, puoi Recupero del materiale delle chiavi pubbliche in modo da poter importare la chiave pubblica nelle altre regioni.

> **Note**
>
> - Se si crea una coppia di chiavi RSA utilizzando Amazon EC2 e poi una chiave pubblica dalla chiave privata Amazon EC2, le chiavi pubbliche importate avranno un'impronta

digitale diversa rispetto alla chiave pubblica originale. Questo accade perché l'impronta digitale della chiave RSA originale creata con Amazon EC2 viene calcolata utilizzando la funzione hash SHA-1, mentre l'impronta digitale delle chiavi RSA importate viene calcolata utilizzando una funzione hash MD5.

- Per le coppie di chiavi ED25519, le impronte digitali saranno uguali indipendentemente dal fatto che siano state create da Amazon EC2 o importate in Amazon EC2, poiché la stessa funzione hash SHA-256 viene utilizzata per calcolare l'impronta digitale.

Creazione di un'impronta digitale dalla chiave privata

Utilizza uno dei seguenti comandi per generare un'impronta digitale dalla chiave privata sul computer locale.

Se si sta utilizzando un computer locale Windows, è possibile eseguire i comandi seguenti tramite Windows Subsystem per Linux (WSL). Installare WSL e una distribuzione Linux seguendo le istruzioni della Guida all'installazione di Windows 10. L'esempio riportato nelle istruzioni installa la distribuzione Ubuntu di Linux, ma si può installare qualunque distribuzione. Affinché vengano applicate le modifiche, ti verrà chiesto di riavviare il computer.

- Se la coppia di chiavi è stata creata tramite Amazon EC2

  Utilizza gli strumenti di OpenSSL per generare un'impronta digitale come riportato negli esempi seguenti.

  Per le coppie di chiavi RSA:

  ```
  openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |
   openssl sha1 -c
  ```

  (istanze Linux) Per le coppie di chiavi ED25519:

  ```
  ssh-keygen -l -f path_to_private_key
  ```

- (Solo coppie di chiavi RSA) Se hai importato la chiave pubblica in Amazon EC2

  Puoi seguire questa procedura indipendentemente dalla modalità con cui hai creato la coppia di chiavi, ad esempio utilizzando uno strumento di terzi o generando una nuova chiave pubblica da una chiave privata esistente creata utilizzando Amazon EC2

Utilizza gli strumenti di OpenSSL per generare l'impronta digitale come riportato nell'esempio seguente.

```
openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
```

- Se una coppia di chiavi OpenSSH è stata creata mediante OpenSSH 7.8 o versioni successive e la chiave pubblica è stata importata in Amazon EC2

  Utilizza ssh-keygen per generare un'impronta digitale come riportato negli esempi seguenti.

  Per le coppie di chiavi RSA:

```
ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER
 | openssl md5 -c
```

  (istanze Linux) Per le coppie di chiavi ED25519:

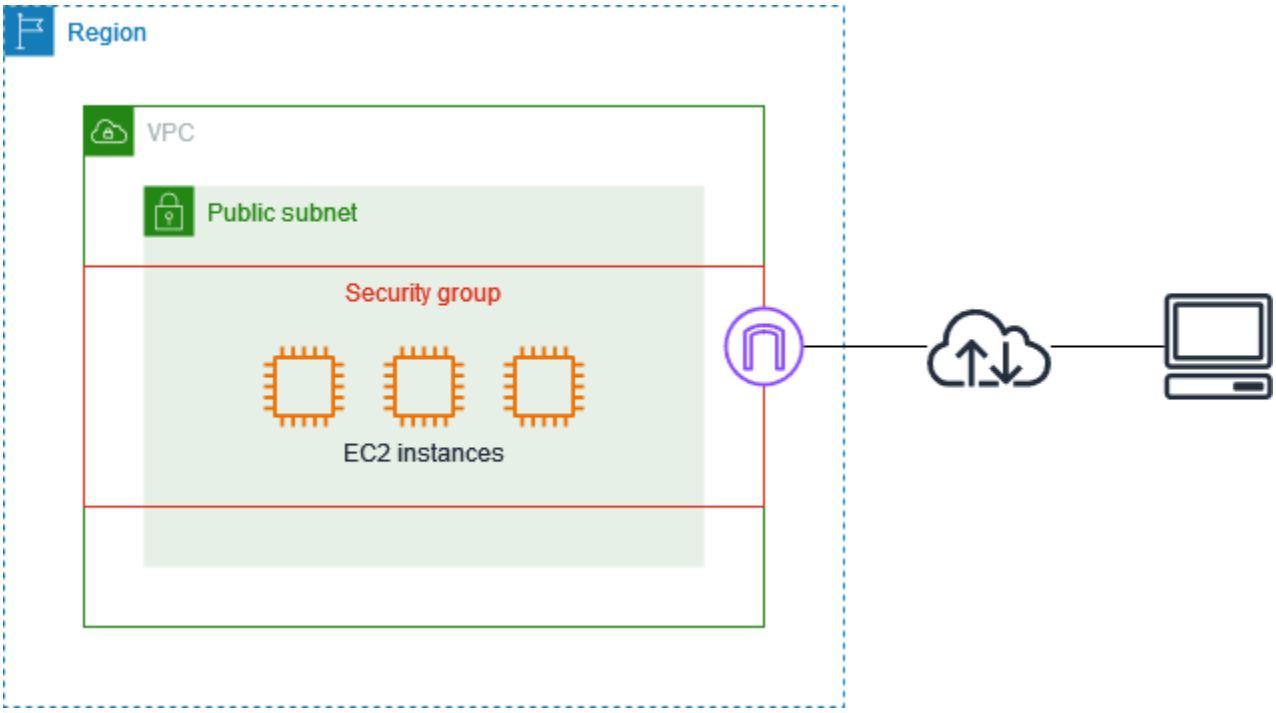
```
ssh-keygen -l -f path_to_private_key
```

Gruppi di sicurezza Amazon EC2 per le tue istanze EC2

Un gruppo di sicurezza funge da firewall virtuale per le istanze EC2 per controllare il traffico in entrata e quello in uscita. Le regole in entrata controllano il traffico in entrata verso l'istanza e le regole in uscita controllano il traffico in uscita dall'istanza. Quando avvii un'istanza puoi specificare uno o più gruppi di sicurezza. Se non specifichi un gruppo di sicurezza, Amazon EC2 usa il gruppo di sicurezza predefinito per il VPC. A ciascun gruppo di sicurezza possono essere aggiunte regole che permettono il traffico da e verso le istanze associate. Puoi modificare le regole di un gruppo di sicurezza in qualsiasi momento. Regole nuove e modificate vengono applicate automaticamente a tutte le istanze associate al gruppo di sicurezza. Quando Amazon EC2 decide se permettere al traffico di raggiungere un'istanza, valuta tutte le regole da tutti i gruppi di sicurezza associati all'istanza.

Il diagramma seguente mostra un VPC con una sottorete, un gateway Internet e un gruppo di sicurezza. La sottorete contiene istanze EC2. Il gruppo di sicurezza viene assegnato alle istanze. L'unico traffico che raggiunge l'istanza è quello consentito dalle regole del gruppo di sicurezza. Ad esempio, se il gruppo di sicurezza contiene una regola che consente il traffico SSH dalla rete, è possibile connettersi all'istanza dal computer tramite SSH. Se il gruppo di sicurezza contiene una

regola che consente tutto il traffico proveniente dalle risorse ad essa assegnate, ogni istanza può ricevere tutto il traffico inviato dalle altre istanze.



Dopo l'avvio di un'istanza, è possibile modificare i relativi gruppi di sicurezza. I gruppi di sicurezza sono associati alle interfacce di rete. Quando si modificano i gruppi di sicurezza di un'istanza, cambiano anche i gruppi di sicurezza associati all'interfaccia di rete primaria (eth0). Per ulteriori informazioni, consulta Modifica del gruppo di sicurezza di un'istanza. Si possono modificare anche i gruppi di sicurezza associati a qualunque altra interfaccia di rete. Per ulteriori informazioni, consulta Modifica degli attributi dell'interfaccia di rete.

La sicurezza è una responsabilità condivisa tra AWS te e te. Per ulteriori informazioni, vedereSicurezza in Amazon EC2. AWS fornisce i gruppi di sicurezza come uno degli strumenti per proteggere le istanze e devi configurarli per soddisfare le tue esigenze di sicurezza. Se i gruppi di sicurezza non soddisfano pienamente i requisiti, oltre a utilizzare i gruppi di sicurezza è possibile mantenere il firewall su tutte le istanze.

L'utilizzo di gruppi di sicurezza non comporta costi supplementari.

Indice

- Utilizzo dei gruppi di sicurezza
- Regole del gruppo di sicurezza per diversi casi d'uso

Regole del gruppo di sicurezza

Le regole di un gruppo di sicurezza controllano il traffico in entrata autorizzato a raggiungere le istanze associate al gruppo di sicurezza e il traffico in uscita autorizzato a lasciarle.

Di seguito sono riportate le caratteristiche delle regole dei gruppi di sicurezza:

- Per impostazione predefinita, i gruppi di sicurezza includono regole in uscita che autorizzano tutto il traffico in uscita. È possibile eliminare queste regole. Notare che per impostazione predefinita, Amazon EC2 blocca il traffico sulla porta 25. Per ulteriori informazioni, consulta Restrizione sull'e-mail inviata tramite la porta 25.
- Le regole dei gruppi di sicurezza sono sempre permissive; non è possibile creare regole che negano l'accesso.
- Le regole dei gruppi di sicurezza consentono di filtrare il traffico in base ai protocolli e ai numeri di porta.
- I gruppi di sicurezza sono stateful — Se invii una richiesta da un'istanza, il traffico in risposta alla richiesta è autorizzato a entrare, indipendentemente dalle regole dei gruppi di sicurezza in entrata. Per i gruppi di sicurezza VPC, ciò significa anche che le risposte al traffico in entrata sono autorizzate a uscire, indipendentemente dalle regole in uscita. Per ulteriori informazioni, consulta Monitoraggio della connessione al gruppo di sicurezza.
- Si possono aggiungere e rimuovere regole in qualunque momento. Le modifiche vengono applicate automaticamente alle istanze associate al gruppo di sicurezza.

  Gli effetti di alcune modifiche delle regole possono dipendere dalle modalità di monitoraggio del traffico. Per ulteriori informazioni, consulta Monitoraggio della connessione al gruppo di sicurezza.
- Se associ a un'istanza più gruppi di sicurezza, le regole di ciascun gruppo di sicurezza vengono aggregate efficacemente per creare un unico set di regole. Amazon EC2 utilizza questo set di regole per determinare se consentire l'accesso o meno.

  Puoi assegnare più gruppi di sicurezza a un'istanza. Pertanto, un'istanza può disporre di centinaia di regole valide. Questo può causare problemi nell'accesso all'istanza. È consigliabile comprimere le regole il più possibile.

> **Note**
>
> I gruppi di sicurezza non possono bloccare le richieste DNS da o verso il Route 53 Resolver, a volte indicato come «indirizzo IP VPC+2» (vedi Cos'è Amazon Route 53 Resolver? nella Amazon Route 53 Developer Guide) o nella 'AmazonProvidedDNS' (consulta Work with DHCP option sets nella Amazon Virtual Private Cloud User Guide). Se desideri filtrare le richieste DNS tramite il risolutore Route 53, puoi abilitare DNS Firewall per il risolutore Route 53 (consulta DNS Firewall per il risolutore Route 53 nella Guida per sviluppatori di Amazon Route 53).

Per ogni regola, occorre specificare quanto segue:

- Nome: il nome del gruppo di sicurezza (ad esempio, "my-security-group«).

  Questo valore può contenere al massimo 255 caratteri. I caratteri consentiti sono a-z, A-Z, 0-9, spazi e ._-:/()#,@[]+=;{}!$*. Quando il nome contiene spazi finali, eliminiamo gli spazi quando salviamo il nome. Ad esempio, se inserisci “Test Security Group ". per il nome, lo memorizziamo come “Test Security Group”.
- Protocollo: il protocollo da autorizzare. I protocolli più comuni sono 6 (TCP) 17 (UDP) e 1 (ICMP).
- Intervallo di porte: per un protocollo personalizzato o per TCP e UDP, l'intervallo di porte da autorizzare. Puoi specificare un solo numero di porta (ad esempio 22) o un intervallo dei numeri di porta (ad esempio `7000-8000`).
- Tipo e codice ICMP: per ICMP, il tipo e il codice ICMP. Ad esempio, utilizza il tipo 8 per la richiesta Echo ICMP o il tipo 128 per la richiesta Echo ICMPv6.
- Origine o destinazione: l'origine (regole in entrata) o la destinazione (regole in uscita) del traffico da consentire. Specifica una delle seguenti proprietà:
  - Un singolo indirizzo IPv4. Devi utilizzare la lunghezza del prefisso `/32`. Ad esempio, `203.0.113.1/32`.
  - Un singolo indirizzo IPv6. Devi utilizzare la lunghezza del prefisso `/128`. Ad esempio, `2001:db8:1234:1a00::123/128`.
  - Un intervallo di indirizzi IPv4 in notazione a blocco CIDR. Ad esempio, `203.0.113.0/24`.
  - Un intervallo di indirizzi IPv6 in notazione a blocco CIDR. Ad esempio, `2001:db8:1234:1a00::/64`.

  - L'ID di un elenco di prefissi. Ad esempio, `pl-1234abc1234abc123`. Per ulteriori informazioni, consulta Elenchi di prefissi nella Guida per l'utente di Amazon VPC.
  - L'ID di un gruppo di sicurezza (indicato di seguito come il gruppo di sicurezza specificato). Ad esempio, il gruppo di sicurezza corrente, un gruppo di sicurezza dello stesso VPC o un gruppo di sicurezza per un VPC in peering. Questo consente il traffico basato sugli indirizzi IP privati delle risorse associate al gruppo di sicurezza specificato. Non aggiunge regole dal gruppo di sicurezza specificato al gruppo di sicurezza corrente.
- (Opzionale) Descrizione: puoi aggiungere una descrizione della regola, per semplificarne l'identificazione in un secondo momento. Una descrizione può essere lunga fino a 255 caratteri. I caratteri consentiti sono a-z, A-Z, 0-9, spazi e ._-:/()#,@[]+=;{}!$*.

Quando crei una regola del gruppo di sicurezza, AWS assegna un ID univoco alla regola. È possibile utilizzare l'ID di una regola quando si utilizza l'API o la CLI per modificare o eliminare la regola.

Quando specifichi un gruppo di sicurezza come l'origine o la destinazione di una regola, la regola influenza tutte le istanze associate al gruppo di sicurezza. Il traffico in entrata è autorizzato in base agli indirizzi IP privati delle istanze associate al gruppo di sicurezza di origine (e non in base agli indirizzi IP elastici o pubblici). Per ulteriori informazioni sugli indirizzi IP, consulta Indirizzamento IP per le istanze Amazon EC2. Una regola di gruppo di sicurezza obsoleta è una regola che fa riferimento a un gruppo di sicurezza eliminato nello stesso VPC o in un VPC simile, o che fa riferimento a un gruppo di sicurezza in un VPC simile per il quale la connessione peering VPC è stata eliminata. Per ulteriori informazioni, consulta Utilizzo di regole di gruppo di sicurezza obsolete nella Amazon VPC Peering Guide.

Se esistono più regole per una determinata porta, Amazon EC2 applica la regola più permissiva. Ad esempio, se disponi di una regola che consente l'accesso alla porta TCP 22 (SSH) dall'indirizzo IP 203.0.113.1 e un'altra regola che consente l'accesso alla porta TCP 22 da parte di tutti, tutti hanno accesso alla porta TCP 22.

Quando aggiungi, aggiorni o rimuovi delle regole, queste si applicano automaticamente a tutte le istanze associate al gruppo di sicurezza.

Monitoraggio della connessione al gruppo di sicurezza

I gruppi di sicurezza utilizzano il monitoraggio delle connessioni per tracciare le informazioni sul traffico da e verso l'istanza. Le regole si applicano in base allo stato della connessione per stabilire se il traffico è autorizzato o negato. Con questo approccio, i gruppi di sicurezza sono con stato. Ovvero,

le risposte al traffico in entrata possono uscire dall'istanza a prescindere dalle regole del gruppo di sicurezza in uscita, e viceversa.

Ad esempio, supponiamo di avviare un comando come netcat o similare sulle istanze dal computer di casa e che le regole del gruppo di sicurezza in entrata consentano il traffico ICMP. Le informazioni sulla connessione (incluse le informazioni sulla porta) vengono monitorate. Il traffico in risposta dall'istanza per il comando non viene monitorato come nuova richiesta, ma come connessione stabilita e può uscire dall'istanza, anche se le regole del gruppo di sicurezza in uscita limitano il traffico ICMP in uscita.

Per i protocolli diversi da TCP, UDP o ICMP, vengono monitorati solo l'indirizzo IP e il numero di protocollo. Se l'istanza invia traffico a un altro host e l'host invia lo stesso tipo di traffico verso l'istanza entro 600 secondi, verrà accettato dal gruppo di sicurezza dell'istanza a prescindere dalle regole del gruppo di sicurezza in entrata. Il gruppo di sicurezza lo accetta perché considerato traffico di risposta al traffico originale.

Quando si modifica una regola del gruppo di sicurezza, le connessioni tracciate non vengono interrotte immediatamente. Il gruppo di sicurezza continua a consentire i pacchetti fino al timeout delle connessioni esistenti. Per avere la certezza che il traffico venga interrotto immediatamente o che tutto il traffico sia soggetto alle regole del firewall indipendentemente dallo stato di tracciamento, è possibile utilizzare una lista di controllo degli accessi di rete per la sottorete. Le liste di controllo degli accessi di rete sono stateless, pertanto non autorizzano automaticamente il traffico di risposta. L'aggiunta di una lista di controllo degli accessi di rete che blocca il traffico in entrambe le direzioni interrompe le connessioni esistenti. Per ulteriori informazioni, consulta la sezione relativa alle Liste di controllo degli accessi di rete nella Guida per l'utente di Amazon VPC.

> **Note**
>
> I gruppi di sicurezza non hanno alcun effetto sul traffico DNS da o verso il Route 53 Resolver, a volte indicato come «indirizzo IP VPC+2» (vedi Cos'è Amazon Route 53 Resolver? nella Amazon Route 53 Developer Guide) o nella 'AmazonProvidedDNS' (consulta Work with DHCP option sets nella Amazon Virtual Private Cloud User Guide). Se desideri filtrare le richieste DNS tramite il risolutore Route 53, puoi abilitare DNS Firewall per il risolutore Route 53 (consulta DNS Firewall per il risolutore Route 53 nella Guida per sviluppatori di Amazon Route 53).

Connessioni non tracciate

Non vengono monitorati tutti i flussi di traffico. Se una regola del gruppo di sicurezza consente i flussi TCP o UDP per tutto il traffico (0.0.0.0/0 o: :/0) e esiste una regola corrispondente nell'altra direzione che consente tutto il traffico di risposta (0.0.0.0/0 o: :/0) per qualsiasi porta (0-65535), quel flusso di traffico non viene tracciato, a meno che non faccia parte di una connessione tracciata automaticamente. Il traffico in risposta per un flusso non monitorato può scorrere in base alla regola in entrata o in uscita che autorizza il traffico in risposta, non in base alle informazioni di monitoraggio.

Un flusso di traffico non monitorato viene interrotto immediatamente se la regola che permette il flusso è rimossa o modificata. Ad esempio, se disponi di una regola in uscita (0.0.0.0/0) aperta e rimuovi una regola che autorizza tutto il traffico SSH (porta TCP 22) in entrata (0.0.0.0/0) verso l'istanza (o la modifichi per non consentire più la connessione), le connessioni SSH all'istanza esistenti vengono immediatamente rimosse. Poiché la connessione non è stata in precedenza tracciata, la modifica interromperà la connessione. D'altra parte, se disponi di una regola in entrata più rigida che inizialmente consente una connessione SSH (ovvero la connessione è stata monitorata), ma modifichi la regola per non consentire più nuove connessioni dall'indirizzo del client SSH corrente, la connessione SSH esistente non verrà interrotta poiché è monitorata.

Connessioni monitorate automaticamente

Le connessioni effettuate tramite quanto segue vengono tracciate automaticamente, anche se la configurazione del gruppo di sicurezza non richiede altrimenti il tracciamento:

- Internet Gateway egress-only
- Acceleratori di Global Accelerator
- Gateway NAT
- Endpoint Firewall Network Firewall
- Network Load Balancers
- AWS PrivateLink (endpoint VPC di interfaccia)
- AWS Lambda (interfacce di rete elastiche Hyperplane)

Permessi di tracciamento delle connessioni

Amazon EC2 definisce il numero massimo di connessioni che possono essere monitorate per ogni istanza. Una volta raggiunto il massimo, tutti i pacchetti inviati o ricevuti vengono eliminati perché non è possibile stabilire una nuova connessione. In questo caso, le applicazioni che inviano e ricevono

pacchetti non possono comunicare correttamente. Utilizza il parametro delle prestazioni di rete `conntrack_allowance_available` per determinare il numero di connessioni tracciate ancora disponibili per quel tipo di istanza.

Per determinare se i pacchetti sono stati eliminati perché il traffico di rete per l'istanza ha superato il numero massimo di connessioni che possono essere monitorate, utilizza il parametro delle prestazioni di rete `conntrack_allowance_exceeded`. Per ulteriori informazioni, consulta Monitoraggio delle prestazioni di rete per l'istanza EC2.

Con Elastic Load Balancing, se si supera il numero massimo di connessioni che è possibile monitorare per istanza, si consiglia di ridimensionare il numero di istanze registrate con il load balancer o la dimensione delle istanze registrate con il load balancer.

Considerazioni sulle prestazioni di tracciamento delle connessioni

Il routing asimmetrico, in cui il traffico entra in un'istanza attraverso un'interfaccia di rete e esce da un'altra interfaccia di rete, può ridurre le prestazioni di picco che un'istanza può raggiungere se i flussi vengono tracciati.

Per mantenere le massime prestazioni quando il tracciamento delle connessioni è abilitato per i gruppi di sicurezza, consigliamo la seguente configurazione:

- Evita topologie di routing asimmetriche, se possibile.
- Invece di utilizzare i gruppi di sicurezza per il filtraggio, utilizzate gli ACL di rete.
- Se devi utilizzare gruppi di sicurezza con tracciamento delle connessioni, configura il timeout di connessione più breve possibile.

Per ulteriori informazioni sull'ottimizzazione delle prestazioni del sistema Nitro, consulta. Considerazioni sul sistema Nitro per l'ottimizzazione delle prestazioni

Timeout di tracciamento delle connessioni inattive

Il gruppo di sicurezza tiene traccia di ogni connessione stabilita per garantire che i pacchetti restituiti vengano consegnati come previsto. Per ciascuna istanza esiste un numero massimo di connessioni che possono essere monitorate. Le connessioni che rimangono inattive possono portare all'esaurimento del tracciamento delle connessioni, impedire il tracciamento delle connessioni ed eliminare i pacchetti. Ora puoi impostare il timeout in secondi per il tracciamento delle connessioni inattive su un'interfaccia di rete elastica.

> **Note**
>
> Questa funzionalità è disponibile solo per le istanze create sul sistema Nitro. AWS

Esistono tre timeout configurabili:

- Timeout TCP stabilito: il timeout (in secondi) per le connessioni TCP inattive in uno stato stabilito. Minimo: 60 secondi. Massimo: 432.000 secondi (5 giorni). Valore predefinito: 432.000 secondi. Consigliato: meno di 432.000 secondi.
- Timeout UDP: il timeout (in secondi) per i flussi UDP inattivi che hanno registrato traffico solo in un'unica direzione o una singola transazione richiesta-risposta. Minimo: 30 secondi. Massimo 60 secondi. Valore predefinito: 30 secondi.
- Timeout del flusso UDP: il timeout (in secondi) per i flussi UDP inattivi classificati come flussi che hanno registrato più di una transazione richiesta-risposta. Minimo: 60 secondi. Massimo: 180 secondi (3 minuti). Valore predefinito: 180 secondi.

Potresti voler modificare i timeout predefiniti per uno dei seguenti casi:

- Se stai monitorando le connessioni tracciate utilizzando i parametri delle prestazioni di rete di Amazon EC2, i parametri conntrack_allowance_exceeded e conntrack_allowance_available consentono di monitorare i pacchetti persi e tenere traccia dell'utilizzo della connessione per gestire in modo proattivo la capacità delle istanze EC2 con azioni di aumento o riduzione per contribuire a soddisfare la domanda di connessioni di rete prima di perdere i pacchetti. Se stai osservando un calo di conntrack_allowance_exceeded sulle tue istanze EC2, potresti trarre vantaggio dall'impostare un timeout TCP più basso per tenere conto delle sessioni TCP/UDP obsolete causate da client o middlebox di rete impropri.
- In genere, i sistemi di bilanciamento del carico o i firewall hanno un timeout di inattività stabilito dal protocollo TCP compreso tra 60 e 90 minuti. Se utilizzi carichi di lavoro che dovrebbero gestire un numero molto elevato di connessioni (superiore a 100.000) da dispositivi come i firewall di rete, si consiglia di configurare un timeout simile su un'interfaccia di rete EC2.
- Se stai eseguendo un carico di lavoro che utilizza una topologia di routing asimmetrica, ti consigliamo di configurare un timeout di inattività stabilito dal protocollo TCP di 60 secondi.
- Se esegui carichi di lavoro con un numero elevato di connessioni come DNS, SIP, SNMP, Syslog, Radius e altri servizi che utilizzano principalmente UDP per soddisfare le richieste, l'impostazione

del timeout 'UDP-Stream' su 60 secondi offre un rapporto scala/prestazioni più elevato per la capacità esistente e per prevenire errori gray.

- Per le connessioni TCP/UDP tramite Network Load Balancer (NLB) ed Elastic Load Balancing (ELB), tutte le connessioni vengono tracciate. Il valore di timeout di inattività per i flussi TCP è di 350 secondi e per i flussi UDP è di 120 secondi e varia a seconda dei valori di timeout a livello di interfaccia. Potresti voler configurare i timeout a livello di interfaccia di rete per consentire una maggiore flessibilità di timeout rispetto ai valori predefiniti per ELB/NLB.

È possibile configurare i timeout di tracciamento della connessione quando si eseguono le seguenti operazioni:

- Creazione di un'interfaccia di rete
- Modifica degli attributi dell'interfaccia di rete
- Avvio di un'istanza EC2
- Creazione di un modello di avvio di un'istanza EC2

Esempio

Nell'esempio seguente, il gruppo di sicurezza ha regole in entrata specifiche che autorizzano il traffico TCP e ICMP e regole in uscita che autorizzano tutto il traffico in uscita.

In entrata

Tipo di protocollo	Numero della porta	Origine
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	Tutti	0.0.0.0/0

In uscita

Tipo di protocollo	Numero della porta	Destinazione
Tutti	Tutti	0.0.0.0/0
Tutti	Tutti	::/0

Con una connessione di rete diretta all'istanza o all'interfaccia di rete, il comportamento di monitoraggio è il seguente:

- Il traffico TCP in entrata e in uscita sulla porta 22 (SSH) viene monitorato in quanto la regola in entrata consente il traffico solo da 203.0.113.1/32 e non da tutti gli indirizzi IP (0.0.0.0/0).
- Il traffico TCP in entrata e in uscita sulla porta 80 (HTTP) non viene monitorato, perché le regole in entrata e in uscita autorizzano il traffico da tutti gli indirizzi IP.
- Il traffico ICMP viene sempre monitorato.

Se viene rimossa la regola in uscita per il traffico IPv4, viene monitorato tutto il traffico IPv4 in entrata e in uscita, incluso il traffico sulla porta 80 (HTTP). Lo stesso vale per il traffico IPv6 se si rimuove la regola in uscita per il traffico IPv6.

Gruppi di sicurezza predefiniti e personalizzati

Il tuo AWS account ha automaticamente un gruppo di sicurezza predefinito per il VPC predefinito in ogni regione. Se non specifichi un gruppo di sicurezza quando avvii un'istanza, questa viene automaticamente associata al gruppo di sicurezza predefinito per il VPC. Se non vuoi che le tue istanze utilizzino il gruppo di sicurezza predefinito, puoi creare gruppi di sicurezza personali e specificarli quando avvii le tue istanze.

Indice

Gruppi di sicurezza predefiniti

Ogni VPC include un gruppo di sicurezza predefinito. Ti consigliamo di creare gruppi di sicurezza per istanze o gruppi di istanze specifici invece di utilizzare il gruppo di sicurezza predefinito. Tuttavia,

se non specifichi un gruppo di sicurezza all'avvio di un'istanza, questa viene associata al gruppo di sicurezza predefinito per il VPC.

Il nome di un gruppo di sicurezza predefinito è "default". Di seguito sono descritte le regole predefinite per un gruppo di sicurezza predefinito.

In entrata

Crea	Protocollo	Intervallo porte	Descrizione
sg-1234567890abcdef0	Tutti	Tutti	Consente il traffico in entrata da tutte le risorse assegnate a questo gruppo di sicurezza. L'origine è l'ID di questo gruppo di sicurezza.

In uscita

Destinazione	Protocollo	Intervallo porte	Descrizione
0.0.0.0/0	Tutti	Tutti	Autorizza tutto il traffico IPv4 in uscita.
::/0	Tutti	Tutti	Autorizza tutto il traffico IPv6 in uscita. Questa regola viene aggiunta solo se il VPC ha un blocco CIDR IPv6 associato.

Nozioni di base sui gruppi di sicurezza predefiniti

- È possibile modificare le regole di un gruppo di sicurezza di default.
- Non è possibile eliminare un gruppo di sicurezza predefinito. Se provi a eliminare un gruppo di sicurezza predefinito, restituiamo il seguente codice di errore: `Client.CannotDelete`.

Gruppi di sicurezza personalizzati

Puoi creare più gruppi di sicurezza per rispecchiare i diversi ruoli eseguiti dalle istanze, ad esempio server Web o server di database.

Quando crei un gruppo di sicurezza, devi indicarne il nome e la descrizione. I nomi e le descrizioni dei gruppi di sicurezza possono essere lunghi al massimo 255 caratteri, limitati ai seguenti:

a-z, A-Z, 0-9, spazi e ._-:/()#,@[]+=&;{}!$*

Il nome di un gruppo di sicurezza non può iniziare con sg-. Il nome di un gruppo di sicurezza deve Essere univoco per il VPC.

Di seguito sono descritte le regole predefinite per un gruppo di sicurezza da te creato:

- Non autorizza il traffico in entrata
- Autorizza tutto il traffico in uscita

Dopo aver creato un gruppo di sicurezza, puoi modificarne le regole in entrata per rispecchiare il tipo di traffico in entrata che vuoi raggiunga le istanze associate. Puoi modificare anche le regole in uscita.

Per ulteriori informazioni sui tipi di regole che è possibile aggiungere a un gruppo di sicurezza, consulta Regole del gruppo di sicurezza per diversi casi d'uso.

Utilizzo dei gruppi di sicurezza

Puoi assegnare un gruppo di sicurezza a un'istanza quando la avvii. Quando aggiungi o rimuovi regole, queste modifiche vengono applicate automaticamente a tutte le istanze a cui hai assegnato il gruppo di sicurezza. Per ulteriori informazioni, consulta Assegnazione di un gruppo di sicurezza a un'istanza.

Dopo l'avvio di un'istanza, è possibile modificare i relativi gruppi di sicurezza. Per ulteriori informazioni, consulta Modifica del gruppo di sicurezza di un'istanza.

Puoi creare, visualizzare, aggiornare ed eliminare i gruppi di sicurezza e le relative regole mediante la console Amazon EC2 e gli strumenti a riga di comando.

Attività

- Creazione di un gruppo di sicurezza
- Copia di un gruppo di sicurezza
- Visualizzazione dei gruppi di sicurezza
- Aggiunta di regole a un gruppo di sicurezza

- Aggiornamento delle regole del gruppo di sicurezza
- Eliminazione delle regole da un gruppo di sicurezza
- Eliminare un gruppo di sicurezza
- Assegnazione di un gruppo di sicurezza a un'istanza
- Modifica del gruppo di sicurezza di un'istanza

Creazione di un gruppo di sicurezza

Anche se puoi utilizzare il gruppo di sicurezza predefinito per le istanze, è consigliabile creare gruppi personalizzati per rispecchiare i diversi ruoli eseguiti dalle istanze nel sistema.

Per impostazione predefinita, i nuovi gruppi di sicurezza hanno solo una regola in uscita che autorizza tutto il traffico a lasciare le istanze. Devi aggiungere le regole per autorizzare qualsiasi tipo di traffico in entrata o per limitare quello in uscita.

Un gruppo di sicurezza può essere utilizzato solo nel VPC in cui viene creato.

Console

Per creare un gruppo di sicurezza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. Scegliere Create Security Group (Crea gruppo di sicurezza).
4. Nella sezione Basic details (Dettagli di base), eseguire le operazioni descritte di seguito.
    a. Immettere un nome descrittivo e una breve descrizione del gruppo di sicurezza. Non possono essere modificati dopo la creazione del gruppo di sicurezza. Il nome e la descrizione possono contenere fino a 255 caratteri. I caratteri validi sono a-z, A-Z, 0-9, spazi e ._-:/()#,@[]+=&;{}!$*.
    b. Per VPC, scegliere il VPC.
5. È possibile aggiungere le regole del gruppo di sicurezza a questo punto oppure in un secondo momento. Per ulteriori informazioni, consulta Aggiunta di regole a un gruppo di sicurezza.
6. È possibile aggiungere tag a questo punto oppure in un secondo momento. Per aggiungere un tag, sceglie Aggiungi tag, quindi specifica la chiave e il valore del tag.

7. Scegliere Create Security Group (Crea gruppo di sicurezza).

Command line

Per creare un gruppo di sicurezza

Utilizzare uno dei seguenti comandi:

- create-security-group (AWS CLI)
- New-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Copia di un gruppo di sicurezza

Puoi creare un nuovo gruppo di sicurezza creando una copia di uno esistente. Quando copi un gruppo di sicurezza, le regole in entrata e in uscita della copia sono identiche a quelle del gruppo di sicurezza originale. Se il gruppo di sicurezza originale si trova in un VPC, la copia viene creata nello stesso VPC, a meno che non specifichi un VPC diverso.

La copia riceve un nuovo ID del gruppo di sicurezza univoco a cui occorre assegnare un nome. Puoi anche aggiungere una descrizione.

Non è possibile copiare un gruppo di sicurezza da una regione a un'altra.

Puoi creare una copia di un gruppo di sicurezza tramite la console Amazon EC2.

Per copiare un gruppo di sicurezza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. Selezionare il gruppo di sicurezza da copiare e scegliere Actions (Operazioni), Copy to new security group (Copia in nuovo gruppo di sicurezza).
4. Specificare un nome e una descrizione opzionale, quindi modificare il VPC e le regole del gruppo di sicurezza, se necessario.
5. Scegliere Create (Crea).

Visualizzazione dei gruppi di sicurezza

Puoi visualizzare informazioni relative ai gruppi di sicurezza mediante uno dei metodi seguenti.

Console

Per visualizzare i gruppi di sicurezza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. I gruppi di sicurezza vengono elencati. Per visualizzare i dettagli di un gruppo di sicurezza specifico, incluse le regole in entrata e in uscita, scegliere il relativo ID nella colonna Security group ID (ID gruppo di sicurezza).

Command line

Per visualizzare i gruppi di sicurezza

Utilizzare uno dei seguenti comandi.

- describe-security-groups (AWS CLI)
- describe-security-group-rules (AWS CLI)
- Get-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Amazon EC2 Global View

Puoi utilizzare Amazon EC2 Global View per visualizzare i tuoi gruppi di sicurezza in tutte le regioni per le quali il tuo AWS account è abilitato. Per ulteriori informazioni, consulta Amazon EC2 Global View.

Aggiunta di regole a un gruppo di sicurezza

Quando aggiungi una regola a un gruppo di sicurezza, la nuova regola viene applicata automaticamente a tutte le istanze associate al gruppo di sicurezza. Prima che la regola venga applicata si potrebbe verificare un breve ritardo. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza per diversi casi d'uso e Regole del gruppo di sicurezza.

Console

Per aggiungere una regola in entrata a un gruppo di sicurezza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Fai clic su Gruppi di sicurezza nel pannello di navigazione.
3. Seleziona il gruppo di sicurezza e scegli Operazioni, Modifica regole in entrata.
4. Per ogni regola, seleziona Aggiungi regola e completa le attività riportate di seguito.

   a. Per Type (Tipo), scegliere il tipo di protocollo consentito.

      - Per Custom TCP o Custom UDP, devi inserire l'intervallo di porte da consentire. Ad esempio, `0-99`.
      - Per Custom ICMP, è necessario scegliere il tipo ICMP da Protocol. L'intervallo di porte è configurato per te. Ad esempio, per consentire i comandi ping, scegli Echo Request (Richiesta Echo) da Protocol (Protocollo).
      - Se scegli qualsiasi altro tipo, il protocollo e l'intervallo di porte vengono configurati automaticamente.

   b. In Origine, per consentire il traffico, esegui una delle operazioni riportate di seguito.

      - Scegli Personalizzato, quindi immetti un indirizzo IP in notazione CIDR, un blocco CIDR, un altro gruppo di sicurezza o un elenco di prefissi.
      - Seleziona Ovunque per permettere a tutto il traffico per il protocollo specificato di raggiungere l'istanza. Questa opzione aggiunge automaticamente il blocco CIDR IPv4 0.0.0.0/0 come origine. Se il gruppo di sicurezza si trova in un VPC abilitato per IPv6, questa opzione aggiunge automaticamente una regola per il blocco CIDR IPv6 ::/0.

        > ⚠ Warning
        >
        > Se scegli Anywhere (Ovunque), abiliti tutti gli indirizzi IPv4 e IPv6 per fare in modo che l'istanza acceda al protocollo specificato. Se si aggiungono regole per le porte 22 (SSH) o 3389 (RDP), è consigliabile autorizzare solo un indirizzo IP specifico o un intervallo di indirizzi per accedere all'istanza.

      - Scegliere My IP (Il mio IP) per permettere il traffico in entrata solo dall'indirizzo IPv4 pubblico del computer locale.

   c. Per Description (Descrizione), specificare facoltativamente una breve descrizione della regola.

5. Scegliere Anteprima modifiche, Salva regole.

Per aggiungere una regola in uscita a un gruppo di sicurezza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Gruppi di sicurezza nel pannello di navigazione.
3. Seleziona il gruppo di sicurezza e scegli Operazioni, Modifica regole in uscita.
4. Per ogni regola, seleziona Aggiungi regola e completa le attività riportate di seguito.
   a. Per Type (Tipo), scegliere il tipo di protocollo consentito.
      - Per Custom TCP o Custom UDP, devi inserire l'intervallo di porte da consentire. Ad esempio, `0-99`.
      - Per Custom ICMP, è necessario scegliere il tipo ICMP da Protocol. L'intervallo di porte è configurato per te.
      - Se si sceglie qualsiasi altro tipo, il protocollo e l'intervallo di porte vengono configurati automaticamente.
   b. Per Destination (Destinazione), eseguire una delle operazioni seguenti.
      - Scegli Personalizzato quindi immetti un indirizzo IP in notazione CIDR, un blocco CIDR, un altro gruppo di sicurezza o un elenco di prefissi per cui consentire il traffico in uscita.
      - Scegliere Anywhere (Ovunque) per consentire il traffico in uscita verso tutti gli indirizzi IP. Questa opzione aggiunge automaticamente il blocco CIDR IPv4 0.0.0.0/0 come destinazione.

        Se il gruppo di sicurezza si trova in un VPC abilitato per IPv6, questa opzione aggiunge automaticamente una regola per il blocco CIDR IPv6 ::/0.
      - Scegliere My IP (Il mio IP) per consentire il traffico in uscita solo verso l'indirizzo IPv4 pubblico del computer locale.
   c. (Facoltativo) Per Descrizione, specifica una breve descrizione della regola.
5. Scegliere Preview changes (Anteprima modifiche), Confirm (Conferma).

Command line

Per aggiungere regole a un gruppo di sicurezza

Utilizzare uno dei seguenti comandi.

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Per aggiungere una o più regole in uscita a un gruppo di sicurezza

Utilizzare uno dei seguenti comandi.

- authorize-security-group-egress (AWS CLI)
- Grant-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Aggiornamento delle regole del gruppo di sicurezza

Puoi aggiornare una regola del gruppo di sicurezza mediante uno dei metodi descritti di seguito. La regola aggiornata viene applicata automaticamente a tutte le istanze associate al gruppo di sicurezza.

Console

Quando modifichi il protocollo, l'intervallo di porte, l'origine o la destinazione di una regola di un gruppo di sicurezza esistente tramite console, la console elimina la regola esistente e ne aggiunge una nuova.

Per aggiornare una regola del gruppo di sicurezza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Gruppi di sicurezza nel pannello di navigazione.
3. Selezionare il gruppo di sicurezza.
4. Scegli Actions (Operazioni), Edit inbound rules (Modifica le regole in entrata) per aggiornare una regola per il traffico in entrata oppure Actions (Operazioni), Edit outbound rules (Modifica le regole in uscita) per aggiornare una regola per il traffico in uscita.
5. Aggiornare la regola come richiesto.
6. Scegliere Preview changes (Anteprima modifiche), Confirm (Conferma).

Come aggiungere i tag a una regola del gruppo di sicurezza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Gruppi di sicurezza nel pannello di navigazione.

3. Selezionare il gruppo di sicurezza.
4. In Regole in entrata o Regole in uscita, seleziona la casella di controllo della regola e quindi scegli Gestisci tag.
5. La pagina Gestisci tag visualizza tutti i tag assegnati alla regola. Per aggiungere un tag, selezionare Add tag (Aggiungi tag), quindi specifica la chiave del tag e il suo valore. Per eliminare un tag, scegliere Remove (Rimuovi) accanto al tag che desideri eliminare.
6. Selezionare Save changes (Salva modifiche).

Command line

Non è possibile modificare il protocollo, l'intervallo di porte o l'origine o la destinazione di una regola esistente mediante l'API di Amazon EC2 o uno strumento a riga di comando. Devi invece eliminare la regola esistente e aggiungerne una nuova. Tuttavia, puoi aggiornare la descrizione di una regola esistente.

Per aggiornare una regola

Utilizza uno dei seguenti comandi.

- modify-security-group-rules (AWS CLI)

Per aggiornare la descrizione di una regola in entrata esistente

Utilizzare uno dei seguenti comandi.

- update-security-group-rule-descrizioni-ingress ()AWS CLI
- Update-EC2SecurityGroupRuleIngressDescription (AWS Tools for Windows PowerShell)

Per aggiornare la descrizione di una regola in uscita esistente

Utilizzare uno dei seguenti comandi.

- update-security-group-rule-descrizioni-uscita ()AWS CLI
- Update-EC2SecurityGroupRuleEgressDescription (AWS Tools for Windows PowerShell)

Come aggiungere i tag a una regola del gruppo di sicurezza

Utilizzare uno dei seguenti comandi.

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Eliminazione delle regole da un gruppo di sicurezza

Quando elimini una regola da un gruppo di sicurezza, la modifica viene applicata automaticamente a tutte le istanze associate al gruppo di sicurezza.

Puoi eliminare regole da un gruppo di sicurezza mediante uno dei metodi descritti di seguito.

Console

Per eliminare una regola del gruppo di sicurezza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. Selezionare il gruppo di sicurezza da aggiornare, scegliere Actions (Operazioni), quindi selezionare Edit inbound rules (Modifica regole in entrata) per rimuovere una regola in entrata o Edit outbound rules (Modifica regole in uscita) per rimuovere una regola in uscita.
4. Scegliere il pulsante Delete (Elimina) a destra della regola da eliminare.
5. Scegliere Salva regole. In alternativa, scegli Anteprima modifiche, rivedi le modifiche e scegli Conferma.

Command line

Per rimuovere una o più regole in entrata da un gruppo di sicurezza

Utilizzare uno dei seguenti comandi.

- revoke-security-group-ingress (AWS CLI)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Per rimuovere una o più regole in uscita da un gruppo di sicurezza

Utilizzare uno dei seguenti comandi.

- revoke-security-group-egress (AWS CLI)
- Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Eliminare un gruppo di sicurezza

Non è possibile eliminare un gruppo di sicurezza collegato a un'istanza. Non è possibile eliminare il gruppo di sicurezza predefinito. Non è possibile eliminare un gruppo di sicurezza a cui fa riferimento una regola di un altro gruppo di sicurezza nello stesso VPC. Se una delle regole fa riferimento al tuo gruppo di sicurezza, devi eliminarla prima di poter eliminare il gruppo di sicurezza.

Console

Per eliminare un gruppo di sicurezza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Gruppi di sicurezza nel pannello di navigazione.
3. Seleziona il gruppo di sicurezza e scegli Operazioni, Elimina gruppi di sicurezza.
4. Quando viene richiesta la conferma, seleziona Delete (Elimina).

Command line

Per eliminare un gruppo di sicurezza

Utilizzare uno dei seguenti comandi.

- delete-security-group (AWS CLI)
- Remove-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Assegnazione di un gruppo di sicurezza a un'istanza

Quando si avvia l'istanza, è possibile assegnare uno o più gruppi di sicurezza a un'istanza. È inoltre possibile specificare uno o più gruppi di sicurezza in un modello di avvio. I gruppi di sicurezza sono assegnati a tutte le istanze avviate utilizzando il modello di avvio.

- Per assegnare un gruppo di sicurezza a un'istanza quando la avvii, consulta Impostazioni di rete di Avvio di un'istanza utilizzando parametri definiti (nuova console) o Fase 6: configura il gruppo di sicurezza (vecchia console).
- Per specificare un gruppo di sicurezza in un modello di avvio, consulta Impostazioni di rete di Crea un modello di lancio dai parametri.

Modifica del gruppo di sicurezza di un'istanza

Dopo avere avviato un'istanza, è possibile modificarne i gruppi di sicurezza aggiungendoli o rimuovendoli.

Requisiti

- L'istanza deve trovarsi nello stato `running` o `stopped`.
- Un gruppo di sicurezza è specifico di un VPC. Puoi assegnare un gruppo di sicurezza a una o più istanze avviate nel VPC per cui hai creato il gruppo di sicurezza.

Console

Per modificare i gruppi di sicurezza per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza, quindi scegliere Actions (Operazioni), Security (Sicurezza), Change security groups (Cambia gruppi di sicurezza).
4. Per Gruppi di sicurezza associati, selezionare un gruppo di sicurezza dall'elenco e scegliere Aggiungi gruppo di sicurezza.

   Per rimuovere un gruppo di sicurezza già associato, scegliere Rimuovi per tale gruppo di sicurezza.
5. Scegliere Save (Salva).

Command line

Per modificare i gruppi di sicurezza per un'istanza

Utilizzare uno dei seguenti comandi.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Regole del gruppo di sicurezza per diversi casi d'uso

Puoi creare un gruppo di sicurezza e aggiungere regole che rispecchiano il ruolo dell'istanza associata al gruppo di sicurezza. Ad esempio, un'istanza configurata come un server Web richiede regole del gruppo di sicurezza che consentano l'accesso HTTP e HTTPS in entrata. Allo stesso modo, un'istanza di database richiede regole che consentano l'accesso per il tipo di database, ad esempio l'accesso sulla porta 3306 per MySQL.

Di seguito sono illustrati esempi dei tipi di regole che è possibile aggiungere ai gruppi di sicurezza per tipi di accesso specifici.

Esempi

Regole del server Web

Le seguenti regole in entrata permettono l'accesso HTTP e HTTPS da qualunque indirizzo IP. Se il tuo VPC può supportare IPv6, puoi aggiungere regole per controllare il traffico HTTP e HTTPS dagli indirizzi IPv6.

Tipo di protocollo	Numero di protocollo	Porta	IP di origine	Note
TCP	6	80 (HTTP)	0.0.0.0/0	Permette l'accesso HTTP in entrata da qualunque indirizzo IPv4

Tipo di protocollo	Numero di protocollo	Porta	IP di origine	Note
TCP	6	443 (HTTPS)	0.0.0.0/0	Permette l'accesso HTTPS in entrata da qualunque indirizzo IPv4
TCP	6	80 (HTTP)	::/0	Permette l'accesso HTTP in entrata da qualunque indirizzo IPv6.
TCP	6	443 (HTTPS)	::/0	Permette l'accesso HTTPS in entrata da qualunque indirizzo IPv6.

Regole del server di database

Le seguenti regole in entrata sono esempi di regole che è possibile aggiungere per l'accesso al database a seconda del tipo di database in esecuzione sull'istanza. Per ulteriori informazioni sulle istanze Amazon RDS, consulta la Guida per l'utente di Amazon RDS.

Per l'IP di origine, specifica uno dei seguenti valori:

- Un indirizzo IP specifico o un intervallo di indirizzi IP (in notazione di blocco CIDR) nella rete locale
- Un ID del gruppo di sicurezza per un gruppo di istanze che accedono al database

Tipo di protocollo	Numero di protocollo	Porta	Note
TCP	6	1433 (MS SQL)	La porta predefinita di accesso al database di Microsoft SQL Server, ad esempio su un'istanza Amazon RDS
TCP	6	3306 (MYSQL/Aurora)	La porta predefinita di accesso a un database MySQL o Aurora, ad esempio su un'istanza Amazon RDS

Tipo di protocollo	Numero di protocollo	Porta	Note
TCP	6	5439 (Redshift)	La porta predefinita per accedere a un database di cluster Amazon Redshift.
TCP	6	5432 (PostgreSQL)	La porta predefinita di accesso a un database PostgreSQL, ad esempio su un'istanza Amazon RDS
TCP	6	1521 (Oracle)	La porta predefinita di accesso a un database Oracle, ad esempio su un'istanza Amazon RDS

Facoltativamente, è possibile limitare il traffico in uscita dai server di database. Ad esempio, è possibile autorizzare l'accesso a Internet per gli aggiornamenti software, ma limitare tutti gli altri tipi di traffico. Occorre prima rimuovere la regola in uscita predefinita che autorizza tutto il traffico in uscita.

Tipo di protocollo	Numero di protocollo	Porta	IP di destinazione	Note
TCP	6	80 (HTTP)	0.0.0.0/0	Permette l'accesso HTTP in uscita verso qualunque indirizzo IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Permette l'accesso HTTPS in uscita verso qualunque indirizzo IPv4
TCP	6	80 (HTTP)	::/0	(Solo VPC che supportano IPv6) Permette l'accesso HTTP in uscita verso qualunque indirizzo IPv6
TCP	6	443 (HTTPS)	::/0	(Solo VPC che supportano IPv6) Permette l'accesso

Tipo di protocollo	Numero di protocollo	Porta	IP di destinazione	Note
				HTTPS in uscita verso qualunque indirizzo IPv6

Regole per la connessione alle istanze dal computer in uso

Per stabilire la connessione all'istanza, il tuo gruppo di sicurezza deve avere regole in entrata che consentono l'accesso SSH (per le istanze Linux) o l'accesso RDP (per le istanze Windows).

Tipo di protocollo	Numero di protocollo	Porta	IP di origine
TCP	6	22 (SSH)	L'indirizzo IPv4 pubblico del tuo computer o un intervallo di indirizzi IP nella rete locale. Se il VPC può supportare IPv6 e la tua istanza ha un indirizzo IPv6, puoi inserire un indirizzo o un intervallo IPv6.
TCP	6	3389 (RDP)	L'indirizzo IPv4 pubblico del tuo computer o un intervallo di indirizzi IP nella rete locale. Se il VPC può supportare IPv6 e la tua istanza ha un indirizzo IPv6, puoi inserire un indirizzo o un intervallo IPv6.

Regole per la connessione alle istanze da un'istanza con lo stesso gruppo di sicurezza

Per consentire alle istanze associate allo stesso gruppo di sicurezza di comunicare tra loro, devi aggiungere esplicitamente regole apposite.

> **Note**
>
> Se le route vengono configurate per inoltrare il traffico tra due istanze in sottoreti diverse attraverso un'appliance middlebox, è necessario assicurarsi che i gruppi di sicurezza per

entrambe le istanze consentano il flusso del traffico tra le istanze. Il gruppo di sicurezza per ogni istanza deve fare riferimento all'indirizzo IP privato dell'altra istanza o all'intervallo CIDR della sottorete che contiene l'altra istanza come origine. Se si fa riferimento al gruppo di sicurezza dell'altra istanza come origine, allora il flusso del traffico tra le istanze non sarà consentito.

La tabella seguente descrive la regola in entrata per un gruppo di sicurezza che permette alle istanze associate di comunicare tra loro. La regola autorizza tutti i tipi di traffico.

Tipo di protocollo	Numero di protocollo	Porte	IP di origine
-1 (Tutti)	-1 (Tutti)	-1 (Tutti)	L'ID del gruppo di sicurezza o l'intervallo CIDR della sottorete che contiene l'altra istanza (vedi nota).

Regole per Ping/ICMP

Il comando ping è un tipo di traffico ICMP. Per effettuare il ping dell'istanza, devi aggiungere una delle seguenti regole ICMP in entrata.

Type	Protocollo	Origine		
ICMP personalizzato - IPv4	Richiesta echo	L'indirizzo IPv4 pubblico del tuo computer, un indirizzo IPv4 specifico o un indirizzo IPv4 o IPv6 di qualsiasi provenienza.		
Tutti ICMP - IPv4	ICMP IPv4 (1)	L'indirizzo IPv4 pubblico del tuo computer, un indirizzo IPv4		

Type	Protocollo	Origine		
		specifico o un indirizzo IPv4 o IPv6 di qualsiasi provenienza.		

Per utilizzare il comando ping6 per eseguire il ping degli indirizzi IPv6 della tua istanza, devi aggiungere la seguente regola ICMPv6 in entrata.

Type	Protocollo	Origine		
Tutto ICMP - IPv6	ICMP IPv6 (58)	L'indirizzo IPv6 del tuo computer, un indirizzo IPv4 specifico o un indirizzo IPv4 o IPv6 di qualsiasi provenienza.		

Regole del server DNS

Se hai configurato un'istanza EC2 come server DNS, devi verificare che il traffico TCP e UDP possa raggiungere il server DNS tramite la porta 53.

Per l'IP di origine, specifica uno dei seguenti valori:

- Un indirizzo IP o un intervallo di indirizzi IP (in notazione di blocco CIDR) in una rete
- L'ID di un gruppo di sicurezza per il set di istanze nella rete che richiedono l'accesso al server DNS

Tipo di protocollo	Numero di protocollo	Porta
TCP	6	53
UDP	17	53

Regole Amazon EFS

Se utilizzi un file system Amazon EFS con le istanze Amazon EC2 il gruppo di sicurezza che associ ai target di montaggio Amazon EFS deve autorizzare il traffico sul protocollo NFS.

Tipo di protocollo	Numero di protocollo	Porte	IP di origine	Note
TCP	6	2049 (NFS)	L'ID del gruppo di sicurezza	Permette l'accesso NFS in entrata dalle risorse (compreso l'obiettivo di montaggio) associate a questo gruppo di sicurezza.

Per montare un file system Amazon EFS su un'istanza Amazon EC2, devi connetterti all'istanza. Di conseguenza, il gruppo di sicurezza associato all'istanza deve avere regole che autorizzano il traffico SSH in entrata dal computer locale o dalla rete locale.

Tipo di protocollo	Numero di protocollo	Porte	IP di origine	Note
TCP	6	22 (SSH)	L'intervallo di indirizzi IP del computer locale o l'intervallo di indirizzi IP (in notazione di blocco CIDR) per la rete.	Permette l'accesso SSH in entrata dal tuo computer locale.

Regole Elastic Load Balancing

Se utilizzi un sistema di bilanciamento del carico (load balancer), il gruppo di sicurezza a esso associato deve avere regole che permettono la comunicazione con le istanze o con i target. Per ulteriori informazioni, consulta Configurazione dei gruppi di sicurezza per Classic Load Balancer nella Guida per l'utente per Classic Load Balancer e Gruppi di sicurezza per l'Application Load Balancer nella Guida per l'utente per Application Load Balancer.

Regole del peering di VPC

Puoi aggiornare le regole in entrata o in uscita per i gruppi di sicurezza VPC per fare riferimento a gruppi di sicurezza nel VPC collegato in peering. In questo modo, si consente il traffico verso e da istanze associate al gruppo di sicurezza a cui si fa riferimento nel VPC collegato in peering. Per ulteriori informazioni su come configurare i gruppi di sicurezza per il peering di VPC, consulta Aggiornamento dei gruppi di sicurezza per fare riferimento a gruppi nel VPC in peering.

NitroTPM

Nitro Trusted Platform Module (NitroTPM) è un dispositivo virtuale fornito da AWS Nitro System e conforme alle specifiche TPM 2.0. Archivia in modo sicuro gli artefatti (come password, certificati o chiavi di crittografia) utilizzati per autenticare l'istanza. NitroTPM può generare chiavi e utilizzarle per funzioni crittografiche (come hashing, firma, crittografia e decrittografia).

NitroTPM fornisce l'avvio misurato, un processo in cui il bootloader e il sistema operativo creano hash crittografici di ogni binario di avvio e li combinano con i valori precedenti nei PCR (Platform Configuration Registers) interni di NitroTPM. Con l'avvio misurato, è possibile ottenere valori PCR firmati da NitroTPM e utilizzarli per dimostrare alle entità remote l'integrità del software di avvio dell'istanza. Questo è noto come attestazione remota.

Con NitroTPM, è possibile taggare chiavi e segreti con un valore PCR specifico in modo da renderli sempre inaccessibili se il valore del PCR, e quindi l'integrità dell'istanza, cambia. Questa speciale forma di accesso condizionale è indicata come sealing e annullamento del sealing. Le tecnologie del sistema operativo, ad esempio BitLocker, possono utilizzare NitroTPM per sigillare una chiave di decrittografia dell'unità in modo che l'unità possa essere decrittografata solo quando il sistema operativo è stato avviato correttamente e si trova in un buono stato noto.

Per utilizzare NitroTPM, devi selezionare un'Amazon Machine Image (AMI) configurata per il supporto NitroTPM, quindi utilizzare l'AMI per avviare istanze basate sul sistema Nitro. AWS È possibile selezionare una delle AMI predefinite di Amazon o crearne una direttamente.

Costi

L'utilizzo di NitroTPM non prevede costi aggiuntivi. È previsto un pagamento solo per le risorse sottostanti utilizzate.

Argomenti

- Considerazioni

Considerazioni

Le seguenti considerazioni si applicano quando si utilizza NitroTPM:

- BitLocker i volumi crittografati con chiavi basate su NitroTPM possono essere utilizzati solo sull'istanza originale.
- Lo stato di NitroTPM non è incluso negli snapshot Amazon EBS.
- Lo stato di NitroTPM non è incluso nelle immagini VM Import/Export.
- Il supporto di NitroTPM viene abilitato specificando un valore di `v2.0` per il parametro `tpm-support` durante la creazione di un'AMI. Dopo l'avvio di un'istanza con l'AMI, non è possibile modificare gli attributi nell'istanza. Le istanze con NitroTPM non supportano l'API. ModifyInstanceAttribute
- Puoi creare un'AMI solo con NitroTPM configurato utilizzando l'RegisterImageAPI utilizzando AWS CLI e non con la console Amazon EC2.
- NitroTPM non è supportato su Outposts.
- NitroTPM non è supportato nelle zone locali o nelle zone Wavelength.

Prerequisiti per l'attivazione al lancio

Per avviare un'istanza con NitroTPM abilitato, devono essere soddisfatti i seguenti prerequisiti.

Istanze Linux

AMI

Richiede un'AMI con NitroTPM abilitato.

Al momento non esistono AMI Amazon Linux abilitate per NitroTPM. Per utilizzare un'AMI supportata, è necessario eseguire una serie di passaggi di configurazione sulla propria AMI Linux. Per ulteriori informazioni, consulta Creazione di un'AMI Linux per il supporto di NitroTPM.

Sistema operativo

L'AMI deve includere un sistema operativo con driver Command Response Buffer (CRB) TPM 2.0. La maggior parte dei sistemi operativi attuali, come Amazon Linux 2, contiene un driver TPM 2.0 CRB.

Modalità di avvio UEFI

NitroTPM richiede l'esecuzione di un'istanza in modalità di avvio UEFI, per cui è necessario che sia configurata l'AMI per la modalità di avvio UEFI. Per ulteriori informazioni, consulta UEFI Secure Boot.

Istanze Windows

AMI

Richiede un'AMI con NitroTPM abilitato.

Le seguenti AMI di Windows sono preconfigurate per abilitare NitroTPM e UEFI Secure Boot con chiavi Microsoft:

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise
- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

Attualmente l'importazione di Windows con NitroTPM tramite il comando import-image non è supportata.

Sistema operativo

L'AMI deve includere un sistema operativo con driver Command Response Buffer (CRB) TPM 2.0. La maggior parte dei sistemi operativi attuali, come TPM-Windows_Server-2022-English-Full-Base, contiene un driver TPM 2.0 CRB.

Modalità di avvio UEFI

NitroTPM richiede l'esecuzione di un'istanza in modalità di avvio UEFI, per cui è necessario che sia configurata l'AMI per la modalità di avvio UEFI. Per ulteriori informazioni, consulta UEFI Secure Boot.

Tipi di istanza

È necessario utilizzare uno dei seguenti tipi di istanze virtualizzate:

- Uso generale: M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7i, M7i-Flex, T3, T3a
- Elaborazione ottimizzata: C5, C5a, C5ad, C5d, C5n, C6a, C6i, C6id, C6in, C7a, C7i, C7i-flex
- Memoria ottimizzata: R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7i, R7iZ, U7i-12TB, U7in-16TB, U7in-24TB, U7in-32TB, X2idn, X2il dN, X2lezN, z1d
- Archiviazione ottimizzata: D3, D3en, I3en, I4i
- Elaborazione accelerata: G4dn, G5, G6, Gr6, Inf1, Inf2
- Elaborazione ad alte prestazioni: HPC6a, HPC6id

> **Note**
>
> Le istanze basate su Graviton, le istanze Xen, le istanze Mac e le istanze bare metal non sono supportate.

Creazione di un'AMI Linux per il supporto di NitroTPM

La configurazione dell'AMI Linux per il supporto di NitroTPM avviene durante la registrazione dell'AMI. Non è possibile configurare il supporto di NitroTPM in un secondo momento.

Per l'elenco delle AMI Windows preconfigurate per il supporto di NitroTPM, consulta. Prerequisiti per l'attivazione al lancio

Per registrare un'AMI Linux per il supporto di NitroTPM

1. Avvia un'istanza temporanea con l'AMI Linux richiesta.

2. Dopo che l'istanza ha raggiunto `running` lo stato, crea un'istantanea del volume principale dell'istanza.
3. Registra il nuovo AMI. Utilizzate il comando register-image. Per `--tpm-support`, specificare `v2.0`. Per `--boot-mode`, specificare `uefi`. E specifica una mappatura del dispositivo a blocchi per il volume principale utilizzando l'istantanea creata nel passaggio precedente.

```
aws ec2 register-image \
    --name my-image \
    --boot-mode uefi \
    --architecture x86_64 \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=snapshot_id} \
    --tpm-support v2.0
```

Output previsto

```
{
"ImageId": "ami-0123456789example"
}
```

4. Termina l'istanza temporanea che hai avviato nel passaggio 1, se non è più necessaria.

Verifica dell'abilitazione di un'AMI per NitroTPM

Puoi utilizzare `describe-images` o `describe-image-attributes` per verificare se un'AMI è abilitata per NitroTPM.

Per verificare se un'AMI è abilitata per NitroTPM utilizzando **`describe-images`**

Utilizza il comando describe-images e specifica l'ID dell'AMI.

```
aws ec2 describe-images --image-ids ami-0123456789example
```

Se NitroTPM è abilitato per l'AMI, `"TpmSupport": "v2.0"` viene visualizzato nell'output.

```
{
    "Images": [
        {
        ...
```

```
        "BootMode": "uefi",
        ...
        "TpmSupport": "v2.0"
        }
    ]
}
```

Per verificare se un'AMI è abilitata per NitroTPM utilizzando **`describe-image-attribute`**

Utilizzate il describe-image-attributecomando e specificate il `attribute` parametro con il `tpmSupport` valore.

> **Note**
>
> Per chiamare `describe-image-attribute` è necessario essere il proprietario dell'AMI.

```
aws ec2 describe-image-attribute \
    --region us-east-1 \
    --image-id ami-0123456789example \
    --attribute tpmSupport
```

Se NitroTPM è abilitato per l'AMI, il valore per `TpmSupport` è `"v2.0"`. Nota che `describe-image-attribute` restituisce solo gli attributi specificati nella richiesta.

```
{
    "ImageId": "ami-0123456789example",
    "TpmSupport": {
        "Value": "v2.0"
    }
}
```

Abilitazione o interruzione dell'utilizzo di NitroTPM su un'istanza

Quando avvii un'istanza da un'AMI con supporto di NitroTPM abilitato, l'istanza viene avviata con NitroTPM abilitato. È possibile configurare l'istanza per interrompere l'utilizzo di NitroTPM. È possibile verificare se un'istanza è abilitata per NitroTPM.

Argomenti

- Avvio di un'istanza con NitroTPM abilitato
- Interruzione dell'utilizzo di NitroTPM su un'istanza
- Verifica dell'accessibilità di NitroTPM all'interno dell'istanza

Avvio di un'istanza con NitroTPM abilitato

Quando viene avviata un'istanza con i prerequisiti, NitroTPM viene abilitato automaticamente sull'istanza. È possibile abilitare NitroTPM solo su un'istanza all'avvio. Per ulteriori informazioni sull'avvio di un'istanza MySQL, consulta Lancio dell'istanza.

Interruzione dell'utilizzo di NitroTPM su un'istanza

Dopo aver avviato un'istanza con NitroTPM abilitato, non è possibile disabilitare NitroTPM per l'istanza. Tuttavia, puoi configurare il sistema operativo affinché interrompa l'utilizzo di NitroTPM disabilitando il driver del dispositivo TPM 2.0 sull'istanza utilizzando i seguenti strumenti:

- [Istanze Linux] Usa tpm-tools.
- [Istanze Windows] Utilizza la console di gestione TPM, tpm.msc.

Per ulteriori informazioni sulla disabilitazione del driver del dispositivo, consulta la documentazione per il sistema operativo in uso.

Verifica dell'accessibilità di NitroTPM all'interno dell'istanza

Per verificare se un'istanza è abilitata per il supporto di NitroTPM utilizzando il AWS CLI

Utilizza il comando describe-instances AWS CLI e specifica l'ID istanza. Attualmente, la console Amazon EC2 non visualizza il campo `TpmSupport`.

```
aws ec2 describe-instances --instance-ids i-0123456789example
```

Se il supporto di NitroTPM è abilitato sull'istanza, `"TpmSupport": "v2.0"` viene visualizzato nell'output.

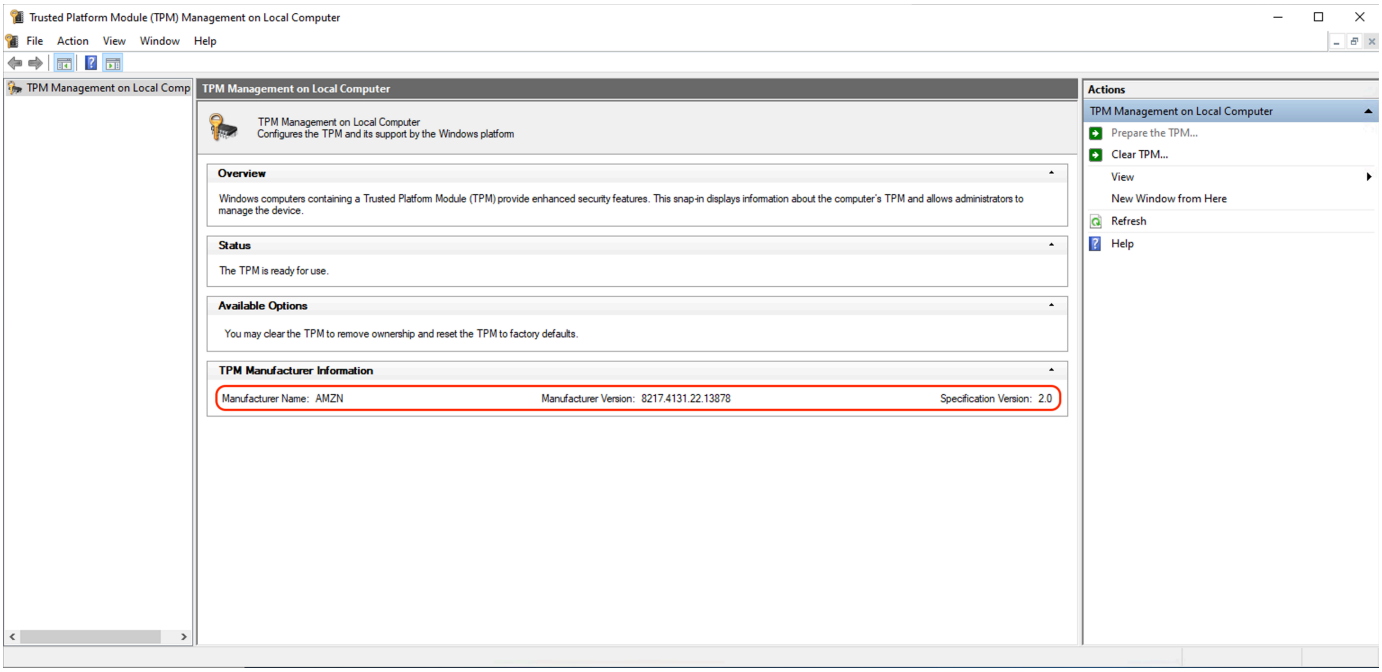
```
"Instances": {
              "InstanceId":"0123456789example",
              "InstanceType":"c5.large",
              ...
```

```
            "BootMode": "uefi",
            "TpmSupport": "v2.0"
            ...
            }
```

(Istanze Windows) Per verificare se NitroTPM è accessibile all'interno di un'istanza Windows di Amazon EC2

1. Connettiti all'istanza EC2 Windows.
2. Nell'istanza, esegui il programma tpm.msc.

   Viene visualizzata la finestra TPM Management on Local Computer (Gestione TPM sul computer locale).
3. Seleziona il campo TPM Manufacturer Information (Informazioni sul produttore TPM). Contiene il nome del produttore e la versione di NitroTPM sull'istanza.



Recupera la chiave di approvazione pubblica per un'istanza

È possibile recuperare in modo sicuro la chiave di approvazione pubblica per un'istanza in qualsiasi momento utilizzando il. AWS CLI

Per recuperare la chiave di approvazione pubblica per un'istanza

Utilizzate il comando get-instance-tpm-ek-pub AWS CLI .

Esempio 1

Il seguente comando di esempio ottiene, ad esempio, la chiave di approvazione `rsa-2048` pubblica in `tpmt` formato. `i-01234567890abcdef`

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format tpmt \
--key-type rsa-2048
```

Di seguito è riportato l'output di esempio.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "tpmt",
    "KeyType": "rsa-2048",
    "KeyValue": "AAEACwADALIAIINxl2dEhLEXAMPLEUal1yT9UtduBlILZPKh2hszFGmqAAYAgABDA
    EXAMPLEAAABAOiRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0LOLiYnEXAMPLERqApiFa/UhvEYqN4
    Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDthlS7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
    0S1ZtNuItMs+Yp4SO6aU28MT/JZkOKsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgVO0QTTJVGdDxh
    vxtXCOu9GYf0crbjEXAMPLEd4YTbWdDdgOKWF9fjzDytJSDhrLAOUctNzHPCd/92l5zEXAMPLEOIFA
    Ss50C0/802c17W2pMSVHvCCa9lYCiAfxH/vYKovAAE="
}
```

Esempio 2

Il seguente comando di esempio ottiene, ad esempio`i-01234567890abcdef`, la chiave di approvazione `rsa-2048` pubblica in `der` formato.

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format der \
--key-type rsa-2048
```

Di seguito è riportato l'output di esempio.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "der",
    "KeyType": "rsa-2048",
    "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DGZb4
```

```
    JcTFuUbykRR82bQs4uJifaKSOv5NGoEXAMPLEG8Rio3hnuMowP+6xuGxBoAHWAoDlGbO6FJrMdEXAMP
    LEnYUHvMO2GVLsc0a5ifl4buqcmd1FxqRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP8lmQ4qxch0x6
    tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNMlUZ0PGG/G1cI670Zh/RytuOdx9iEXAMPLEtZ0N2A4pYX
    1+PMPK0lIOGssA5Ry03Mc8J3/3aXnOD2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi
    8AAQIDAQAB"
}
```

Credential Guard per istanze Windows

Il sistema AWS Nitro supporta Credential Guard per le istanze Windows di Amazon Elastic Compute Cloud (Amazon EC2). Credential Guard è una funzionalità di sicurezza basata sulla virtualizzazione di Windows (VBS) che consente la creazione di ambienti isolati per proteggere le risorse di sicurezza, come le credenziali utente di Windows e l'applicazione dell'integrità del codice, oltre alle protezioni del kernel di Windows. Quando esegui istanze EC2 per Windows, Credential Guard utilizza il sistema AWS Nitro per proteggere le credenziali di accesso di Windows dall'estrazione dalla memoria del sistema operativo.

Indice

Prerequisiti

L'istanza Windows deve soddisfare i seguenti prerequisiti per utilizzare Credential Guard.

Amazon Machine Images (AMI)

L'AMI deve essere preconfigurata per abilitare NitroTPM e UEFI Secure Boot. Per ulteriori informazioni sulle AMI supportate, consulta. the section called “Prerequisiti”

Integrità della memoria

L'integrità della memoria, nota anche come Hypervisor-protected Code Integrity (HVCI) o Hypervisor enforced Code Integrity, non è supportata. Prima di attivare Credential Guard, devi

assicurarti che questa funzionalità sia disattivata. Per ulteriori informazioni, consulta Disabilitare l'integrità della memoria.

Tipi di istanza

I seguenti tipi di istanza supportano Credential Guard in tutte le dimensioni `C5C5d`, salvo diversa indicazione: `C5n` `C6iC6id`,`C6in`,,`C7i`,`C7i-flex`,`M5`,`M5d`,`M5dn`,`M5n`,`M5zn`,`M6i`,`M6id`,,`M6idn`,`M6in`,`M7i`,`M7i-flex`,`R5`,`R5b`,`R5d`,`R5dn`,`R5n`,,`R6i`,`R6id`, `R6idn` `R6inR7i`,`R7iz`. `T3`

> **Note**
>
> - Sebbene NitroTPM abbia alcuni tipi di istanza richiesti in comune, il tipo di istanza deve essere uno dei tipi di istanza precedenti per supportare Credential Guard.
> - Credential Guard non è supportato per:
>   - Istanze bare metal.
>   - I seguenti tipi di istanza: `C7i.48xlarge` `M7i.48xlarge`, e. `R7i.48xlarge`

Per ulteriori informazioni sui tipi di istanze, consulta la Amazon EC2 Instance Types Guide.

Avvia un'istanza supportata

Puoi utilizzare la console Amazon EC2 o AWS Command Line Interface (AWS CLI) per avviare un'istanza in grado di supportare Credential Guard. Avrai bisogno di un ID AMI compatibile per avviare l'istanza, che sia unico per ciascuna Regione AWS.

> **Tip**
>
> Puoi utilizzare il seguente link per scoprire e avviare istanze con AMI compatibili fornite da Amazon nella console Amazon EC2: https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Amazon EC2 console

Per avviare un'istanza tramite la console Amazon EC2

Segui i passaggi per avviare un'istanza, specificando un tipo di istanza supportato e un'AMI Windows preconfigurata.

AWS CLI

Per avviare un'istanza utilizzando AWS CLI

Utilizza il comando run-instances per avviare un'istanza utilizzando un tipo di istanza supportato e un'AMI Windows preconfigurata.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base \
    --instance-type c6i.large \
    --region us-east-1 \
    --subnet-id subnet-id
    --key-name key-name
```

PowerShell

Per avviare un'istanza utilizzando il AWS Tools for PowerShell

Utilizza il comando New-EC2Instance per avviare un'istanza utilizzando un tipo di istanza supportato e un'AMI Windows preconfigurata.

```
New-EC2Instance `
    -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base `
    -InstanceType c6i.large `
    -Region us-east-1 `
    -SubnetId subnet-id `
    -KeyName key-name
```

Disabilitare l'integrità della memoria

È possibile utilizzare l'Editor Criteri di gruppo locali per disabilitare l'integrità della memoria negli scenari supportati. Le seguenti indicazioni possono essere applicate per ogni impostazione di configurazione in Protezione dell'integrità del codice basata sulla virtualizzazione:

- Abilitata senza blocco: modifica l'impostazione impostandola su Disabilitato per disabilitare l'integrità della memoria.

- Abilitato con blocco UEFI: l'integrità della memoria è stata abilitata con il blocco UEFI. L'integrità della memoria non può essere disabilitata una volta abilitata con il blocco UEFI. Ti consigliamo di creare una nuova istanza con l'integrità della memoria disabilitata e di terminare l'istanza non supportata se non è in uso.

Per disabilitare l'integrità della memoria con l'Editor Criteri di gruppo locali

1. Connettiti alla tua istanza come account utente con privilegi di amministrazione utilizzando il protocollo RDP (Remote Desktop Protocol). Per ulteriori informazioni, consulta the section called “Connect alla tua istanza Windows utilizzando un client RDP”.
2. Apri il menu Start e cerca **`cmd`** per avviare un prompt dei comandi.
3. Esegui i comandi seguenti per aprire l'Editor Criteri di gruppo locali: `gpedit.msc`
4. Nell'Editor Criteri di gruppo locali, scegli Configurazione computer, Modelli amministrativi, Sistema, Protezione dispositivi.
5. Seleziona Attiva la sicurezza basata sulla virtualizzazione, quindi seleziona Modifica impostazione delle policy.
6. Apri il menu a discesa delle impostazioni per Protezione basata su virtualizzazione dell'integrità del codice, scegli Disabilitata, quindi scegli Applica.
7. Riavvia l'istanza per applicare le modifiche.

Attiva Credential Guard

Dopo aver avviato un'istanza Windows con un tipo di istanza supportato e un'AMI compatibile e aver confermato che l'integrità della memoria è disabilitata, puoi attivare Credential Guard.

> **Important**
>
> Per eseguire i seguenti passaggi di attivazione di Credential Guard sono necessari i seguenti privilegi di amministratore.

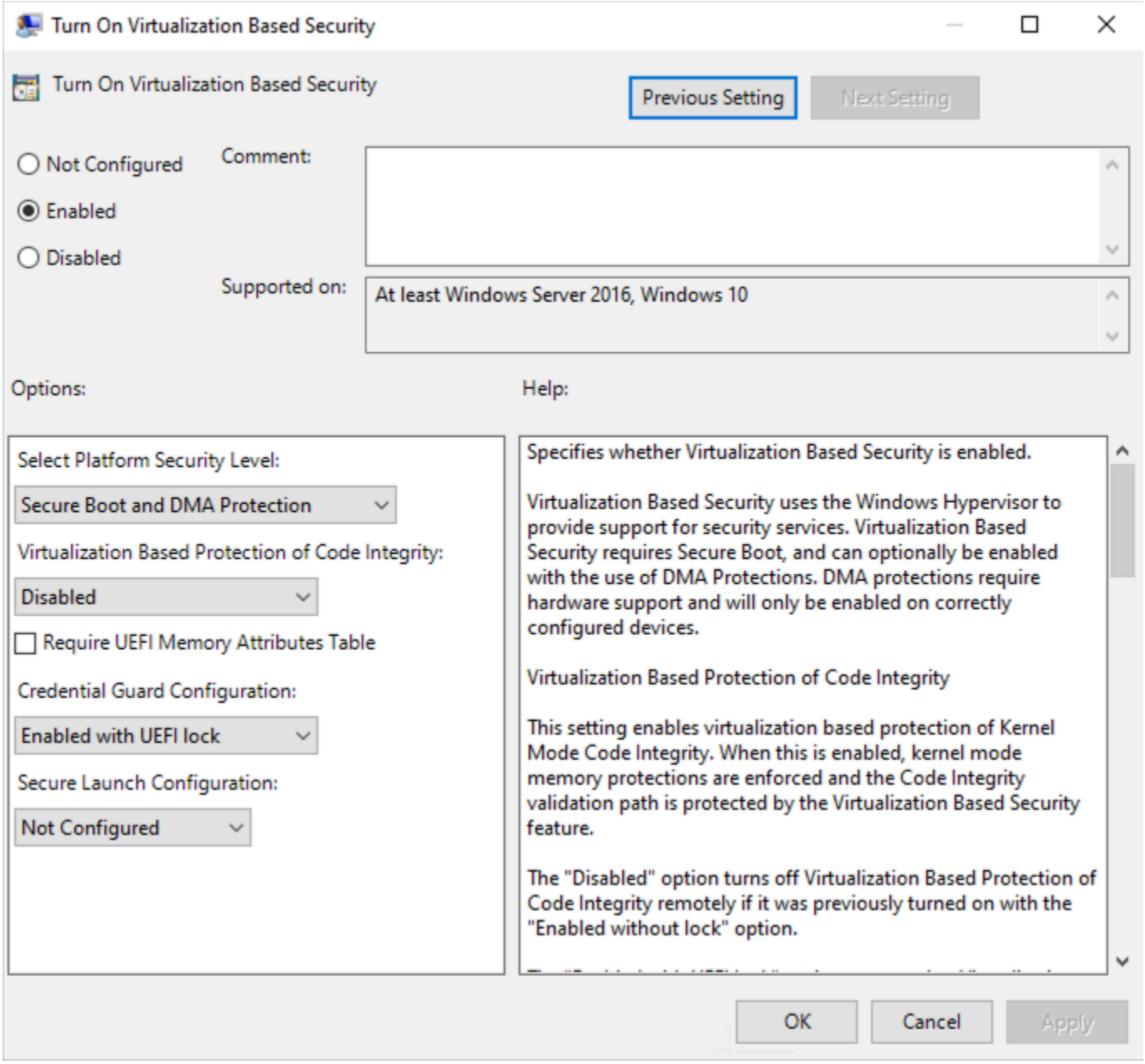
Per attivare Credential Guard

1. Connettiti alla tua istanza come account utente con privilegi di amministrazione utilizzando il protocollo RDP (Remote Desktop Protocol). Per ulteriori informazioni, consulta the section called “Connect alla tua istanza Windows utilizzando un client RDP”.

2. Apri il menu Start e cerca **`cmd`** per avviare un prompt dei comandi.
3. Esegui i comandi seguenti per aprire l'Editor Criteri di gruppo locali: `gpedit.msc`
4. Nell'Editor Criteri di gruppo locali, scegli Configurazione computer, Modelli amministrativi, Sistema, Protezione dispositivi.
5. Seleziona Attiva la sicurezza basata sulla virtualizzazione, quindi seleziona Modifica impostazione delle policy.
6. Scegli Abilitata nel menu Attiva la sicurezza basata sulla virtualizzazione.
7. Per Seleziona livello di sicurezza della piattaforma, scegli Secure Boot e protezione DMA.
8. Per la configurazione di Credential Guard, scegli Abilitato con blocco UEFI.

> **Note**
>
> Le restanti impostazioni delle policy non sono necessarie per abilitare Credential Guard e possono essere lasciate come Non configurate.

L'immagine seguente mostra le impostazioni VBS configurate come descritto in precedenza:



9. Riavvia l'istanza per applicare le impostazioni.

Verifica che Credential Guard sia in esecuzione

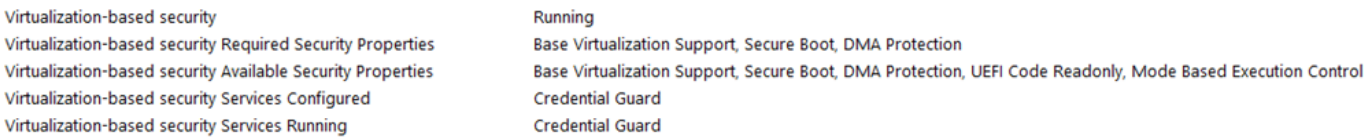
Puoi utilizzare lo strumento Microsoft System Information (`Msinfo32.exe`) per confermare che Credential Guard è in esecuzione.

> **Important**
>
> È necessario innanzitutto riavviare l'istanza per completare l'applicazione delle impostazioni delle policy richieste per abilitare Credential Guard.

Per verificare se Credential Guard è in esecuzione

1. Connettiti all'istanza utilizzando il protocollo RDP (Remote Desktop Protocol). Per ulteriori informazioni, consulta the section called “Connect alla tua istanza Windows utilizzando un client RDP”.
2. All'interno della sessione RDP dell'istanza, apri il menu Start e cerca **`cmd`** per avviare un prompt dei comandi.
3. Apri Informazioni sul sistema eseguendo il comando seguente: `msinfo32.exe`
4. Lo strumento Microsoft System Information elenca i dettagli per la configurazione VBS. Accanto a Servizi di sicurezza basati sulla virtualizzazione, verifica che Credential Guard sia visualizzato come In esecuzione.

   L'immagine seguente mostra che VBS è in esecuzione come descritto in precedenza:



Opzioni di archiviazione per le istanze Amazon EC2

Amazon EC2 ti offre opzioni di storage easy-to-use dei dati flessibili, convenienti e per le tue istanze. Ogni opzione è associata a un'esclusiva combinazione di prestazioni e durabilità. Queste opzioni di archiviazione possono essere utilizzate in modo indipendente oppure combinate, per adattarsi alle proprie esigenze.

Amazon EBS

Amazon EBS fornisce volumi di archiviazione durevoli a livello di blocchi, che possono essere collegati e scollegati dalle istanze. È possibile collegare più volumi EBS a una singola istanza. Un volume EBS persiste indipendentemente dalla vita di esecuzione dell'istanza associata. Puoi crittografare i tuoi volumi EBS. Per conservare una copia di backup dei dati, è possibile creare snapshot dai volumi EBS. Gli snapshot vengono archiviati in Amazon S3. È possibile creare un volume EBS da uno snapshot.

Instance store

L'archivio istanza offre un'archiviazione temporanea per le istanze a livello di blocchi. Il numero, la dimensione e il tipo di volumi dell'archivio dell'istanza sono determinati dal tipo e dalla dimensione dell'istanza. I dati contenuti in un volume di archivio istanze sono persistenti solo per la durata dell'istanza associata; se arresti, iberni o termini un'istanza, i dati nei volumi dell'archivio istanze andranno perduti.

Amazon EFS(Solo istanze Linux)

Amazon EFS fornisce l'archiviazione di file scalabile da utilizzare con Amazon EC2. Puoi creare un file system EFS e configurare le istanze per montare il file system. Puoi utilizzare un file system EFS come origine dati comune per carichi di lavoro e applicazioni in esecuzione su più istanze.

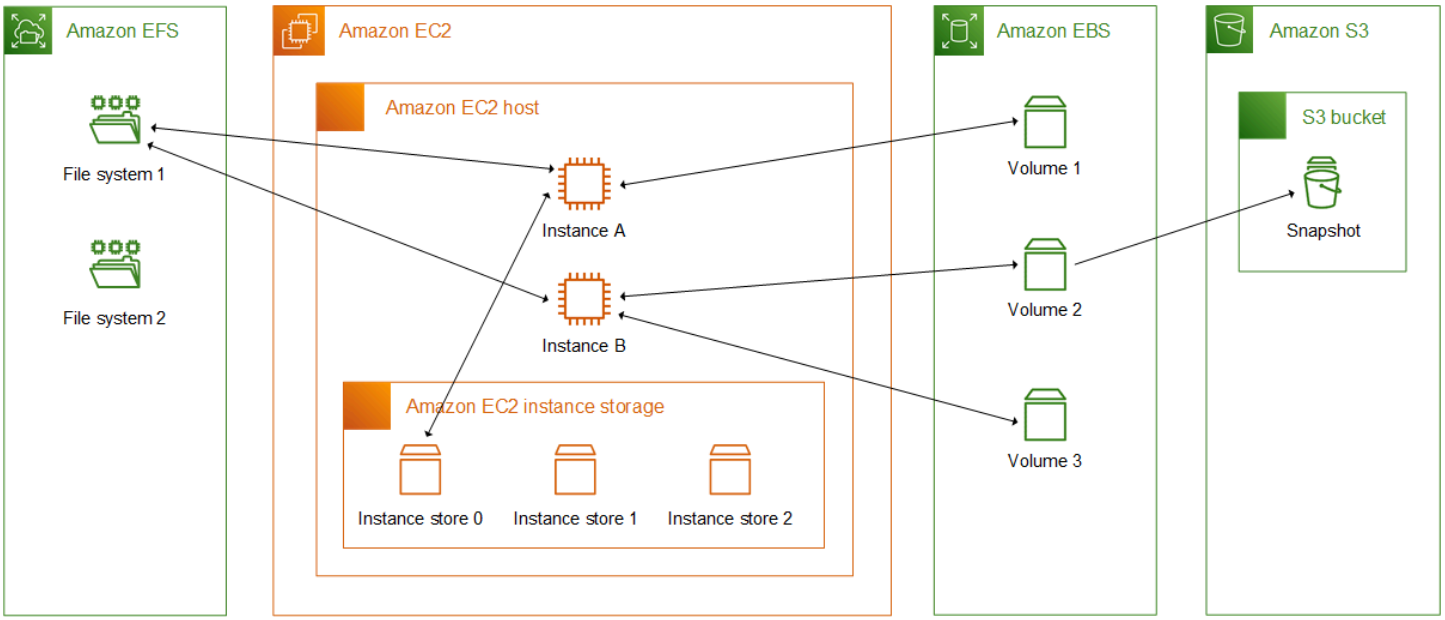
Amazon S3

Amazon S3 fornisce l'accesso a un'infrastruttura di archiviazione dei dati affidabile e conveniente. È progettata per semplificare le operazioni di calcolo a livello di Web, permettendoti di archiviare e recuperare una quantità qualsiasi di dati, in qualsiasi momento, dall'interno di Amazon EC2 o da qualsiasi posizione sul Web. Ad esempio, puoi usare Amazon S3 per archiviare le copie di backup dei dati e delle applicazioni. Amazon EC2 utilizza Amazon S3 per archiviare gli snapshot EBS e le AMI supportate da instance store.

Amazon FSx

Con Amazon FSx, puoi avviare, eseguire e scalare file system ricchi di funzionalità e ad alte prestazioni nel cloud. Amazon FSx è un servizio completamente gestito che supporta un'ampia gamma di carichi di lavoro. Puoi scegliere tra questi file system ampiamente utilizzati: Lustre, NetApp ONTAP, OpenZFS e Windows File Server.

L'illustrazione seguente mostra la relazione tra queste opzioni di archiviazione e la tua istanza.



Prezzi dello archiviazione

Apri AWS Prezzi, scorri fino a Prezzi dei prodotti e seleziona Archiviazione. AWS Scegli il prodotto di archiviazione per aprirne la pagina dei prezzi.

Usa Amazon EBS con Amazon EC2

Amazon Elastic Block Store (Amazon EBS) fornisce risorse di storage a blocchi scalabili e ad alte prestazioni che possono essere utilizzate con istanze Amazon Elastic Compute Cloud (Amazon EC2). Con Amazon EBS, puoi creare e gestire le seguenti risorse di storage a blocchi:

- Volumi Amazon EBS: si tratta di volumi di storage che colleghi alle istanze Amazon EC2. Dopo aver collegato un volume a un'istanza, puoi utilizzarlo nello stesso modo in cui utilizzeresti lo storage a blocchi. L'istanza può interagire con il volume proprio come farebbe con un'unità locale.
- Snapshot di Amazon EBS: si tratta point-in-time di backup di volumi Amazon EBS che persistono indipendentemente dal volume stesso. Puoi creare istantanee per eseguire il backup dei dati

sui tuoi volumi Amazon EBS. Puoi quindi ripristinare nuovi volumi da tali istantanee in qualsiasi momento.

Puoi creare e collegare volumi Amazon EBS a un'istanza durante il lancio e puoi creare e collegare volumi EBS a un'istanza in qualsiasi momento dopo il lancio. Inoltre, puoi creare istantanee da un volume in qualsiasi momento dopo la creazione.

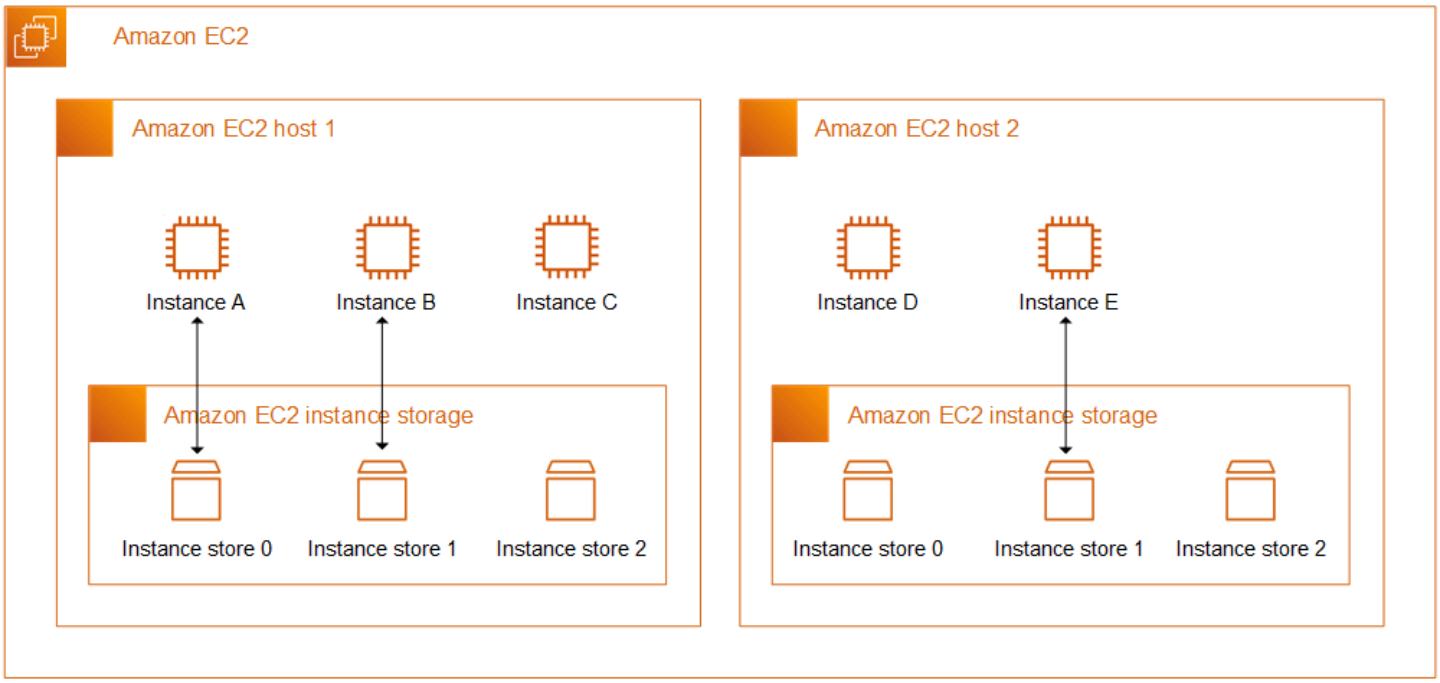
Per ulteriori informazioni sull'utilizzo di volumi e snapshot, consulta la Amazon EBS User Guide.

Instance store Amazon EC2

Un instance store fornisce un'archiviazione temporanea di livello per le istanze. L'archiviazione è collocata all'interno dei dischi fisicamente collegati al computer host. L'archivio dell'istanza è ideale per l'archiviazione temporanea di informazioni che cambiano frequentemente, quali buffer, cache, dati Scratch e altri contenuti temporanei. Inoltre, è possibile utilizzarlo per l'archiviazione di dati temporanei che vengono replicati in un parco istanze, come il pool per il sistema di bilanciamento del carico dei server Web.

Un instance store consta di uno o più volumi di instance store esposti come dispositivi a blocchi. La dimensione di un archivio dell'istanza e il numero dei dispositivi disponibili variano a seconda del tipo di istanza. Per ulteriori informazioni, consulta Volumi di archivio dell'istanza.

I dispositivi virtuali per li volumi di instance store sono `ephemeral[0-23]`. I tipi di instance che supportano un volume,e di instance store hanno `ephemeral0`. I tipi di istanze che supportano due o più volumi dell'archivio dell'istanza hanno `ephemeral0`, `ephemeral1` e così via.



Prezzi dell'archivio dell'istanza

I volumi di instance store sono inclusi ne costo dell'utilizzo dell'istanza.

Indice

Volume dell'archivio dell'istanza e durata dei dati

Il numero, la dimensione e il tipo di volumi dell'archivio dell'istanza sono determinati dal tipo e dalla dimensione dell'istanza. Per ulteriori informazioni, consulta Volumi di archivio dell'istanza.

I volumi dell'archivio dell'istanza vengono collegati solo all'avvio dell'istanza. Non puoi collegare un volume dell'archivio dell'istanza dopo l'avvio. Non puoi scollegare un volume dell'archivio dell'istanza da un'istanza e collegarlo a un'altra.

Un volume dell'archivio dell'istanza esiste solo durante la durata dell'istanza a cui è collegato. Non puoi configurare un volume dell'archivio dell'istanza in modo che persista oltre la durata dell'istanza associata.

I dati presenti in un volume dell'archivio dell'istanza persistono anche se l'istanza viene riavviata. Tuttavia, i dati non persistono se l'istanza viene arrestata, ibernata o terminata. Quando l'istanza viene arrestata, ibernata o terminata, ogni blocco del volume dell'archivio dell'istanza viene cancellato crittograficamente.

Pertanto, è consigliabile non fare affidamento sui volumi dell'archivio dell'istanza per dati preziosi e a lungo termine. Se devi mantenere i dati archiviati su un volume dell'archivio dell'istanza oltre la durata dell'istanza, devi copiarli manualmente su un'archiviazione più persistente, come un volume Amazon EBS, un bucket Amazon S3 o un file system Amazon EFS.

Alcuni eventi possono far sì che i dati non persistano per tutta la durata dell'istanza. La tabella seguente indica se i dati sui volumi dell'archivio dell'istanza vengono mantenuti durante eventi specifici, sia per le istanze virtualizzate che per quelle bare metal.

Evento	Cosa succede ai tuoi dati?
Eventi del ciclo di vita delle istanze avviate dall'utente	
L'istanza viene riavviata	I dati persistono
L'istanza viene interrotta	I dati non persistono
L'istanza è ibernata	I dati non persistono
L'istanza è terminata	I dati non persistono
Il tipo di istanza è cambiato	I dati non persistono*
Dall'istanza viene creata un'AMI supportata da EBS	I dati non persistono nell'AMI creata**
Dall'istanza viene creata un'AMI basata su storage di istanze (istanze Linux)	I dati persistono nel pacchetto AMI caricato su Amazon S3***
Eventi del sistema operativo avviati dall'utente	
Viene avviato un arresto	I dati non persistono †

Evento	Cosa succede ai tuoi dati?
Viene avviato un riavvio	I dati persistono
AWS eventi programmati	
Interruzione dell'istanza	I dati non persistono
Riavvio dell'istanza	I dati persistono
Riavvio del sistema	I dati persistono
Ritiro dell'istanza	I dati non persistono
Eventi non pianificati	
Ripristino automatico semplificato	I dati non persistono
CloudWatch ripristino basato sull'azione	I dati non persistono
Il disco sottostante si guasta	I dati sul disco guasto non persistono
Interruzione dell'alimentazione	I dati persistono al riavvio

* Se il nuovo tipo di istanza supporta l'archivio dell'istanza, l'istanza ottiene il numero di volumi di quest'ultimo supportati dal nuovo tipo di istanza, ma i dati non vengono trasferiti all'istanza nuova. Se il nuovo tipo di istanza non supporta l'archivio dell'istanze, l'istanza non ottiene i volumi di quest'ultimo.

** I dati non sono inclusi nell'AMI supportata da EBS e non sono inclusi nei volumi dell'archivio dell'istanza collegati alle istanze avviate da tale AMI.

*** I dati sono inclusi nel bundle AMI che viene caricato su Amazon S3. Quando avvii un'istanza da tale AMI, l'istanza ottiene i volumi dell'archivio dell'istanza raggruppati nell'AMI con i dati che contenevano al momento della creazione di quest'ultima.

† La protezione dalla terminazione e dall'arresto delle istanze non le protegge dagli arresti o dalle terminazioni dovute alle interruzioni avviate tramite il sistema operativo dell'istanza. I dati archiviati nei volumi dell'archivio dell'istanza non persistono sia negli eventi di arresto che in quelli di terminazione dell'istanza.

Volumi di archivio dell'istanza

Il numero, la dimensione e il tipo di volumi dell'archivio dell'istanza sono determinati dal tipo e dalla dimensione dell'istanza. Alcuni tipi di istanze, come M6, C6 e R6, non supportano i volumi dell'archivio dell'istanza, mentre altri tipi come M5d, C6gd e R6gd, supportano tali volumi. Non puoi collegare più volumi dell'archivio dell'istanza a un'istanza di quelli supportati dal tipo di istanza. Per i tipi di istanze che supportano i volumi dell'archivio dell'istanza, il numero e le dimensioni di questi ultimi variano in base alla dimensione dell'istanza. Ad esempio, `m5d.large` supporta 1 volume dell'archivio dell'istanza da 75 GB, mentre `m5d.24xlarge` supporta 4 volumi da 900 GB.

Per i tipi di istanze con volumi dell'archivio dell'istanza NVMe, tutti i volumi dell'archivio dell'istanza supportati vengono automaticamente collegati all'istanza all'avvio. Per i tipi di istanza con volumi di instance store non NVMe, come C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, è necessario specificare manualmente le mappature dei dispositivi a blocchi per i volumi di instance store che si desidera collegare all'avvio. Quindi, dopo l'avvio dell'istanza, devi formattare e montare i volumi dell'archivio dell'istanza collegati prima di poterli utilizzare. Non puoi collegare un volume dell'archivio dell'istanza dopo l'avvio dell'istanza.

Alcuni tipi di istanze utilizzano supporti SSD (Solid State Drive) basati su NVMe o SATA, mentre altri utilizzano supporti HDD (Hard Disk Drive) basati su SATA. Gli SSD offrono prestazioni I/O casuali molto elevate con latenza bassissima, ma non occorre che i dati persistano alla terminazione dell'istanza, oppure puoi sfruttare le architetture con tolleranza ai guasti. Per ulteriori informazioni, consulta Volumi di instance store SSD.

I dati sui volumi dell'archivio istanza NVMe e alcuni volumi dell'archivio istanza HDD sono crittografati a riposo. Per ulteriori informazioni, consulta Protezione dei dati in Amazon EC2.

Volumi di archivio dell'istanza disponibili

La Amazon EC2 Instance Types Guide fornisce le ottimizzazioni della quantità, delle dimensioni, del tipo e delle prestazioni dei volumi di instance store disponibili su ogni tipo di istanza supportato. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Specifiche dell'Instance Store: scopo generale
- Specifiche dell'Instance Store: ottimizzate per il calcolo
- Specifiche dell'Instance Store: memoria ottimizzata
- Specifiche dell'Instance Store: archiviazione ottimizzata
- Specifiche dell'Instance Store: elaborazione accelerata

- Specifiche dell'Instance Store: elaborazione ad alte prestazioni
- Specifiche dell'Instance Store: generazione precedente

Per recuperare le informazioni sul volume dell'Instance Store utilizzando AWS CLI

È possibile utilizzare il describe-instance-types AWS CLI comando per visualizzare informazioni su un tipo di istanza, ad esempio i volumi dell'Instance Store. Nell'esempio seguente viene visualizzata la dimensione totale dell'archiviazione dell'istanza per tutte le istanze R5 con volumi dell'instance store.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5*" "Name=instance-storage-
supported,Values=true" \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Output di esempio

```
---------------------------
|  DescribeInstanceTypes  |
+----------------+--------+
|  r5ad.24xlarge |  3600  |
|  r5ad.12xlarge |  1800  |
|  r5dn.8xlarge  |  1200  |
|  r5ad.8xlarge  |  1200  |
|  r5ad.large    |  75    |
|  r5d.4xlarge   |  600   |
   . . .
|  r5dn.2xlarge  |  300   |
|  r5d.12xlarge  |  1800  |
+----------------+--------+
```

Nell'esempio seguente vengono visualizzati i dettagli completi dell'archiviazione dell'istanza per il tipo di istanza specificato.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5d.4xlarge" \
    --query "InstanceTypes[].InstanceStorageInfo"
```

L'output di esempio mostra che questo tipo di istanza dispone di due volumi SSD NVMe da 300 GB, per un totale di 600 GB di archiviazione dell'istanza.

```
[
    {
        "TotalSizeInGB": 600,
        "Disks": [
            {
                "SizeInGB": 300,
                "Count": 2,
                "Type": "ssd"
            }
        ],
        "NvmeSupport": "required"
    }
]
```

Aggiunta di un volume di instance store all'istanza EC2

Per i tipi di istanze con volumi dell'archivio dell'istanza NVMe, tutti i volumi dell'archivio dell'istanza supportati vengono automaticamente collegati all'istanza all'avvio. Questi volumi vengono enumerati automaticamente e viene assegnato loro un nome di dispositivo all'avvio dell'istanza.

Per i tipi di istanza con volumi di instance store non NVMe, come C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, è necessario specificare manualmente le mappature dei dispositivi a blocchi per i volumi di instance store che si desidera collegare all'avvio. Le mappature dei dispositivi a blocchi possono essere specificate nella richiesta di avvio dell'istanza o nell'AMI utilizzata per avviare l'istanza. La mappatura dei dispositivi a blocchi comprende il nome del dispositivo e il volume sul quale si esegue la mappatura. Per ulteriori informazioni, consulta Mappatura dei dispositivi a blocchi

> **Important**
>
> I volumi dell'archivio dell'istanza possono essere collegati a un'istanza solo al momento dell'avvio della stessa. Non è collegare un volume di instance store dopo averlo avviato.

Dopo aver avviato l'istanza, è necessario assicurarsi che i volumi instance store per l'istanza siano stati formattati e montati, prima di poterla utilizzare. Il volume root di un'istanza supportata da instance store viene montato automaticamente.

Considerazione dei volumi root

Una mappatura dei dispositivi a blocchi specifica sempre il volume root per l'istanza. Il volume root viene sempre montato automaticamente.

Istanze Linux: il volume root è un volume Amazon EBS o un volume di instance store. Per le istanze con un volume di instance store per il volume root, la dimensione di questo volume varia a seconda dell'AMI, ma la dimensione massima è di 10 GB. Per ulteriori informazioni, consulta Archiviazione del dispositivo root.

Istanze Windows: il volume root deve essere un volume Amazon EBS. L'Instance Store non è supportato per il volume root.

Indice

Aggiunta di volumi di instance store a un'AMI

È possibile creare un'AMI con una mappatura dei dispositivi a blocchi che include volumi di instance store.

Se avvii un'istanza con un tipo di istanza che supporta i volumi dell'archivio dell'istanza non NVMe utilizzando un'AMI che specifica questi ultimi nelle proprie mappature dei dispositivi a blocchi, l'istanza include tali volumi dell'archivio dell'istanza. Se il numero di mappature dei dispositivi a blocchi del volume dell'archivio dell'istanza nell'AMI supera il numero disponibile di volumi dell'archivio dell'istanza per un'istanza, le mappature aggiuntive vengono ignorate.

Se avvii un'istanza che supporta i volumi dell'archivio dell'istanza NVMe utilizzando un'AMI che specifica le mappature dei dispositivi a blocchi del volume dell'archivio dell'istanza, tali mappature vengono ignorate. Le istanze che supportano i volumi dell'archivio dell'istanza NVMe ottengono tutti i volumi dell'archivio dell'istanza supportati, indipendentemente dalle mappature dei dispositivi a blocchi specificate nella richiesta di avvio dell'istanza e nell'AMI.

Considerazioni

- Per le istanze M3, specificare i volumi di archivio istanze nella mappatura dei dispositivi a blocchi dell'istanza, non nell'AMI. Amazon EC2 può ignorare le mappature dei dispositivi a blocchi del volume dell'archivio dell'istanza nell'AMI.

- All'avvio di un'istanza è possibile omettere i volumi instance store non-NVMe specificati nella mappatura dei dispositivi a blocchi AMI e i volumi instance store.

Console

Aggiungere volumi di instance store a un'AMI supportata da un Amazon EBS utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza.
3. Scegliere Actions (Operazioni), Image and templates (Immagine e modelli), Create image (Crea immagine).
4. Nella pagina Create image (Crea immagine), immettere un nome e una descrizione significativi per l'immagine.
5. Per ogni volume di instance store da aggiungere, selezionare Add volume (Aggiungi nuovo volume), selezionare un volume di instance store in Volume type (Tipo di volume) e selezionare il nome del dispositivo in Device (Dispositivo). Per ulteriori informazioni, consulta Nomi dei dispositivi sulle istanze Amazon EC2. Il numero di volumi di instance store disponibili dipende dal tipo di istanza. Per le istanze con volumi di instance store NVMe, la mappature del dispositivo per questi volumi dipende dall'ordine secondo cui il sistema operativo enumera i volumi.
6. Scegliere Create Image (Crea immagine).

AWS CLI

Aggiungere volumi di instance store a un'AMI tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- create-image o register-image (AWS CLI)
- New-EC2Imagee Register-EC2Image(AWS Tools for Windows PowerShell)

Aggiunta di volumi dell'archivio dell'istanza non NVMe a un'istanza

Quando avvi un'istanza che supporta i volumi dell'archivio dell'istanza non NVMe devi specificare le mappature dei dispositivi a blocchi per i volumi dell'archivio dell'istanza da collegare. Le mappature

dei dispositivi a blocchi devono essere specificate nella richiesta di avvio dell'istanza o nell'AMI utilizzata per avviare l'istanza.

Se l'AMI include mappature dei dispositivi a blocchi per i volumi dell'archivio dell'istanza, non devi specificare le mappature dei dispositivi a blocchi nella richiesta di avvio dell'istanza, a meno che non siano necessari più volumi dell'archivio dell'istanza rispetto a quelli inclusi nell'AMI.

Se l'AMI non include le mappature dei dispositivi a blocchi per i volumi dell'archivio dell'istanza, devi specificare le mappature dei dispositivi a blocchi nella richiesta di avvio dell'istanza.

Considerazioni

- Per le istanze M3, potresti ricevere i volumi di instance store nella mappatura dei dispositivi a blocchi dell'istanza, anche se non li si specifica.

Per specificare le mappature dei dispositivi a blocchi nella richiesta di avvio dell'istanza, utilizza uno dei seguenti metodi.

Amazon EC2 console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di controllo, selezionare Avvia istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona l'AMI da utilizzare.
4. Nella sezione Configura storage, il campo Volumi Instance store elenca i volumi dell'archivio dell'istanza che possono essere collegati all'istanza. Il numero di volumi di instance store disponibili dipende dal tipo di istanza.
5. Per ogni volume dell'archivio dell'istanza da allegare, in Nome dispositivo, seleziona il nome del dispositivo da utilizzare.
6. Configura le impostazioni dell'istanza rimanenti in base alle esigenze, quindi scegli Avvia istanza.

Command line

Puoi utilizzare uno dei seguenti comandi con l'opzione corrispondente.

- `--block-device-mappings` con run-instances (AWS CLI)

- `-BlockDeviceMapping`con New-EC2Instance(AWS Tools for Windows PowerShell)

Rendere i volumi di instance store disponibili per l'istanza

Dopo aver avviato un'istanza con volumi di instance store collegati, è necessario montare i volumi prima di potervi accedere.

Istanze Linux

Puoi formattare i volumi con il file system di tua scelta dopo aver avviato l'istanza.

È possibile visualizzare e montare i volumi dell'Instance Store come descritto nella procedura seguente.

Rendere un volume archivio istanza disponibile per Linux

1. Connettiti all'istanza tramite un client SSH. Per ulteriori informazioni, consulta Connessione all'istanza di Linux.
2. Utilizza il comando `df -h` per visualizzare i volumi formattati e montati.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   72K  3.8G   1% /dev
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Utilizza `lsblk` per visualizzare tutti i volumi che sono stati mappati al lancio, ma che non sono stati formattati e montati.

```
$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. Per formattare e montare un volume instance store che è stato solamente mappato, segui il procedimento elencato di seguito:

   a. Crea un file di sistema sul dispositivo utilizzando il comando `mkfs`.

```
$ sudo mkfs -t xfs /dev/nvme1n1
```

b. Crea una directory all'interno della quale montare il dispositivo utilizzando il comando `mkdir`.

```
$ sudo mkdir /data
```

c. Monta il dispositivo nella directory appena creata utilizzando il comando `mount`.

```
$ sudo mount /dev/nvme1n1 /data
```

Istanze Windows

Per le istanze Windows, riformattiamo i volumi di instance store con il file di sistema NTFS.

È possibile visualizzare i volumi dell'Instance Store utilizzando Gestione disco di Windows. Per ulteriori informazioni, consulta Elencare i dischi utilizzando Gestione disco.

Per montare manualmente un volume di instance store

1. Scegliere Inizia, immettere Gestione computer, quindi premere Invio.
2. Nel pannello a sinistra, scegliere Gestione disco.
3. Se viene richiesto di inizializzare il volume, scegliere il volume da inizializzare, selezionare il tipo di partizione richiesta in base al caso d'uso, quindi scegliere OK.
4. Nell'elenco dei volumi fare clic con il tasto destro del mouse sul volume da montare e quindi scegliere Nuovo volume semplice.
5. Nella procedura guidata scegliere Avanti.
6. Nella schermata Specifica dimensioni volume scegliere Avanti per utilizzare la dimensione massima del volume. In alternativa, scegliere una dimensione del volume compresa tra lo spazio minimo e quello massimo su disco.
7. Nella schermata Assegna lettera di unità o percorso eseguire una delle operazioni seguenti e scegliere Avanti.

   - Per montare il volume con una lettera di unità, scegliere Assegna la lettera di unità seguente quindi scegliere la lettera di unità da utilizzare.

- Per montare il volume come cartella, scegliere Monta nella seguente cartella NTFS vuota e quindi scegliere Sfoglia per creare o selezionare la cartella da utilizzare.
- Per montare il volume senza una lettera o un percorso di unità, scegliere Non assegnare una lettera di unità o un percorso di unità.

8. Nella schermata Formatta partizione specificare se formattare o meno il volume. Se si sceglie di formattare il volume, scegliere il file system e le dimensioni dell'unità richieste e specificare un'etichetta del volume.
9. Scegliere Avanti, Fine.

Per istruzioni su come montare automaticamente un volume collegato dopo il riavvio, consulta Montare automaticamente un volume collegato dopo il riavvio nella Guida per l'utente di Amazon EBS.

Volumi di instance store SSD

Come avviene per gli altri volumi di instance store, è necessario eseguire la mappatura dei volumi di instance store dell'istanza all'avvio di essa. I dati su un volume di instance di un SSF persistono solo durante la vita dell'istanza associata. Per ulteriori informazioni, consulta Aggiunta di un volume di instance store all'istanza EC2.

Volumi SSD NVMe

Alcune istanze offrono volumi di instance store SSD di tipo NVMe (Non-Volatile Memory Express). Per ulteriori informazioni sul tipo di volume di instance store supportato da ciascun tipo di istanza, consulta Volumi di archivio dell'istanza.

I dati sull'archivio istanza NVMe sono crittografati utilizzando un codice di cifratura a blocchi XTS-AES-256 implementato tramite un modulo hardware sull'istanza. Le chiavi crittografiche sono generate utilizzando il modulo hardware e sono univoche per ciascun dispositivo di archivio NVMe. Quando l'istanza viene arrestata o terminata, tutte le chiavi crittografiche vengono distrutte e non possono essere ripristinate. Non è possibile disattivare questa cifratura e non è possibile fornire una propria chiave crittografica.

Istanze Linux

Per accedere ai volumi NVMe, è necessario installare i driver NVMe. Le seguenti AMI soddisfano questo requisito:

- AL2023
- Amazon Linux 2
- AMI Amazon Linux 2018.03 e versioni successive
- Ubuntu 14.04 o versioni successive con kernel `linux-aws`

> **Note**
>
> AWS I tipi di istanza basati su Graviton richiedono Ubuntu 18.04 o versione successiva con kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 o versioni successive
- SUSE Linux Enterprise Server 12 SP2 o versioni successive
- CentOS 7.4.1708 o versioni successive
- FreeBSD 11.1 o versioni successive
- Debian GNU/Linux 9 o versioni successive

- Bottlerocket

Dopo avere effettuato la connessione all'istanza, è possibile elencare i dispositivi NVMe utilizzando il comando lspci. Quello elencato di seguito è l'output di esempio di un'istanza `i3.8xlarge` che supporta quattro dispositivi NVMe.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Se si sta utilizzando un sistema operativo supportato, ma non compaiono i dispositivi NVME, verifica che il modulo NVMe sia caricato utilizzando il seguente comando.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

```
$ lsmod | grep nvme
nvme           48813  0
```

- Ubuntu 18

```
$ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
s/nvme/host/nvme-core.ko
kernel/drivers/nvme/host/nvme.ko
kernel/drivers/nvmem/nvmem_core.ko
```

I volumi NVMe sono in linea con le specificazioni NVMe 1.0e. È possibile utilizzare i comandi NVMe con i volumi NVMe. Con Amazon Linux, è possibile installare il pacchetto `nvme-cli` dal repository utilizzando il comando yum install. Con altre versioni supportate di Linux, è possibile scaricare il pacchetto `nvme-cli`, se non è disponibile nell'immagine.

Istanze Windows

Le AMI AWS Windows più recenti per i seguenti sistemi operativi contengono i driver AWS NVMe utilizzati per interagire con i volumi di archiviazione delle istanze SSD esposti come dispositivi a blocchi NVMe per prestazioni migliori:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Ad avvenuta connessione all'istanza, è possibile verificare la visualizzazione dei volumi NVMe da Gestione Disco. Nella barra delle applicazioni, aprire il menu contestuale (pulsante destro del mouse) per il logo Windows e scegliere Disk Management (Gestione disco).

Le AMI AWS Windows fornite da Amazon includono il driver AWS NVMe. Se non utilizzi le AMI AWS Windows più recenti, puoi installare il driver NVMe corrente. AWS

Volumi SSD non-NVMe

Le seguenti istanze supportano volumi di instance store che utilizzano SSD non NVMe per offrire prestazioni I/O casuali elevate: C3, I2, M3, R3 e X1. Per ulteriori informazioni sui volumi di instance store supportati da ogni tipo di istanza, consulta Volumi di archivio dell'istanza.

Prestazioni I/O dei volumi dell'archivio dell'istanza basati su SSD

Mano a mano che riempi i volumi instance store basati su SSD della tua istanza, il numero di IOPS di scrittura che puoi raggiungere diminuisce. Questa riduzione è dovuta al lavoro aggiuntivo che il controller SSD deve svolgere per individuare spazio disponibile, riscrivere i dati esistenti e cancellare lo spazio inutilizzato in modo che possa essere riscritto. Questo processo di garbage collection produce un'amplificazione della scrittura interna dell'SSD, espressa come il rapporto delle operazioni di scrittura dell'SSD e le operazioni di scrittura dell'utente. La riduzione delle prestazioni è ancora maggiore se le operazioni di scrittura non sono in multipli di 4.096 byte o non sono allineate con il limite di 4.096 byte. Se scrivi una quantità inferiore di byte o di byte non allineati, il controller SSD deve leggere i dati circostanti e archiviare il risultato in una nuova posizione. Questo modello comporta un'amplificazione della scrittura notevolmente maggiore, una latenza maggiore e una riduzione drastica delle prestazioni di I/O.

I controller SSD possono utilizzare svariate strategie per ridurre l'impatto dell'amplificazione della scrittura. Una di queste strategie è di riservare spazio nell'archiviazione dell'istanza SSD in modo che il controller possa gestire più efficacemente lo spazio disponibile per le operazioni di scrittura. Si tratta dell'over-provisioning. I volumi di instance store basati su SSD forniti a un'istanza non dispongono di spazio riservato per l'over-provisioning. Per ridurre l'amplificazione in scrittura, si consiglia di lasciare il 10 percento del volume non partizionato in modo che il controller SSD possa utilizzarlo per l'over-provisioning. In questo modo, l'archiviazione che si può utilizzare diminuisce, ma aumentano le prestazioni anche se il disco è prossimo alla capacità completa.

Ad esempio, archivia volumi che supportano TRIM, puoi utilizzare il comando TRIM per notificare al controller SSD ogni volta che non hai più bisogno dei dati che hai scritto. Il controller avrà così più spazio libero, l'amplificazione della scrittura potrà ridursi e le prestazioni aumentare. Per ulteriori informazioni, consulta Supporto TRIM per i volumi di instance store.

Supporto TRIM per i volumi di instance store

Alcuni tipi di istanza supportano i volumi SSD con TRIM. Per ulteriori informazioni, consulta Volumi di archivio dell'istanza.

> **Note**
>
> (Solo istanze Windows) Le istanze che eseguono Windows Server 2012 R2 supportano TRIM a partire dalla versione 7.3.0 di PV Driver. AWS Le istanze che eseguono versioni precedenti di Windows Server non supportano il TRIM.

Volumi di instance store che supportano TRIM vengono tagliati prima di essere allocati per l'istanza. Questi volumi non sono formattati con un file system in cui un'istanza viene avviata; pertanto è necessario formattarli prima che essi possano essere montati e utilizzati. Per accedere più rapidamente a questi volumi. è consigliabile saltare l'operazione TRIM al momento della formattazione.

(Istanze Windows) Per disabilitare temporaneamente il supporto TRIM durante la formattazione iniziale, utilizzate il comando. `fsutil behavior set DisableDeleteNotify 1` Al termine della formattazione, riattiva il supporto TRIM utilizzando. `fsutil behavior set DisableDeleteNotify 0`

Con i volumi di instance store che supportano TRIM, è possibile usare il comando TRIM per notificare al controller SSD che i dati scritti non sono più necessari. Il controller avrà così più spazio libero, l'amplificazione della scrittura potrà ridursi e le prestazioni aumentare. Nelle istanze Linux, utilizzate il `fstrim` comando per abilitare il TRIM periodico. Nelle istanze Windows, usa il `fsutil behavior set DisableDeleteNotify 0` comando per assicurarti che il supporto TRIM sia abilitato durante il normale funzionamento.

Volumi di scambio di istanze (Instance Store) per istanze Linux

> **Note**
>
> Questo argomento si applica solo alle istanze Linux.

È possibile utilizzare lo spazio di swapping su Linux quando un sistema richiede più memoria di quanta ne è stata allocata fisicamente. Quando lo spazio di swapping è abilitato, i sistemi possono scambiare le pagine di memoria utilizzate meno frequentemente dalla memoria fisica allo spazio di swapping (che sia una partizione dedicata o file di cambio all'interno di un file system esistente) e liberare lo spazio necessario alle pagine di memoria che richiedono un accesso ad alta velocità.

> **Note**
>
> L'utilizzo dello spazio di scambio il pagine di memoria non è veloce o efficiente come quello della RAM. Se il carico di lavoro sta effettuando regolarmente il paging della memoria nello spazio di scambio, è consigliabile pensare di migrare a un tipo di istanza di dimensioni maggiori e con più RAM. Per ulteriori informazioni, consulta Cambiare il tipo di istanza.

I tipi di istanza `c1.medium` e `m1.small` dispongono di una quantità limitata di memoria fisica con cui lavorare e all'avvio viene loro assegnato un volume di swap da 900 MiB che funge da memoria virtuale per le AMIs Linux. Sebbene il kernel di Linux veda questo spazio di swap come una partizione sul dispositivo di root, in realtà è un volume di instance store separato, indipendentemente dal tipo di dispositivo di root.

Amazon Linux abilita e utilizza automaticamente questo spazio di swap, ma la tua AMI potrebbe richiedere qualche passaggio ulteriore per il riconoscimento e l'utilizzo di questo spazio di swap. Per vedere se l'istanza sta utilizzando dello spazio di scambio, è possibile utilizzare il comando swapon -s.

```
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

L'istanza sopra elencata dispone di un volume di scambio di 900 MiB allegato e abilitato. Se non si visualizza un volume di scambio elencato con questo comando, potrebbe essere necessaria l'abilitazione dello spazio di scambio per il dispositivo. Controllare i dischi disponibili utilizzando il comando lsblk.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk
```

In questo caso, il volume di swap `xvda3` è disponibile per l'istanza, ma non è abilitato (notare che il campo `MOUNTPOINT` è vuoto). È possibile abilitare il volume di swap con il comando swapon.

> **Note**
>
> È necessario inserire come prefisso `/dev/` al nome del dispositivo elencato da lsblk. Il dispositivo può avere un nome diverso, come `sda3`, `sde3`, oppure `xvde3`. Utilizza il nome del dispositivo per il sistema nel comando di seguito.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

Adesso lo spazio di scambio dovrebbe comparire nell'output lsblk e swapon -s.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

È inoltre necessario modificare i file `/etc/fstab` perché questo spazio di swapping sia abilitato automaticamente ad ogni avvio del sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Aggiungere la seguente linea al file `/etc/fstab` (utilizzando il nome del dispositivo di scambio per il sistema):

```
/dev/xvda3       none    swap    sw  0       0
```

Utilizzare un volume di instance store a uno spazio di swap

È possibile utilizzare un qualsiasi volume di instance store come spazio di swapping. Ad esempio il tipo di istanza `m3.medium` include un volume di instance store volume SSD di 4GB adatto allo spazio di swapping. Se il volume di instance store dovesse essere di dimensioni maggiori (ad esempio 350 GB), potrebbe essere necessaria la partizione del volume in partizioni di swap più piccole di 4-8GB e il resto assegnarlo a un volume di dati.

> **Note**
>
> Questa procedura si applica solamente a tipo di istanze che supportano l'archiviazione di istanze. Per una lista di tipi di istanze supportate, consulta Volumi di archivio dell'istanza.

1. Vengono elencati i dispositivi a blocchi collegati all'istanza per ottenere il nome del dispositivo per il volume di instance store.

```
[ec2-user ~]$ lsblk -p
NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
/dev/xvda1 202:1    0   8G  0 disk /
```

   In questo esempio, il volume di instance store è `/dev/xvdb`. Poiché si tratta di un'istanza Amazon Linux il volume di instance store viene formattato e montato su `/media/ephemeral0`; questa operazione non viene eseguita automaticamente su tutti i sistemi operativi Linux.

2. (Facoltativo) se il volume di instance store è stato montato (presenta `MOUNTPOINT` nell'output di comando lsblk), smontarlo utilizzando il seguente comando.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Impostare un'area di swapping Linux sul dispositivo con il comando mkswap.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Abilita la quantità di spazio di swapping.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Verifica che il nuovo spazio di swapping sia utilizzato.

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
/dev/xvdb                               partition 4188668 0 -1
```

6. Modifica i file `/etc/fstab` così che questo spazio di swapping venga automaticamente abilitato ad ogni avvio di sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Se il file `/etc/fstab` dovesse avere una voce per `/dev/xvdb` (o per `/dev/sdb`) cambiala per farla corrispondere a quella riportata nella riga seguente: se non dovesse avere alcuna voce per questo dispositivo, aggiungi la riga seguente al file `/etc/fstab` (utilizzando il nome del dispositivo di swap per il sistema):

```
/dev/xvdb       none    swap    sw  0       0
```

> **Important**
>
> I dati del volume di instance store vengono persi all'interruzione o all'ibernazione di un'istanza; inclusa la formattazione dello spazio di swapping creata su Step 3. Se si arresta e riavvia un'istanza che è stata configurata per l'utilizzo di uno spazio di swapping di un'instance store, è necessario ripetere Step 1 da Step 5 sul nuovo volume di instance store.

Ottimizza le prestazioni del disco, ad esempio archivia i volumi su istanze Linux

> **Note**
>
> Questo argomento si applica solo alle istanze Linux.

A causa della modalità di visualizzazione dei dischi virtuali di Amazon EC2, la prima scrittura di una qualsiasi destinazione su alcuni volumi di instance store viene eseguita più lentamente delle scritture successive. Per la maggior parte delle applicazioni, è accettabile ammortizzare questo costo nel ciclo di vita dell'istanza. Tuttavia, se fosse necessaria una prestazione elevata del disco, è consigliabile inizializzare i drive scrivendo una volta sulla posizione di ogni disco prima di utilizzarlo in produzione.

> **Note**
>
> Alcuni tipi di istanze con supporti Solid State Drive (SSD) e TRIM forniscono le massime prestazioni all'avvio, senza l'inizializzazione. Per ulteriori informazioni sui volumi di instance store per ogni tipo di istanza, consulta Volumi di archivio dell'istanza.

Se è necessaria maggiore flessibilità nella latenza o nel throughput. è consigliabile utilizzare Amazon EBS.

Per inizializzare i volumi di instance store, utilizza il seguenti comandi dd a seconda dello store da inizializzare (ad esempio, `/dev/sdb` o `/dev/nvme1n1`).

> **Note**
>
> Assicurati di aver smontato il drive prima di eseguire questo comando.
> L'inizializzazione potrebbe richiedere tempi lunghi (circa 8 ore per un'istanza extra large).

Per inizializzare i volumi di instance store, utilizza i seguenti comandi nei tipi di istanze `m1.large`, `m1.xlarge`, `c1.xlarge`, `m2.xlarge`, `m2.2xlarge` e `m2.4xlarge`:

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Per eseguire l'inizializzazione su tutti i volumi di instance store contemporaneamente,, utilizza i seguenti comandi:

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

La configurazione dei drive per RAID li inizializza scrivendo su ogni posizione del disco. Durante la configurazione di un software basato sul RAID, assicurati di modificare la velocità minima di ricostruzione:

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Archiviazione dei file

L'archiviazione di file nel cloud è un metodo di archiviazione di file nel cloud che permette a server e applicazioni di accedere ai dati tramite file system condivisi. Tale caratteristica di compatibilità rende questo servizio ideale per i carichi di lavoro che fanno affidamento su file system condivisi e fornisce integrazione semplificata per non dover modificare il codice.

Esistono molte soluzioni di storage di file, che vanno da un file server a nodo singolo su un'istanza di calcolo che utilizza lo storage a blocchi come base senza scalabilità o poche ridondanze per proteggere i dati, a una soluzione in do-it-yourself cluster, a una soluzione completamente gestita. Il seguente contenuto presenta alcuni dei servizi di storage forniti da AWS per l'uso con le istanze Amazon EC2.

Indice

Utilizzo di Amazon S3 con Amazon EC2

Amazon Simple Storage Service (Amazon S3) è un servizio di archiviazione di oggetti che offre scalabilità, disponibilità dei dati, sicurezza e prestazioni tra le migliori del settore. Puoi usare Amazon S3 per archiviare e recuperare qualsiasi quantità di dati per un'ampia gamma di casi d'uso, come data lake, siti Web, backup e analisi dei big data, da un'istanza Amazon EC2 o da qualsiasi luogo su Internet. Per ulteriori informazioni, consulta Cos'è Amazon S3?

Gli oggetti sono le entità fondamentali archiviate in Amazon S3 e Ogni oggetto archiviato in Amazon S3 è contenuto in un bucket. I bucket organizzano lo spazio dei nomi di Amazon S3 al livello più alto e definiscono l'account responsabile dell'archiviazione. I bucket Amazon S3 sono simili ai nomi di dominio Internet. Gli oggetti archiviati nei bucket hanno un valore di chiave univoco e vengono recuperati tramite un URL. Ad esempio, se un oggetto con un valore di chiave `/photos/mygarden.jpg` è archiviato nel bucket `DOC-EXAMPLE-BUCKET1`, è indirizzabile tramite l'URL `https://DOC-EXAMPLE-BUCKET1.s3.amazonaws.com/photos/mygarden.jpg`. Per ulteriori informazioni, consulta Come funziona Amazon S3.

Esempi di utilizzo

Dati i vantaggi di Amazon S3 per quanto riguarda le funzionalità di archiviazione, è possibile decidere di utilizzare questo servizio per archiviare file e set di dati da usare con le istanze EC2. Ci sono diversi modi per trasferire i dati da e ad Amazon S3 alle istanze. Oltre agli esempi trattati di seguito, è disponibile un'ampia gamma di strumenti che puoi utilizzare per accedere ai di in Amazon S3 dal computer o dall'istanza in uso. Alcuni dei più comuni sono trattati nei forum AWS .

Se disponi delle autorizzazioni necessarie, puoi copiare un file in o da Amazon S3 e nella tua istanza uno dei seguenti metodi.

GET or wget (Linux)

> **Note**
>
> Questo metodo funziona solo per oggetti pubblici. Se l'oggetto non è pubblico, riceverai un messaggio `ERROR 403: Forbidden`. Se ricevi questo errore, devi utilizzare la console Amazon S3, l' AWS API AWS CLI, l' AWS SDK o AWS Tools for Windows PowerShell, e devi disporre delle autorizzazioni richieste. Per ulteriori informazioni, consulta Identity and Access Management in Amazon S3 e Download di un oggetto nella Guida per l'utente di Amazon S3.

La utility wget è un client HTTP e FTP che ti permette di scaricare oggetti pubblici da Amazon S3. Viene installata per impostazione di default in Amazon Linux e nella maggior parte delle altre distribuzione ed è disponibile per il download su Windows. Per scaricare un oggetto Amazon S3, utilizza il seguente comando, ricordando di sostituire l'URL dell'oggetto da scaricare.

```
[ec2-user ~]$ wget https://my_bucket.s3.amazonaws.com/path-to-file
```

AWS Tools for Windows PowerShell (Windows)

Le istanze Windows sfruttano un browser grafico che puoi utilizzare per accedere direttamente alla console Amazon S3. Tuttavia, per motivi di scripting, gli utenti di Windows possono anche utilizzare gli AWS Tools for Windows PowerShell per spostare oggetti da e verso Amazon S3.

Utilizza il comando seguente per copiare un oggetto Amazon S3 nell'istanza Windows.

```
PS C:\> Copy-S3Object -BucketName my_bucket -Key path-to-file -
LocalFile my_copied_file.ext
```

AWS CLI (Linux and Windows)

Il AWS Command Line Interface (AWS CLI) è uno strumento unificato per gestire i tuoi servizi. AWS AWS CLI permette agli utenti di eseguire l'autenticazione e scaricare oggetti con restrizioni da Amazon S3, nonché di caricare oggetti. Per ulteriori informazioni, ad esempio su come installare e configurare gli strumenti, consulta la pagina dei dettagli di AWS Command Line Interface.

L'output del comando aws s3 cp è simile a comando Unix cp seguente. Puoi copiare file da Amazon S3 alla tua istanza, copiare file dalla tua istanza in Amazon S3 e copiare file da posizioni Amazon S3 diverse.

Utilizza il comando seguente per copiare un oggetto da Amazon S3 alla tua istanza.

```
aws s3 cp s3://my_bucket/my_folder/my_file.ext my_copied_file.ext
```

Utilizza il comando seguente per copiare di nuovo un oggetto dalla tua istanza ad Amazon S3.

```
aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

Il comando aws s3 sync può sincronizzare un intero bucket Amazon S3 in una posizione di directory locale. Questo può essere utile per scaricare un set di dati e conservare la copia locale up-to-date con il set remoto. Se disponi delle autorizzazioni adeguate per il bucket Amazon S3, puoi eseguire il push del backup della directory locale nel cloud quando sei pronto invertendo le posizioni di origine e di destinazione nel comando.

Utilizza il comando seguente per scaricare un intero bucket Amazon S3 in una directory locale sull'istanza.

```
aws s3 sync s3://remote_S3_bucket local_directory
```

Amazon S3 API

Gli sviluppatori possono utilizzare un'API per accedere ai dati in Amazon S3. Puoi utilizzare questa API per sviluppare la tua applicazione e integrarla con altre API e SDK. Per ulteriori

informazioni, consulta Esempi di codice per Amazon S3 con AWS SDK nella Amazon S3 User Guide.

Usa Amazon EFS con istanze Linux

> **Note**
>
> Amazon EFS non è supportato sulle istanze Windows.

Amazon EFS fornisce lo storage di file scalabile da utilizzare con Amazon EC2. Puoi utilizzare un file system EFS come origine dati comune per carichi di lavoro e applicazioni in esecuzione su più istanze. Per ulteriori informazioni, consulta la pagina dei dettagli del prodotto Amazon Elastic File System.

Questo tutorial mostra come creare e collegare un file system Amazon EFS utilizzando la procedura guidata Amazon EFS Quick Create durante l'avvio dell'istanza. Per un tutorial su come creare un file system utilizzando la console Amazon EFS, consulta Nozioni di base su Amazon Elastic File System nella Guida per l'utente di Amazon Elastic File System.

> **Note**
>
> Quando si crea un file system EFS utilizzando la creazione rapida di EFS, il file system viene creato con le seguenti impostazioni consigliate per il servizio:
>
> - Backup automatici abilitati.
> - Monta le destinazioni in ogni sottorete predefinita nel VPC selezionato.
> - Modalità prestazionale General Purpose.
> - Modalità Bursting Throughput.
> - La crittografia dei dati inattivi è abilitata utilizzando la chiave predefinita per Amazon EFS (`aws/elasticfilesystem`).
> - Gestione del ciclo di vita di Amazon EFS abilitata con una policy di 30 giorni.

Attività

- Creazione di un file system EFS utilizzando la creazione rapida di Amazon EFS

- Testare il file system EFS
- Eliminare il file system EFS

Creazione di un file system EFS utilizzando la creazione rapida di Amazon EFS

Puoi creare un file system EFS e montarlo sull'istanza al momento dell'avvio utilizzando la funzionalità di creazione rapida di Amazon EFS della procedura guidata dell'istanza di Amazon EC2.

Per creare un file system EFS utilizzando la creazione rapida di Amazon EFS

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).
3. (Facoltativo) In Name and tags (Nome e tag), per Name (Nome) inserisci un nome descrittivo per identificare l'istanza.
4. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), scegli un sistema operativo Linux, quindi per Amazon Machine Image (AMI) (Amazon Machine Image [AMI]), seleziona un'AMI Linux.
5. In Instance type (Tipo di istanza), per Instance type (Tipo di istanza), seleziona un tipo di istanza o mantieni il valore predefinito.
6. In Key pair (login) (Coppia di chiavi (login), per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o creane una nuova.
7. In Network settings (Impostazioni di rete), scegli Edit (Modifica) a destra, quindi seleziona una sottorete in Subnet (Sottorete).

   > **Note**
   >
   > Devi selezionare una sottorete prima di poter aggiungere un file system EFS.

8. In Configure storage (Configura lo storage), scegli Edit (Modifica) in basso a destra, quindi esegui le operazioni riportate di seguito:

   a. Per File system, assicurati che EFS sia selezionato, quindi scegli Crea nuovo file system condiviso.

   b. Per Nome del file system, inserisci un nome per il file system Amazon EFS, quindi scegli Crea file system.

c. Per Mount point, specifica un punto di montaggio personalizzato o mantieni quello predefinito.

d. Per consentire l'accesso al file system, seleziona Automatically create and attach security groups (Crea e allega automaticamente i gruppi di sicurezza). Selezionando questa casella di controllo, i seguenti gruppi di sicurezza verranno creati e collegati automaticamente all'istanza e alle destinazioni di montaggio del file system:

- Gruppo di sicurezza dell'istanza: include una regola in uscita che consente il traffico sulla porta NFS 2049, ma non include regole in entrata.
- Gruppo di sicurezza delle destinazioni di montaggio del file system: include una regola in entrata che consente il traffico sulla porta NFS 2049 dal gruppo di sicurezza dell'istanza (descritta sopra) e una regola in uscita che consente il traffico sulla porta NFS 2049.

> **Note**
>
> In alternativa, è possibile creare e collegare manualmente i gruppi di sicurezza. Se vuoi creare e allegare manualmente i gruppi di sicurezza, deseleziona Automatically create and attach the required security groups (Crea e allega automaticamente i gruppi di sicurezza richiesti).

e. Per montare automaticamente il file system condiviso all'avvio dell'istanza, seleziona Automatically mount shared file system by attaching required user data script (Monta automaticamente il file system condiviso allegando lo script di dati utente richiesto). Per visualizzare i dati utente generati automaticamente, espandi Advanced details (Dettagli avanzati) e scorri verso il basso fino a User data (Dati utente).

> **Note**
>
> Se sono stati aggiunti dati utente prima di selezionare questa casella di controllo, i dati utente originali vengono sovrascritti dai dati utente generati automaticamente.

9. Configura qualsiasi altra impostazione di configurazione dell'istanza in base alle esigenze.
10. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.

Testare il file system EFS

Puoi connetterti all'istanza e verificare che il file system sia montato sulla directory specificata (ad esempio /mnt/efs).

Per verificare che il file system sia montato

1. Connettiti alla tua istanza. Per ulteriori informazioni, consulta Connessione all'istanza di Linux.
2. Dalla finestra del terminale dell'istanza esegui il comando df -T per verificare che il file system EFS sia montato.

```
$ df -T
Filesystem     Type              1K-blocks    Used          Available Use% Mounted
 on
/dev/xvda1     ext4                8123812 1949800            6073764  25% /
devtmpfs       devtmpfs            4078468      56            4078412   1% /dev
tmpfs          tmpfs               4089312       0            4089312   0% /dev/shm
efs-dns        nfs4       9007199254740992       0   9007199254740992   0% /mnt/efs
```

   Il nome del file system, mostrato nell'output di esempio come *efs-dns*, ha il seguente formato:

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. (Facoltativo) Crea un file nel file system dall'istanza, quindi verifica di poter visualizzare il file da un'altra istanza.

   a. Dall'istanza, esegui il comando seguente per creare il file.

```
$ sudo touch /mnt/efs/test-file.txt
```

   b. Dall'altra istanza, esegui il comando seguente per visualizzare il file.

```
$ ls /mnt/efs
test-file.txt
```

Eliminare il file system EFS

Se il file system non è più necessario, puoi eliminarlo.

Per eliminare il file system

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Selezionare il file system da eliminare.
3. Scegliere Actions (Operazioni), Delete file system (Elimina file system).
4. Quando viene richiesta la conferma, immettere l'ID del file system e scegliere Delete file system (Elimina file system).

Utilizzo di Amazon FSx con Amazon EC2

La famiglia di servizi Amazon FSx semplifica l'avvio, l'esecuzione e il dimensionamento dell'archivio condiviso basato su file system commerciali e open source più diffusi. Puoi utilizzare la nuova procedura guidata di avvio dell'istanza per collegare automaticamente i seguenti tipi di file system Amazon FSx alle istanze Amazon EC2 al momento dell'avvio:

- Amazon FSx for NetApp ONTAP offre uno storage condiviso completamente gestito nel AWS cloud con le popolari funzionalità di accesso e gestione dei dati di ONTAP. NetApp
- Amazon FSx for OpenZFS offre un archivio condiviso a costi contenuti completamente gestito con il popolare file system OpenZFS.

> **Note**
>
> - Questa funzionalità è disponibile solo nella procedura guidata di avvio dell'istanza. Per ulteriori informazioni, consulta Avvio di un'istanza tramite la procedura guidata di avvio istanza.
> - I file system Amazon FSx per Windows File Server e Amazon FSx per Lustre non possono essere montati all'avvio . È necessario montare questi file system manualmente dopo l'avvio.

È possibile scegliere di montare un file system esistente creato in precedenza oppure creare un nuovo file system da montare su un'istanza all'avvio.

Argomenti

- Script di dati utente e gruppi di sicurezza

- Montaggio di un file system Amazon FSx all'avvio

Script di dati utente e gruppi di sicurezza

Quando si monta un file system Amazon FSx su un'istanza utilizzando la procedura guidata di avvio dell'istanza, è possibile scegliere se creare e allegare automaticamente i gruppi di sicurezza necessari per abilitare l'accesso al file system e se includere automaticamente gli script di dati utente necessari per montare il file system e renderlo disponibile per l'uso.

Argomenti

- Gruppi di sicurezza
- Script di dati utente

Gruppi di sicurezza

Se si sceglie di creare automaticamente i gruppi di sicurezza necessari per abilitare l'accesso al file system, la procedura guidata di avvio dell'istanza crea e allega due gruppi di protezione: un gruppo di sicurezza è collegato all'istanza e l'altro è collegato al file system. Per ulteriori informazioni sui requisiti del gruppo di sicurezza, consulta FSx for ONTAP file system access control with Amazon VPC (Controllo degli accessi al file system FSx for ONTAP con Amazon VPC) e FSx for OpenZFS file system access control with Amazon VPC (Controllo degli accessi al file system FSx for OpenZFS).

Aggiungiamo il tag `Name=instance-sg-`*`1`* al gruppo di sicurezza creato e collegato all'istanza. Il valore del tag viene incrementato automaticamente ogni volta che la procedura guidata di avvio dell'istanza crea un nuovo gruppo di sicurezza per i file system Amazon FSx.

Il gruppo di sicurezza include le regole in uscita indicate di seguito, ma nessuna regola in entrata.

Regole in uscita

Tipo di protocollo	Numero della porta	Destinazione
UDP	111	*gruppo di sicurezza del file system*
UDP	20001-2003	*gruppo di sicurezza del file system*
UDP	4049	*gruppo di sicurezza del file system*
UDP	2049	*gruppo di sicurezza del file system*

Tipo di protocollo	Numero della porta	Destinazione
UDP	635	*gruppo di sicurezza del file system*
UDP	4045 - 4046	*gruppo di sicurezza del file system*
TCP	4049	*gruppo di sicurezza del file system*
TCP	635	*gruppo di sicurezza del file system*
TCP	2049	*gruppo di sicurezza del file system*
TCP	111	*gruppo di sicurezza del file system*
TCP	4045 - 4046	*gruppo di sicurezza del file system*
TCP	20001 - 2003	*gruppo di sicurezza del file system*
Tutti	Tutti	*gruppo di sicurezza del file system*

Il gruppo di sicurezza creato e collegato al file system è contrassegnato con il tag `Name=fsx-sg-`*1*. Il valore del tag viene incrementato automaticamente ogni volta che la procedura guidata di avvio dell'istanza crea un nuovo gruppo di sicurezza per i file system Amazon FSx.

Il gruppo di sicurezza include le regole seguenti.

Regole in entrata

Tipo di protocollo	Numero della porta	Origine
UDP	2049	*gruppo di sicurezza dell'istanza*
UDP	20001 - 2003	*gruppo di sicurezza dell'istanza*
UDP	4049	*gruppo di sicurezza dell'istanza*
UDP	111	*gruppo di sicurezza dell'istanza*
UDP	635	*gruppo di sicurezza dell'istanza*
UDP	4045 - 4046	*gruppo di sicurezza dell'istanza*

Tipo di protocollo	Numero della porta	Origine
TCP	4045 - 4046	*gruppo di sicurezza dell'istanza*
TCP	635	*gruppo di sicurezza dell'istanza*
TCP	2049	*gruppo di sicurezza dell'istanza*
TCP	4049	*gruppo di sicurezza dell'istanza*
TCP	20001 - 2003	*gruppo di sicurezza dell'istanza*
TCP	111	*gruppo di sicurezza dell'istanza*

Regole in uscita

Tipo di protocollo	Numero della porta	Destinazione
Tutti	Tutti	0.0.0.0/0

Script di dati utente

Se si sceglie di allegare automaticamente gli script di dati utente, la procedura guidata di avvio dell'istanza aggiunge i seguenti dati utente all'istanza. Questo script installa i pacchetti necessari, monta il file system e aggiorna le impostazioni dell'istanza in modo che il file system venga rimontato automaticamente ogni volta che l'istanza viene riavviata.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
```

```
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Montaggio di un file system Amazon FSx all'avvio

Come montare un file system Amazon FSx nuovo o esistente all'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instance (Avvia istanza) per aprire la procedura guidata di avvio dell'istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona l'AMI da utilizzare.
4. Nella sezione Instance type (Tipo di istanza), seleziona il tipo di istanza.
5. Nella sezione Key pair (Coppia di chiavi), seleziona una coppia di chiavi esistenti o creane una nuova.
6. Nella sezione Network settings (Impostazioni di rete), procedi nel seguente modo:

   a. Scegli Modifica.

   b. Se vuoi montare un file system esistente, in Subnet (Sottorete), scegli la sottorete preferita del file system. Ti consigliamo di avviare l'istanza nella stessa zona di disponibilità della sottorete preferita del file system per ottimizzare le prestazioni.

      Se vuoi creare un nuovo file system da montare su un'istanza, in Subnet (Sottorete), scegli la sottorete in cui avviare l'istanza.

      > **Important**
      >
      > È necessario selezionare una sottorete per abilitare la funzionalità Amazon FSx nella nuova procedura guidata di avvio dell'istanza. Se non si seleziona una sottorete, non sarà possibile montare un file system esistente o crearne uno nuovo.

7. Nella sezione Storage (Archiviazione), procedi come segue:

a. Configura i volumi secondo necessità.

b. Espandi la sezione File systems (File system) e seleziona FSx.

c. Scegli Add shared file system (Aggiungi file system condiviso).

d. In File system, seleziona il file system da montare.

> **Note**
>
> L'elenco mostra tutti i file system Amazon FSx for NetApp ONTAP e Amazon FSx for OpenZFS presenti nel tuo account nella regione selezionata.

e. Per creare e collegare automaticamente i gruppi di sicurezza necessari per abilitare l'accesso al file system, seleziona Automatically create and attach security groups (Crea e collega automaticamente gruppi di sicurezza). Se preferisci creare manualmente i gruppi di sicurezza, deseleziona la casella di controllo. Per ulteriori informazioni, consulta Gruppi di sicurezza.

f. Per collegare automaticamente gli script di dati utente necessari per montare il file system, seleziona Automatically mount shared file system by attaching required user data script (Monta automaticamente il file system condiviso collegando lo script di dati utente richiesto). Se preferisci fornire manualmente gli script di dati utente, deseleziona la casella di controllo. Per ulteriori informazioni, consulta Script di dati utente.

8. Nella sezione Advanced (Avanzate), configura le impostazioni aggiuntive dell'istanza in base alle esigenze.

9. Scegli Avvia.

Usa Amazon File Cache con Amazon EC2

Amazon File Cache è una cache ad alta velocità completamente gestita AWS che viene utilizzata per elaborare i dati dei file, indipendentemente da dove sono archiviati. Amazon File Cache funge da posizione di archiviazione temporanea ad alte prestazioni per i dati archiviati in file system, AWS file system e bucket Amazon Simple Storage Service (Amazon S3) locali. Puoi utilizzare questa funzionalità per rendere disponibili set di dati dispersi per applicazioni basate su file con una vista unificata e a velocità elevate, AWS con latenze inferiori al millisecondo e throughput elevato. Per ulteriori informazioni, consulta Cos'è Amazon File Cache? .

Puoi accedere alla cache dalle tue istanze Amazon EC2 utilizzando il client Lustre open source. Le istanze Amazon EC2 possono accedere alla cache da altre zone di disponibilità all'interno dello stesso Amazon Virtual Private Cloud (Amazon VPC), a condizione che la rete consenta l'accesso tra sottoreti all'interno del VPC. Dopo aver montato la cache, puoi lavorare con i file e le directory in essa contenuti come quando usi un file system locale.

Per iniziare, consulta la sezione Guida introduttiva ad Amazon File Cache.

Limiti dei volumi delle istanze

Il numero massimo di volumi Amazon EBS che puoi collegare a un'istanza dipende dal tipo di istanza e dalle dimensioni dell'istanza. Durante la definizione del numero di volumi da aggiungere all'istanza, consigliamo di valutare se si necessita di maggiore larghezza di banda I/O o di maggiore capacità di archiviazione.

Larghezza di banda e capacità

Per casi d'uso di larghezza di banda coerenti e prevedibili, utilizza istanze ottimizzate per Amazon EBS con volumi SSD General Purpose o volumi SSD Provisioned IOPS. Per ottimizzare le prestazioni, segui le linee guida riportate nella sezione per individuare la corrispondenza corretta tra l'IOPS per il quale hai eseguito il provisioning per i volumi in uso e la larghezza di banda delle istanze.

Per le configurazioni RAID, molti amministratori hanno riscontrato una riduzione delle prestazioni a causa di un aumento dell'overhead di I/O con array contenenti più di 8 volumi. Esegui il test delle prestazioni di un'applicazione specifica e apporta le modifiche richieste, se necessario.

Argomenti

- Limiti di volume per le istanze basate sul sistema Nitro
- Limiti di volume per le istanze basate su XEN

Limiti di volume per le istanze basate sul sistema Nitro

Argomenti

- Limite di volume dedicato ad Amazon EBS
- Limite di volume Amazon EBS condiviso

Limite di volume dedicato ad Amazon EBS

I seguenti tipi di istanze Nitro hanno un limite di volume Amazon EBS dedicato che varia a seconda delle dimensioni dell'istanza. Il limite non è condiviso con altri allegati del dispositivo. In altre parole, puoi collegare un numero qualsiasi di volumi Amazon EBS fino al limite di allegati al volume, indipendentemente dal numero di dispositivi collegati, come i volumi di archiviazione delle istanze NVMe e le interfacce di rete.

- Uso generale: M7a, M7i, M7i-Flex
- Elaborazione ottimizzata: C7a, C7i, C7i-Flex
- Memoria ottimizzata: R7a, R7i, R7iZ, R8g, U7i
- Calcolo accelerato: G6, Gr6

Per questi tipi di istanze che supportano limiti di volume dedicati, i limiti di volume dipendono dalla dimensione dell'istanza. La tabella seguente mostra il numero di unità normalizzate per ogni dimensione di istanza database.

Dimensioni istanza	Limite di volumi
`medium | large | xlarge | 2xlarge | 4xlarge | 8xlarge | 12xlarge`	32
`16xlarge`	48
`24xlarge`	64
`32xlarge`	88
`48xlarge`	128
`metal-16xl | metal-24xl`	39
`metal-32xl | metal-48xl`	79

Limite di volume Amazon EBS condiviso

Tutti gli altri tipi di istanze Nitro (non elencati inLimite di volume dedicato ad Amazon EBS) hanno un limite di volume allegato condiviso tra volumi Amazon EBS, interfacce di rete e volumi di instance store NVMe. Puoi collegare un numero qualsiasi di volumi Amazon EBS fino a quel limite, meno il numero di interfacce di rete collegate e i volumi di archiviazione delle istanze NVMe. Tieni presente che ogni istanza deve avere almeno un'interfaccia di rete e che i volumi di archiviazione delle istanze NVMe vengono collegati automaticamente all'avvio.

La maggior parte di queste istanze supporta un massimo di 28 allegati. Ad esempio, se non disponi di alcun allegato all'interfaccia di rete aggiuntiva su un'istanza `m5.xlarge`, puoi collegare fino a 27 volumi EBS (limite di volumi 28 - 1 interfaccia di rete). Se si dispone di due interfacce di rete aggiuntive su un`m5.xlarge`ad esempio, puoi allegare fino a 25 volumi EBS (Limite di volume 28 - 3 interfacce di rete). Allo stesso modo, se si dispone di due interfacce di rete aggiuntive su un`m5d.xlarge`istanza, che ha 1 volume di archiviazione dell'istanza NVMe, è possibile collegare fino a 24 volumi EBS (Limite di 28 volumi - 3 interfacce di rete - 1 volume di archiviazione di istanze NVMe).

Le seguenti eccezioni sono i tipi di istanza con limiti di volume condivisi:

- Le istanze DL2q supportano un massimo di 19 volumi EBS.
- La maggior parte delle istanze bare metal supporta un massimo di 31 volumi EBS.
- `U-*tb1`le istanze virtualizzate supportano un massimo di 27 volumi EBS.
- `U-*tb1`le istanze bare metal supportano un massimo di 19 volumi EBS.
- Le istanze `inf1.xlarge` e `inf1.2xlarge` supportano fino a 26 volumi EBS.
- Le istanze `inf1.6xlarge` supportano fino a 23 volumi EBS.
- `mac1.metal`Le istanze supportano fino a 16 volumi EBS.
- `Mac2`, `Mac2-m2``Mac2-m2pro`, e `Mac2-m1ultra` le istanze supportano un massimo di 10 volumi EBS.
- `inf1.24xlarge`Le istanze supportano fino a 11 volumi EBS.
- Le istanze `g5.48xlarge` supportano fino a 9 volumi EBS.
- Le istanze `d3.8xlarge` e `d3en.12xlarge` supportano fino a 3 volumi EBS.
- Per le istanze di elaborazione accelerate, gli acceleratori collegati vengono conteggiati ai fini del limite di volume condiviso. Ad esempio, per`p4d.24xlarge`istanze, che hanno un limite di volume

condiviso di 28, 8 GPU e 8 volumi di archiviazione di istanze NVMe, puoi collegare fino a 11 volumi Amazon EBS (Limite di 28 volumi - 1 interfaccia di rete - 8 GPU - 8 volumi di archiviazione delle istanze NVMe).

Limiti di volume per le istanze basate su XEN

Istanze Linux

Il collegamento di più di 40 volumi a un'istanza Linux basata su Xen può causare errori di avvio. Questo numero include il volume root, qualsiasi volume di archivio dell'istanza collegato e i volumi Amazon EBS.

Se si verificano problemi di avvio su un'istanza con un numero elevato di volumi, arresta l'istanza, scollega i volumi non importanti per il processo di avvio, quindi ricollega i volumi quando l'istanza è in esecuzione.

> **Important**
>
> Il collegamento di oltre 40 volumi a un'istanza Linux è supportato solo sulla base del miglior tentativo e non è garantito.

Istanze Windows

La tabella riportata di seguito mostra i limiti dei volumi per le istanze Windows in base al driver utilizzato. Questi numeri includono il volume root, qualsiasi volume di archivio dell'istanza collegato e i volumi Amazon EBS.

> **Important**
>
> Il collegamento a un'istanza Windows di un numero di volumi superiore a quello riportato di seguito è supportato solo sulla base del miglior tentativo e non è garantito.

Driver	Limite di volumi
AWS PV	26

Driver	Limite di volumi
Citrix PV	26
Red Hat PV	17

Si consiglia di non collegare più di 26 volumi a un'istanza Windows basata su Xen con driver AWS PV o Citrix PV, poiché è probabile che ciò causi problemi di prestazioni. Per determinare i driver PV utilizzati dall'istanza o per aggiornare l'istanza Windows dai driver Red Hat ai driver Citrix PV, consulta the section called “Aggiornamento dei driver PV”.

Per ulteriori informazioni su come i nomi dei dispositivi sono correlati ai volumi, vedereMappare i dischi ai volumi nell'istanza Windows.

Volumi root per le tue istanze Amazon EC2

Quando avvii un'istanza, viene creato un volume root per l'istanza. Il volume root contiene l'immagine utilizzata per avviare l'istanza. Ogni istanza ha un singolo volume root. Puoi aggiungere volumi di storage alle tue istanze durante o dopo il lancio.

L'AMI che usi per avviare un'istanza determina il tipo di volume root. Puoi avviare un'istanza da un'AMI supportata da Amazon EBS (istanze Linux e Windows) o da un'AMI supportata da storage di istanze (solo istanze Linux). Esistono differenze significative tra ciò che è possibile fare con ciascun tipo di AMI. Per ulteriori informazioni su queste differenze, consulta Archiviazione del dispositivo root.

Consigliamo di utilizzare le AMI supportate da Amazon EBS perché queste istanze sono caratterizzate da un avvio più veloce e utilizzano un'archiviazione persistente.

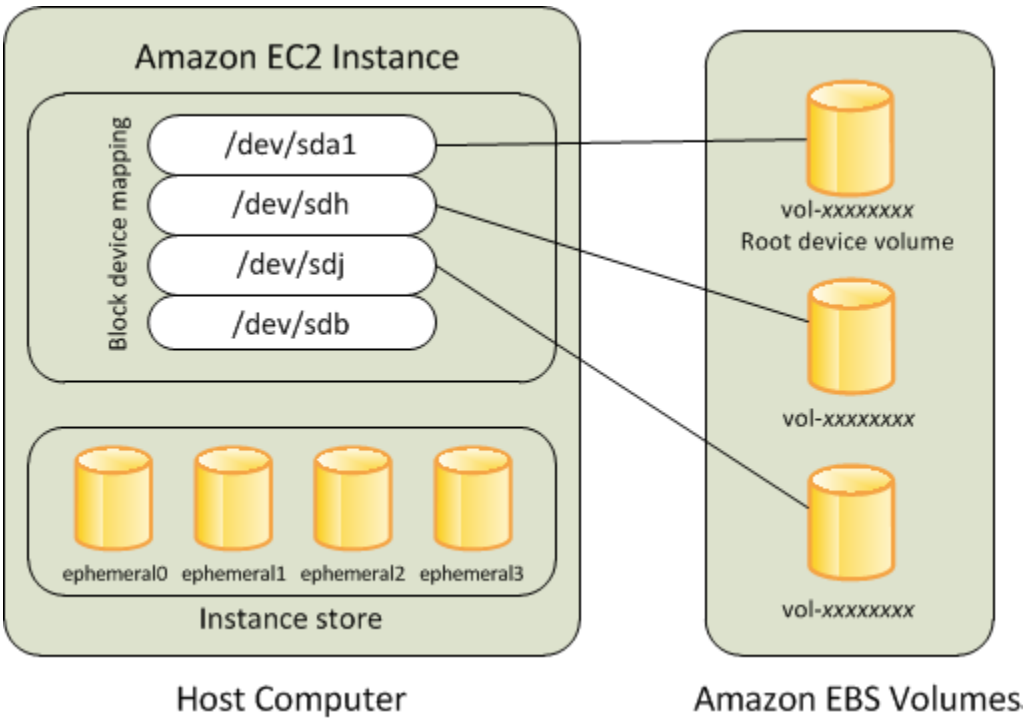
Riserviamo nomi di dispositivi specifici per i volumi root. Per ulteriori informazioni, consulta Nomi dei dispositivi sulle istanze Amazon EC2.

Indice

Istanze supportate da Amazon EBS

Alle istanze che utilizzano Amazon EBS per il volume root viene collegato automaticamente un volume Amazon EBS. Quando avvii un'istanza supportata da Amazon EBS, viene creato un volume Amazon EBS per ogni snapshot Amazon EBS a cui l'AMI utilizzata fa riferimento. Puoi facoltativamente utilizzare altri volumi Amazon EBS o volumi instance store, a seconda del tipo di istanza.

Un'istanza supportata da Amazon EBS può essere arrestata e riavviata in un secondo momento senza alcuna ripercussione sui dati archiviati nei volumi collegati. Sono disponibili varie attività relative alle istanze e ai volumi, che puoi eseguire quando un'istanza supportata da Amazon EBS si trova in uno stato arrestato. Ad esempio, puoi modificare le proprietà dell'istanza, modificarne le dimensioni o aggiornare il kernel utilizzato oppure puoi collegare il volume root a una diversa istanza in esecuzione a scopo di debug o altro. Per ulteriori informazioni, consulta Volumi Amazon EBS.



Limitazione

Non è possibile utilizzare i volumi EBS `st1` o `sc1` come volumi root.

Errore di un'istanza

Se l'esecuzione di un'istanza supportata da Amazon EBS non riesce, puoi ripristinare la sessione utilizzando uno dei seguenti metodi:

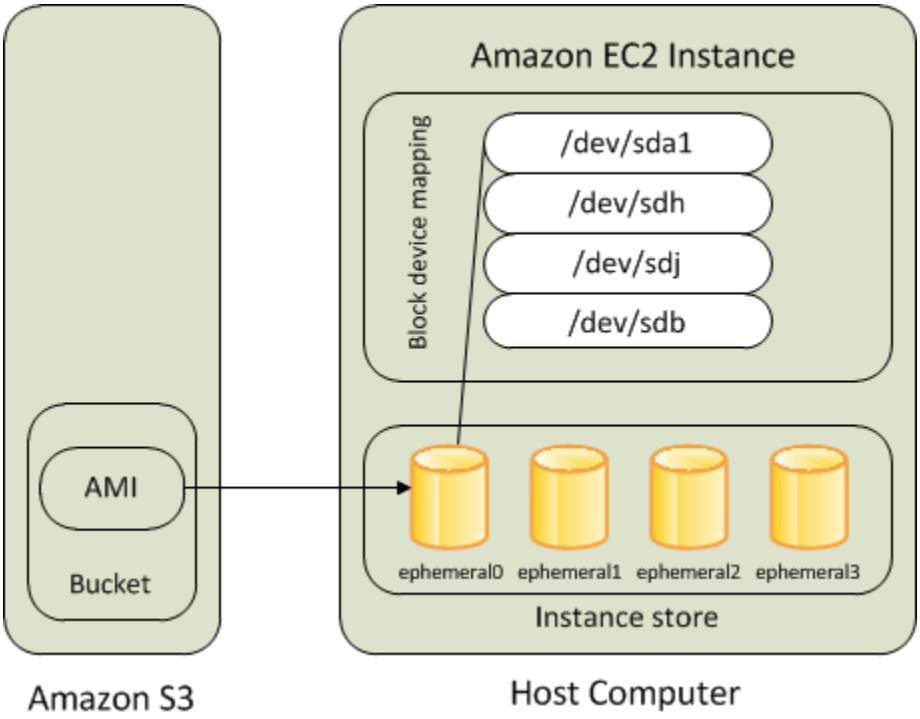
- Arrestare e quindi riavviare di nuovo (provare questo metodo come primo tentativo di soluzione).
- Creare automaticamente snapshot di tutti i volumi rilevanti e creare una nuova AMI. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.
- Collegare il volume a una nuova istanza effettuando la seguente procedura:
  1. Creare una snapshot del volume root.
  2. Registrare una nuova AMI utilizzando lo snapshot.
  3. Avviare una nuova istanza dalla nuova AMI.
  4. Scollegare i restanti volumi Amazon EBS dalla vecchia istanza.
  5. Ricollegare i volumi Amazon EBS alla nuova istanza.

Istanze supportate dall'archivio delle istanze (solo istanze Linux)

> **Note**
>
> Le istanze Windows non supportano i volumi root supportati da instance-store.

Le istanze che utilizzano un archivio dell'istanza per il volume root dispongono automaticamente di uno o più volumi di archivi dell'istanza disponibili, dove un volume funge da volume root. Quando un'istanza viene avviata, l'immagine utilizzata per l'avvio dell'istanza viene copiata nel volume root. Puoi facoltativamente utilizzare volumi instance store aggiuntivi, a seconda del tipo di istanza.

I dati presenti nei volumi instance store sono persistenti finché l'istanza è in esecuzione. Tali dati vengono tuttavia eliminati quando l'istanza viene terminata (le istanze supportate da instance store non supportano l'operazione Stop [Arresta]) oppure se l'avvio dell'istanza non riesce (ad esempio, se si verifica un problema in un'unità sottostante). Per ulteriori informazioni, consulta Instance store Amazon EC2.



Tipi di istanze supportati

Solo i seguenti tipi di istanza supportano un volume di instance store come volume root: C3, D2, I2, M3 e R3.

Errore di un'istanza

Se l'esecuzione di un'istanza supportata da instance store non riesce o viene terminata, non potrà essere terminata. Se prevedi di utilizzare istanze supportate da instance store Amazon EC2, ti consigliamo di distribuire i dati sugli instance store tra più zone di disponibilità. Consigliamo anche di eseguire regolarmente una copia di backup dei dati critici dai volumi dell'archivio istanza in modo da rendere persistente l'archiviazione.

Visualizza il tipo di dispositivo root dell'istanza

Nella console Amazon EC2, seleziona l'istanza e scegli la scheda Storage. In Dettagli del dispositivo root, controlla il valore del tipo di dispositivo root, che è uno dei seguenti valori:

- `EBS`— Si tratta di un'istanza supportata da Amazon EBS.
- `INSTANCE-STORE`— Si tratta di un'istanza supportata da un archivio di istanze.

In alternativa, è possibile utilizzare uno dei seguenti comandi:

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Modifica il volume root di un'istanza Amazon EC2 in modo che rimanga

Per impostazione predefinita, il volume root di Amazon EBS per un'istanza viene eliminato quando l'istanza termina. Puoi modificare il comportamento predefinito per garantire che un volume root di Amazon EBS persista dopo la chiusura dell'istanza. Per modificare il comportamento predefinito, imposta l'attributo su. `DeleteOnTermination` `false` Puoi farlo all'avvio dell'istanza o in un secondo momento.

Attività

- Configurare il volume root per la persistenza durante l'avvio dell'istanza
- Configurare il volume root in modo che persista per un'istanza esistente
- Confermare che un volume root è configurato per la persistenza

Configurare il volume root per la persistenza durante l'avvio dell'istanza

È possibile configurare il volume root in modo che persista all'avvio di un'istanza.

Console

Per configurare il volume root in modo che persista quando si avvia un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Instances (Istanze), quindi selezionare Launch Instance (Avvia istanza).
3. Scegliere una Amazon Machine Image (AMI), scegliere un tipo di istanza, scegliere una coppia di chiavi e configurare le impostazioni di rete.
4. Per Configura archiviazione, selezionare Avanzate.
5. Espandere il volume root.
6. In Elimina al termine, scegliere No.
7. Al termine della configurazione dell'istanza, scegliere Avvia istanza.

AWS CLI

Per configurare il volume root in modo che persista all'avvio di un'istanza, utilizza il AWS CLI

Utilizzare il comando run-instances e includere una mappatura dei dispositivi a blocchi che imposta l'attributo `DeleteOnTermination` su `false`.

```
aws ec2 run-instances --block-device-mappings file://mapping.json ...other
 parameters...
```

Specifica quanto segue nel file `mapping.json`.

```
[
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

Tools for Windows PowerShell

Per configurare il volume root in modo che persista all'avvio di un'istanza utilizzando gli Strumenti per Windows PowerShell

Utilizzate il New-EC2Instancecomando e includete una mappatura dei dispositivi a blocchi che imposta l'`DeleteOnTermination`attributo su. `false`

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
C:\> $bdm.DeviceName = "dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> New-EC2Instance -ImageId ami-0abcdef1234567890 -BlockDeviceMapping
 $bdm ...other parameters...
```

Configurare il volume root in modo che persista per un'istanza esistente

È possibile configurare il volume root in modo che persista per un'istanza in esecuzione. Tieni presente che non puoi completare questa attività utilizzando la console Amazon EC2.

AWS CLI

Per configurare il volume root in modo che persista per un'istanza esistente, utilizza il AWS CLI

Utilizzate il modify-instance-attributecomando con una mappatura dei dispositivi a blocchi che imposta l'`DeleteOnTermination`attributo su. `false`

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

Specifica quanto segue nel file `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

Tools for Windows PowerShell

Configurazione del volume root in modo che persista per un'istanza esistente utilizzando l' AWS Tools for Windows PowerShell

Utilizzare il Edit-EC2InstanceAttributecomando con una mappatura dei dispositivi a blocchi che imposta l'`DeleteOnTermination`attributo su. `false`

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
C:\> $bdm.DeviceName = "/dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -BlockDeviceMapping
 $bdm
```

Confermare che un volume root è configurato per la persistenza

Puoi verificare che un volume root sia configurato per la persistenza utilizzando la console Amazon EC2 o gli strumenti della riga di comando.

Console

Per verificare che un volume root sia configurato per la persistenza utilizzando la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e quindi selezionare l'istanza desiderata.
3. Nella scheda Storage (archiviazione) in Block devices (Dispositivi a blocchi), individuare la voce per il volume root. Se l'opzione Delete on termination (Elimina all'interruzione) è No, il volume è configurato per la persistenza.

AWS CLI

Per confermare che un volume root è configurato per persistere, utilizzare il AWS CLI

Utilizzare il comando describe-instances e verificare che l'attributo `DeleteOnTermination` nell'elemento di risposta `BlockDeviceMappings` sia impostato su `false`.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

```
...
    "BlockDeviceMappings": [
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "Status": "attached",
            "DeleteOnTermination": false,
            "VolumeId": "vol-1234567890abcdef0",
            "AttachTime": "2013-07-19T02:42:39.000Z"
        }
    }
...
```

Tools for Windows PowerShell

Per confermare che un volume root è configurato per persistere, utilizzare il AWS Tools for Windows PowerShell

Utilizzate Get-EC2Instancee verificate che l'`DeleteOnTermination`attributo nell'elemento `BlockDeviceMappings` response sia impostato `false` su.

```
C:\> (Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Sostituisci il volume principale di un'istanza EC2

Amazon EC2 consente di sostituire il volume Amazon EBS root per un'istanza in esecuzione mantenendo i seguenti elementi:

- Dati archiviati nei volumi di archivio dell'istanza: i volumi di archivio dell'istanza restano collegati all'istanza dopo il ripristino del volume root.
- Dati memorizzati nei volumi Amazon EBS di dati (non root): i volumi Amazon EBS non root restano collegati all'istanza dopo il ripristino del volume root.
- Configurazione di rete — Tutte le interfacce di rete rimangono collegate all'istanza e conservano gli indirizzi IP, gli identificatori e gli ID allegati. Quando l'istanza diventa disponibile, tutto il traffico di rete in sospeso viene scaricato. Inoltre, l'istanza rimane sullo stesso host fisico, quindi conserva gli indirizzi IP pubblici e privati e il nome DNS.
- Policy IAM — IAM I profili e le policy (ad esempio, le policy basate su tag) associati all'istanza vengono mantenuti e applicati.

Indice

Come funziona la sostituzione del volume root

Quando sostituisci il volume root per un'istanza, creiamo un'attività di sostituzione del volume root. Il volume root originale viene scollegato dall'istanza e al suo posto viene collegato il nuovo volume. La mappatura dei dispositivi a blocchi dell'istanza viene aggiornata per riflettere l'ID del volume root sostitutivo.

Quando sostituite il volume principale di un'istanza, dovete specificare l'origine dell'istantanea per il nuovo volume. Di seguito sono elencate le opzioni possibili.

Ripristina un volume root allo stato originale

Questa opzione sostituisce il volume principale corrente con un volume basato sull'istantanea utilizzata per crearlo.

Considerazioni sull'utilizzo dello stato di avvio

Il volume root sostitutivo ottiene gli stessi attributi di tipo, dimensione ed eliminazione alla terminazione del volume root originale.

Sostituisci il volume principale utilizzando un'istantanea

Questa opzione sostituisce il volume principale corrente con un volume sostitutivo basato sull'istantanea specificata. Ad esempio, un'istantanea specifica creata in precedenza da questo volume principale. Ciò è utile se è necessario risolvere problemi causati dal danneggiamento del volume root o da errori di configurazione di rete nel sistema operativo guest.

Il volume root sostitutivo ottiene gli stessi attributi di tipo, dimensione ed eliminazione alla terminazione del volume root originale.

Considerazioni sull'utilizzo di uno snapshot

- È possibile utilizzare solo istantanee che appartengono allo stesso lignaggio del volume root corrente.
- Non è possibile utilizzare copie snapshot create da snapshot acquisiti dal volume root.
- Dopo aver sostituito con successo il volume root, è ancora possibile utilizzare istantanee scattate dal volume root originale per sostituire il nuovo volume root (sostitutivo).

Sostituisci il volume root usando un AMI

Questa opzione sostituisce il volume root corrente utilizzando un AMI specificato dall'utente. Questa funzionalità è utile se è necessario eseguire patch o aggiornamenti del sistema operativo e delle applicazioni. L'AMI deve avere lo stesso codice di prodotto, informazioni di fatturazione, tipo di architettura e tipo di virtualizzazione dell'istanza.

Se l'istanza è abilitata per ENA o sriov-net, è necessario utilizzare un'AMI che supporti tali funzionalità. Se l'istanza non è abilitata per ENA o sriov-net, puoi selezionare un AMI che non include

il supporto per tali funzionalità oppure puoi aggiungere automaticamente il supporto se selezioni un AMI che supporta ENA o sriov-net.

Se l'istanza è abilitata per NitroTPM, è necessario utilizzare un'AMI con NitroTPM abilitato. Il supporto NitroTPM non è abilitato se l'istanza non è stata configurata per tale istanza, indipendentemente dall'AMI selezionata.

Puoi selezionare un'AMI con una modalità di avvio diversa da quella dell'istanza, purché l'istanza supporti la modalità di avvio dell'AMI. Se l'istanza non supporta la modalità di avvio, la richiesta non va a buon fine. Se l'istanza supporta la modalità di avvio, la nuova modalità di avvio viene propagata all'istanza e i relativi dati UEFI vengono aggiornati di conseguenza. Se hai modificato manualmente l'ordine di avvio o hai aggiunto una chiave UEFI Secure Boot privata per caricare i moduli privati del kernel, le modifiche vengono perse durante la sostituzione del volume root.

Il volume root sostitutivo ottiene gli stessi attributi di tipo ed eliminazione alla terminazione del volume root originale mentre ottiene la dimensione della mappatura dei dispositivi a blocchi del volume root dell'AMI.

> **Note**
>
> La dimensione della mappatura dei dispositivi a blocchi del volume root dell'AMI deve essere maggiore o uguale alla dimensione del volume root originale. Se la dimensione della mappatura dei dispositivi a blocchi del volume root dell'AMI è inferiore alla dimensione del volume root originale, la richiesta avrà esito negativo.

Una volta completata l'attività di sostituzione del volume root, le seguenti informazioni nuove e aggiornate vengono riportate nella descrizione dell'istanza utilizzando la console o gli SDK: AWS CLI AWS

- Nuovo ID AMI
- Nuovo ID volume per il volume root
- Configurazione della modalità di avvio aggiornata (se modificata dall'AMI)
- Configurazione NitroTPM aggiornata (se abilitata dall'AMI)
- Configurazione ENA aggiornata (se abilitata dall'AMI)
- Configurazione sriov-net aggiornata (se abilitata dall'AMI)

Il nuovo ID AMI si riflette anche nei metadati dell'istanza.

Considerazioni sull'utilizzo di un'AMI:

- Se utilizzi un'AMI con più mappature dei dispositivi a blocchi, viene utilizzato solo il volume root dell'AMI. Gli altri volumi (non root) vengono ignorati.
- Puoi utilizzare questa funzionalità solo se disponi delle autorizzazioni per l'AMI e per la snapshot del volume root associato. Non è possibile utilizzare questa funzionalità con Marketplace AWS le AMI.
- Puoi utilizzare un'AMI senza un codice prodotto solo se l'istanza non dispone di un codice prodotto.
- La dimensione della mappatura dei dispositivi a blocchi del volume root dell'AMI deve essere maggiore o uguale alla dimensione del volume root originale. Se la dimensione della mappatura dei dispositivi a blocchi del volume root dell'AMI è inferiore alla dimensione del volume root originale, la richiesta avrà esito negativo.
- I documenti di identità dell'istanza per l'istanza vengono aggiornati automaticamente.
- Se l'istanza supporta NitroTPM, i dati NitroTPM per l'istanza vengono ripristinati e vengono generate nuove chiavi.

È possibile scegliere se mantenere il volume root originale dopo il completamento del processo di sostituzione del volume root. Se decidi di eliminare il volume root originale dopo il completamento del processo di sostituzione, questo viene eliminato automaticamente e non può più essere recuperato. Se scegli di mantenere il volume root originale dopo il completamento del processo, il volume rimane fornito nel tuo account; devi eliminare manualmente il volume quando non ti serve più.

L'attività di sostituzione del volume principale passa attraverso i seguenti stati:

- `pending`— Il volume sostitutivo viene creato.
- `in-progress`— Il volume originale viene rimosso e il volume sostitutivo viene collegato.
- `succeeded`— Il volume sostitutivo è stato collegato correttamente all'istanza e l'istanza è disponibile.
- `failing`— L'operazione di sostituzione è in fase di fallimento.
- `failed`— L'operazione di sostituzione non è riuscita, ma il volume principale è ancora collegato.
- `failing-detached`— L'operazione di sostituzione sta per fallire e all'istanza potrebbe non essere collegato un volume root.

- `failed-detached`— L'operazione di sostituzione non è riuscita e all'istanza non è collegato un volume root.

Se l'operazione di sostituzione del volume root non riesce, l'istanza viene riavviata e il volume root originale rimane collegato all'istanza.

Considerazioni

Prima di iniziare, considerate quanto segue.

Requisiti

- L'istanza deve essere nello stato `running`.
- L'istanza viene riavviata automaticamente durante il processo. Il contenuto della memoria (RAM) viene cancellato durante il riavvio. Non sono necessari riavvii manuali.
- Non è possibile sostituire il volume root se si tratta di un volume di instance store. Sono supportate solo le istanze con volumi root di Amazon EBS.
- Puoi sostituire il volume root per tutti i tipi di istanza virtualizzati e per le istanze bare metal di EC2 per Mac. Non sono supportati altri tipi di istanze bare metal.
- Puoi utilizzare qualsiasi snapshot appartenente alla stessa linea dei volumi root precedenti dell'istanza.
- Se il tuo account è abilitato perCrittografia Amazon EBS di defaultnella regione corrente, il volume radice sostitutivo creato dall'attività di sostituzione del volume radice è sempre crittografato, indipendentemente dallo stato di crittografia dell'istantanea specificata o dal volume radice dell'AMI specificata.

Risultati della crittografia

La tabella seguente riepiloga i possibili risultati della crittografia.

	Volume root originale	Istantanea o AMI specificata	Crittografia per impostazione predefinita	Volume root sostitutivo	Chiave di crittografia utilizzata per sostituire il volume root
Ripristino del volume root sostitutivo allo stato di avvio	Crittografato	Non applicabile	Non considerato	Crittografato	Stessa chiave KMS del volume principale originale
	Non crittografato	Non applicabile	Disabilitato	Non crittografato	Non applicabile
	Non crittografato	Non applicabile	Abilitato	Crittografato	Accountchiave KMS predefinita per la crittografia Amazon EBS
Ripristina il volume root sostitutivo da snapshot o AMI	Crittografato	Non crittografato	Non considerato	Crittografato	Stessa chiave KMS del volume principale originale
	Crittografato	Crittografato	Non considerato	Crittografato	Stessa chiave KMS del volume principale originale
	Non crittografato	Non crittografato	Disabilitato	Non crittografato	Non applicabile

	Volume root originale	Istantanea o AMI specificata	Crittografia per impostazione predefinita	Volume root sostitutivo	Chiave di crittografia utilizzata per sostituire il volume root
	Non crittografato	Non crittografato	Abilitato	Crittografato	Accountchiave KMS predefinita per la crittografia Amazon EBS

	Volume root originale	Istantanea o AMI specificata	Crittografia per impostazione predefinita	Volume root sostitutivo	Chiave di crittografia utilizzata per sostituire il volume root
	Non crittografato	Crittografato	Non considerato	Crittografato	Se l'AMI o l'istantanea è di proprietà dell'account, il volume sostitutivo viene crittografato con la chiave KMS dell'AMI o dell'istantanea. Se AMI o snapshot sono condivisi con l'account, il volume sostitutivo viene crittografato con quello dell'account chiave KMS predefinita per la crittografia Amazon EBS.

Sostituzione di un volume root

Quando sostituisci il volume root per un'istanza, viene creata un'attività di sostituzione del volume root. Puoi utilizzare l'attività di sostituzione del volume root per monitorare l'avanzamento e l'esito del processo di sostituzione.

Console

Per sostituire il volume root

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza per la quale sostituire il volume root e scegliere Operazioni, Monitoraggio e risoluzione dei problemi, Sostituzione di un volume root.

   > **Note**
   >
   > Se l'istanza selezionata non è nello stato `running`, l'operazione Replace root volume (Sostituisci il volume root) è disabilitata.

4. Nella schermata Sostituisci volume root, per Ripristina, scegliete una delle seguenti opzioni:
   - Stato di avvio: ripristina il volume root sostitutivo dall'istantanea utilizzata per creare il volume root corrente.
   - Istantanea: ripristina il volume root sostitutivo nell'istantanea specificata. Per Snapshot, selezionate l'istantanea da usare.
   - Immagine: ripristina il volume root sostitutivo utilizzando l'AMI specificato. Per Immagine, seleziona l'AMI da usare.
5. (Facoltativo) Per eliminare il volume principale che state sostituendo, selezionate Elimina il volume radice sostituito.
6. Scegliete Crea attività sostitutiva.
7. Per monitorare l'attività di sostituzione, scegli la scheda Archiviazione per l'istanza ed espandi Attività recenti di sostituzione del volume principale.

AWS CLI

Ripristino del volume root sostitutivo allo stato di avvio

Utilizzate il comando create-replace-root-volume-task. Per `--instance-id`, specifica l'ID dell'istanza per la quale sostituire il volume root. Ometti i parametri `--snapshot-id` e `--image-id`. Per eliminare il volume root originale dopo che è stato sostituito, includi `--delete-replaced-root-volume` e specifica `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--delete-replaced-root-volume true
```

Ripristino del volume root sostitutivo in uno snapshot specifico

Utilizzare il comando create-replace-root-volume-task. Per `--instance-id`, specifica l'ID dell'istanza per la quale sostituire il volume root. Per `--snapshot-id`, specifica l'ID dello snapshot da utilizzare. Per eliminare il volume root originale dopo che è stato sostituito, includi `--delete-replaced-root-volume` e specifica `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--snapshot-id snap-9876543210abcdef0 \
--delete-replaced-root-volume true
```

Ripristino del volume root sostitutivo tramite un'AMI

Utilizzare il comando create-replace-root-volume-task. Per `--instance-id`, specifica l'ID dell'istanza per la quale sostituire il volume root. Per `--image-id`, specifica l'ID dell'AMI da utilizzare. Per eliminare il volume root originale dopo che è stato sostituito, includi `--delete-replaced-root-volume` e specifica `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-01234567890abcdef \
--image-id ami-09876543210abcdef \
--delete-replaced-root-volume true
```

Per visualizzare lo stato di un'attività di sostituzione del volume root

Utilizzate il comando describe-replace-root-volume-tasks e specificate gli ID delle attività di sostituzione del volume root da visualizzare.

```
$ aws ec2 describe-replace-root-volume-tasks \
--replace-root-volume-task-ids replacevol-1234567890abcdef0
```

```
{
  "ReplaceRootVolumeTasks": [
  {
    "ReplaceRootVolumeTaskId": "replacevol-1234567890abcdef0",
    "InstanceId": "i-1234567890abcdef0",
    "TaskState": "succeeded",
    "StartTime": "2020-11-06 13:09:54.0",
    "CompleteTime": "2020-11-06 13:10:14.0",
    "SnapshotId": "snap-01234567890abcdef",
    "DeleteReplacedRootVolume": "True"
  }]
}
```

In alternativa, specificare il filtro `instance-id` per filtrare i risultati in base all'istanza.

```
$ aws ec2 describe-replace-root-volume-tasks \
--filters Name=instance-id,Values=i-1234567890abcdef0
```

Tools for Windows PowerShell

Ripristino del volume root sostitutivo allo stato di avvio

Utilizza il comando New-EC2ReplaceRootVolumeTask. Per `-InstanceId`, specifica l'ID dell'istanza per la quale sostituire il volume root. Ometti i parametri `-SnapshotId` e `-ImageId`. Per eliminare il volume root originale dopo che è stato sostituito, includi `-DeleteReplacedRootVolume` e specifica `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
DeleteReplacedRootVolume $true
```

Ripristino del volume root sostitutivo in uno snapshot specifico

Utilizza il comando New-EC2ReplaceRootVolumeTask. Per `--InstanceId`, specifica l'ID dell'istanza per la quale sostituire il volume root. Per `-SnapshotId`, specifica l'ID dello snapshot da utilizzare. Per eliminare il volume root originale dopo che è stato sostituito, includi `-DeleteReplacedRootVolume` e specifica `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
SnapshotId snap-9876543210abcdef0 -DeleteReplacedRootVolume $true
```

Ripristino del volume root sostitutivo tramite un'AMI

Utilizza il comando New-EC2ReplaceRootVolumeTask. Per `-InstanceId`, specifica l'ID dell'istanza per la quale sostituire il volume root. Per `-ImageId`, specifica l'ID dell'AMI da utilizzare. Per eliminare il volume root originale dopo che è stato sostituito, includi `-DeleteReplacedRootVolume` e specifica `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
ImageId ami-09876543210abcdef -DeleteReplacedRootVolume $true
```

Per visualizzare lo stato di un'attività di sostituzione del volume root

Utilizzate il Get-EC2ReplaceRootVolumeTaskcomando e specificate gli ID delle attività di sostituzione del volume root da visualizzare.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -
ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0
```

In alternativa, specificare il filtro `instance-id` per filtrare i risultati in base all'istanza.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =
 'i-1234567890abcdef0'} | Format-Table
```

Nomi dei dispositivi sulle istanze Amazon EC2

Quando colleghi un volume alla tua istanza, includi un nome di dispositivo per il volume. Questo nome viene utilizzato da Amazon EC2. Il driver del dispositivo a blocchi per l'istanza assegna il nome di volume effettivo al momento del montaggio del volume e tale nome può differire da quello utilizzato da Amazon EC2.

Il numero di volumi che l'istanza può supportare viene determinato dal sistema operativo. Per ulteriori informazioni, consulta Limiti dei volumi delle istanze.

Indice

Nomi dei dispositivi disponibili

Istanze Linux

Sono disponibili due tipi di virtualizzazione per le istanze Linux: paravirtuale (PV) e della macchina virtuale hardware (HVM). Il tipo di virtualizzazione viene determinato dall'AMI utilizzata per avviare l'istanza. Tutti i tipi di istanza supportano le AMI HVM. Alcuni tipi di istanza di generazioni precedenti supportano PV AMI. Assicurati di prendere nota del tipo di virtualizzazione della tua AMI, poiché i nomi di dispositivo consigliati e disponibili dipendono dal tipo di virtualizzazione dell'istanza. Per ulteriori informazioni, consulta Tipi di virtualizzazione dell'AMI.

Nella tabella seguente sono elencati i nomi dei dispositivi disponibili che è possibile specificare in una mappatura dei dispositivi a blocchi o quando si collega un volume EBS.

Tipo di virtualizzazione	Disponibilità	Riservato per il volume root	Consigliato per volumi EBS	Volumi di instance store
Paravirtuale	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
HVM	/dev/sd[a-z] /dev/xvd [a-d] [a-z] /dev/xvd [e-z]	Differisce per AMI /dev/sda1 o /dev/xvda	/dev/sd[f-p] *	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge) **

* I nomi dei dispositivi specificati per i volumi EBS NVMe in una mappatura dei dispositivi a blocchi vengono rinominati utilizzando i nomi dei dispositivi NVMe (`/dev/nvme[0-26]n1`). Il driver del dispositivo a blocchi può assegnare i nomi del dispositivo NVMe con un ordine diverso da quello che hai specificato per i volumi nella mappatura del dispositivo a blocchi.

** I volumi instance store NVMe vengono enumerati automaticamente e viene loro assegnato un nome di dispositivo NVMe.

Istanze Windows

Le AMI Windows utilizzano uno dei seguenti set di driver per consentire l'accesso all'hardware virtualizzato: AWS PV, Citrix PV e PV. RedHat Per ulteriori informazioni, consulta the section called “Driver Windows PV”.

Nella tabella seguente sono elencati i nomi dei dispositivi disponibili che è possibile specificare in una mappatura dei dispositivi a blocchi o quando si collega un volume EBS.

Tipo di driver	Disponibilità	Riservato per il volume root	Consigliato per volumi EBS	Volumi di instance store
AWS PV, Citrix PV	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z] *	xvdc[a-x] xvd[a-e] **
Red Hat PV	xvd[a-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-p]	xvdc[a-x] xvd[a-e]

* Per Citrix PV e Red Hat PV, se si mappa un volume EBS con lo stesso nome`xvda`, Windows non riconosce il volume (il volume è visibile per PV o NVMe). AWS AWS

** I volumi instance store NVMe vengono enumerati automaticamente e viene loro assegnata una lettera di unità Windows.

Per ulteriori informazioni sui volumi di instance store, consulta Instance store Amazon EC2. Per ulteriori informazioni sui volumi NVMe EBS (istanze basate su Nitro), incluso come identificare il dispositivo EBS, consulta Amazon EBS e NVMe nella Amazon EBS User Guide.

Considerazioni sul nome dei dispositivi

Quando selezioni un nome di dispositivo, tieni presenti le informazioni seguenti:

- La parte finale dei nomi dei dispositivi che usi non deve sovrapporsi in quanto può causare problemi all'avvio dell'istanza. Ad esempio, evita di utilizzare combinazioni come `/dev/xvdf` e `xvdf` per volumi collegati alla stessa istanza.
- Sebbene tu possa collegare i volumi EBS utilizzando i nomi di dispositivo usati per collegare i volumi instance store, ti sconsigliamo fortemente di procedere in tal modo perché il comportamento potrebbe essere imprevedibile.
- Il numero di volumi instance store NVMe disponibili per un'istanza dipende dalla dimensione di quest'ultima. I volumi NVMe Instance Store vengono automaticamente enumerati e assegnati un nome di dispositivo NVMe (istanze Linux) o una lettera di unità Windows (istanze Windows).
- (Istanze Windows) Le AMI AWS Windows sono dotate di software aggiuntivo che prepara un'istanza al primo avvio. Si tratta del servizio EC2Config (AMI Windows precedente a Windows Server 2016) o del servizio EC2Launch (Windows Server 2016 e versioni successive). Dopo essere stati mappati alle unità, i dispositivi vengono inizializzati e montati. L'unità root viene inizializzata e montata come `C:\`. Per impostazione predefinita, quando un volume EBS viene collegato a un'istanza Windows, può comparire come qualsiasi lettera di unità nell'istanza. Puoi modificare le impostazioni per configurare le lettere di unità dei volumi in base alle tue specifiche. Ad esempio, i volumi di archiviazione, l'impostazione predefinita dipende dal driver. AWS I driver PV e i driver Citrix PV assegnano ai volumi di archiviazione delle istanze le lettere di unità che vanno da Z: a A:. I driver Red Hat assegnano, ai volumi instance store, lettere di unità che vanno dalla D: alla Z:. Per ulteriori informazioni, consulta Configura le impostazioni di avvio per le istanze Windows di Amazon EC2 e Mappare i dischi ai volumi nell'istanza Windows.
- (Istanze Linux) A seconda del driver del dispositivo a blocchi del kernel, il dispositivo potrebbe essere collegato con un nome diverso da quello specificato. Ad esempio, se specifichi un nome dispositivo `/dev/sdh`, il tuo dispositivo potrebbe essere rinominato `/dev/xvdh` o `/dev/hdh`. Nella maggior parte dei casi, la lettera finale rimane la stessa. In alcune versioni di Red Hat Enterprise Linux (e relative varianti, come CentOS), anche la lettera finale potrebbe cambiare (`/dev/sda` potrebbe diventare `/dev/xvde`). In questi casi, la lettera finale del nome di ciascun dispositivo aumenta dello stesso numero di volte. Ad esempio, se `/dev/sdb` è rinominato `/dev/`

`xvdf`, `/dev/sdc` viene rinominato `/dev/xvdg`. Amazon Linux crea un collegamento simbolico per il nome che hai specificato per il dispositivo rinominato. Altri sistemi operativi potrebbero avere un comportamento diverso.

- (Istanze Linux) Le AMI HVM non supportano l'uso di numeri finali nei nomi dei dispositivi, ad eccezione di, che è riservato al dispositivo root`/dev/sda1`, e. `/dev/sda2` Sebbene sia possibile utilizzare `/dev/sda2`, l'uso di questa mappatura dei dispositivi non è consigliata con istanze HVM.
- (Istanze Linux) Quando si utilizzano AMI PV, non è possibile allegare volumi che condividono le stesse lettere del dispositivo con e senza cifre finali. Ad esempio, se colleghi un volume come `/dev/sdc` e un altro volume come `/dev/sdc1`, solo `/dev/sdc` è visibile per l'istanza. Per utilizzare cifre finali nei nomi dei dispositivi, è necessario usarle in tutti i nomi che condividono le stesse lettere di base (come `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- (Istanze Linux) Alcuni kernel personalizzati potrebbero avere restrizioni che limitano l'uso a o. `/dev/sd[f-p]` `/dev/sd[f-p][1-6]` Se riscontri problemi con l'utilizzo di `/dev/sd[q-z]` o `/dev/sd[q-z][1-6]`, prova a passare a `/dev/sd[f-p]` o `/dev/sd[f-p][1-6]`.

Prima di specificare il nome del dispositivo che hai selezionato, verifica che sia disponibile. Altrimenti, riceverai un messaggio di errore indicante che il nome del dispositivo è già in uso. Per visualizzare i dispositivi a disco e i relativi punti di montaggio, utilizzate il lsblk comando (istanze Linux) o l'utilità Gestione disco o il diskpart comando (istanze Windows).

Mappatura dei dispositivi a blocchi

Ogni istanza che avvii dispone di un volume dispositivo root associato, che è un volume Amazon EBS o un volume instance store. Puoi utilizzare una mappatura dei dispositivi a blocchi per specificare ulteriori volumi EBS o volumi instance store da collegare a un'istanza quando viene avviata. Puoi anche collegare volumi EBS aggiuntivi a un'istanza in esecuzione. Tuttavia, il solo modo di collegare volumi instance store a un'istanza è utilizzare la mappatura dei dispositivi a blocchi per collegarli ai volumi quando l'istanza viene avviata.

Indice

Concetti relativi alla mappatura dei dispositivi a blocchi

Un dispositivo a blocchi è un dispositivo di archiviazione che sposta i dati in sequenze di byte o bit (blocchi). Tali dispositivi supportano l'accesso casuale e generalmente utilizzano I/O con buffering. Tra gli esempi sono inclusi hard disk, unità CD-ROM e unità flash. Un dispositivo a blocchi può essere collegato fisicamente a un computer oppure è possibile accedervi in remoto come se fosse collegato fisicamente.

Amazon EC2 supporta due tipi di dispositivi a blocchi:

- Volumi di instance store (dispositivi virtuali il cui hardware sottostante è fisicamente collegato al computer host per l'istanza)
- Volumi EBS (dispositivi di archiviazione remoti)

Una mappatura dei dispositivi a blocchi definisce i dispositivi a blocchi (volumi instance store e volumi EBS) da collegare a un'istanza. Puoi specificare una mappatura dei dispositivi a blocchi come parte del processo di creazione di un'AMI in modo che la mappatura venga utilizzata da tutte le istanze avviate dall'AMI. In alternativa, puoi specificare una mappatura dei dispositivi a blocchi quando avvii un'istanza, in modo che la mappatura sostituisca quella specificata nell'AMI da cui hai avviato l'istanza. Tieni presente che i volumi instance store NVMe supportati da un tipo di istanza vengono enumerati e assegnati a un nome di dispositivo automaticamente all'avvio dell'istanza; includerli nella mappatura dei dispositivi a blocchi non ha nessuna conseguenza.

Indice

Voci della mappatura dei dispositivi a blocchi

Quando crei una mappatura dei dispositivi a blocchi, devi specificare le seguenti informazioni per ogni dispositivo a blocchi che devi collegare all'istanza:

- Il nome del dispositivo utilizzato in Amazon EC2. Il driver dei dispositivi a blocchi dell'istanza assegna il nome del volume effettivo durante il montaggio del volume. Il nome assegnato può

essere diverso dal nome che Amazon EC2 consiglia. Per ulteriori informazioni, consulta Nomi dei dispositivi sulle istanze Amazon EC2.

Per i volumi dell'Instance store, è inoltre possibile specificare le seguenti informazioni:

- Il dispositivo virtuale: `ephemeral[0-23]`. Tieni presente che il numero e la dimensione dei volumi instance store per l'istanza variano a seconda del tipo di istanza stessa.

Per i volumi dell'Instance store di NVMe, si applicano anche le seguenti informazioni:

- Questi volumi vengono enumerati e assegnati a un nome di dispositivo automaticamente all'avvio dell'istanza; includerli nella mappatura dei dispositivi a blocchi non ha nessuna conseguenza.

Per i volumi EBS, specificare anche le seguenti informazioni:

- L'ID dello snapshot da utilizzare per creare il dispositivo a blocchi (snap-xxxxxxxx). Questo valore è opzionale se specifichi una dimensione per il volume. Non è possibile specificare l'ID di uno snapshot archiviato.
- La dimensione del volume in GiB. La dimensione specificata deve essere maggiore o uguale a quella della snapshot specificata.
- Determina se eliminare il volume al momento dell'interruzione dell'istanza (`true` o `false`). Il valore predefinito è `true` per il volume dispositivo root e `false` per i volumi collegati. Quando crei un'AMI, la relativa mappatura dei dispositivi a blocchi eredita questa impostazione dall'istanza. Quando avvii un'istanza, eredita questa impostazione dall'AMI.
- Il tipo di volume, che può essere `gp2` e `gp3` per SSD per scopo generico, `io1` e `io2` per SSD IOPS con provisioning, `st1` per HDD ottimizzati per velocità effettiva, `sc1` per HDD Cold o `standard` per Magnetici.
- Il numero di operazioni di input/output I/O al secondo (IOPS) supportato dal volume (Utilizzato solo con i volumi `io1` e `io2`).

Precisazioni sui volumi instance store nelle mappature dei dispositivi a blocchi

Ci sono molte precisazioni da tenere in considerazione quando avvii le istanze con le AMIs che nelle mappature dei dispositivi a blocchi hanno dei volumi instance store.

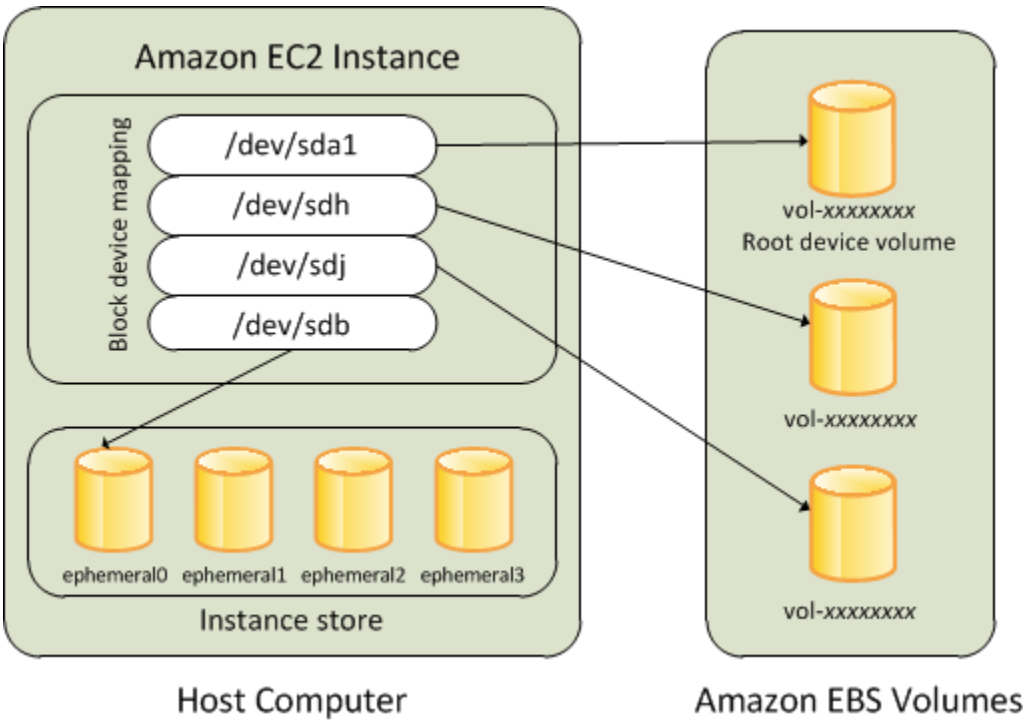
- Alcuni tipi di istanza includono più volumi instance store di altre, mentre alcune non ne contengono affatto. Se il tuo tipo di istanza supporta un volume instance store e la tua AMI dispone di mappature per due volumi instance store, l'istanza verrà avviata con un volume instance store.
- I volumi instance store possono essere mappati solo al momento dell'avvio. Non puoi arrestare un'istanza senza volumi instance store (come `t2.micro`), modificare l'istanza in un tipo che supporta i volumi instance store e riavviarla con volumi instance store. Tuttavia, puoi creare un'AMI dall'istanza e avviarla su un tipo di istanza che supporta i volumi instance store, quindi mappare questi volumi all'istanza.
- Se avvii un'istanza con volumi instance store mappati, quindi la arresti e la modifichi in un tipo di istanza con meno volumi instance store e la riavvii, le mappature dei volumi instance store dell'avvio iniziale mostreranno ancora i metadati dell'istanza. Tuttavia, per l'istanza è disponibile solo il numero massimo di volumi instance store supportati per quel tipo di istanza.

  > **Note**
  >
  > Quando un'istanza viene arrestata, tutti i dati sui volumi instance store vengono persi.

- A seconda della capacità dell'instance store al momento dell'avvio, le istanze M3 potrebbero ignorare le mappature dei dispositivi a blocchi dell'instance store dell'AMI, a meno che non vengano specificate all'avvio. Per essere certo che i volumi instance store siano disponibili all'avvio dell'istanza, anche se l'AMI che stai avviando include volumi instance store mappati nell'AMI, devi specificare le mappature dei dispositivi a blocchi dell'instance store.

Esempio di mappatura dei dispositivi a blocchi

L'illustrazione sottostante mostra un esempio di mappatura dei dispositivi a blocchi di un'istanza supportata da EBS. `/dev/sdb` viene mappato a `ephemeral0`, mentre un volume EBS viene mappato a `/dev/sdh` e l'altro a `/dev/sdj`. Nell'illustrazione è mostrato anche il volume EBS che rappresenta il volume dispositivo root, `/dev/sda1`.



Tieni presente che in questo argomento l'esempio di mappatura dei dispositivi a blocchi viene utilizzando nei comandi e nelle API di esempio. Puoi trovare i comandi e le API di esempio che consentono di creare le mappatura dei dispositivi a blocchi in Specificare una mappatura dei dispositivi a blocchi di un'AMI e Aggiornamento della mappatura dei dispositivi a blocchi all'avvio di un'istanza.

Come i dispositivi vengono resi disponibili nel sistema operativo

Nomi di dispositivo come `/dev/sdh` e `xvdh` vengono utilizzati da Amazon EC2 per descrivere i dispositivi a blocchi. La mappatura dei dispositivi a blocchi è utilizzata da Amazon EC2 per specificare i dispositivi a blocchi da collegare a un'istanza EC2. Prima che si possa accedere al dispositivo di archiviazione, dopo che è stato allegato a un'istanza, un dispositivo a blocchi deve essere montato dal sistema operativo. Se viene distaccato da un'istanza, un dispositivo a blocchi viene smontato dal sistema operativo e non è più possibile accedere al dispositivo di archiviazione.

Istanze Linux: i nomi dei dispositivi specificati nella mappatura dei dispositivi a blocchi vengono mappati sui dispositivi a blocchi corrispondenti al primo avvio dell'istanza. Il tipo di istanza determina quali volumi instance store formattare e montare per impostazione predefinita. Puoi montare volumi instance store aggiuntivi all'avvio, a condizione che non venga superato il numero consentito di volumi instance store per il tipo di istanza che hai scelto. Per ulteriori informazioni, consulta Instance store Amazon EC2. Il driver dei dispositivi a blocchi dell'istanza determina quali dispositivi utilizzare quando i volumi vengono formattati e montati.

Istanze Windows: i nomi dei dispositivi specificati nella mappatura dei dispositivi a blocchi vengono mappati sui dispositivi a blocchi corrispondenti al primo avvio dell'istanza, quindi il servizio Ec2Config inizializza e monta le unità. Il volume dispositivo root viene montato come `C:\`. I volumi instance store vengono montati come `Z:\`, `Y:\` e così via. Per montare un volume EBS, puoi utilizzare qualsiasi lettera di unità disponibile. Tuttavia, è possibile configurare il modo in cui le lettere di unità vengono assegnate ai volumi EBS; per ulteriori informazioni, consulta. the section called “Configura gli agenti di avvio di Windows”

Mappatura dei dispositivi a blocchi dell'AMI

Ogni AMI dispone di una mappatura dei dispositivi a blocchi che specifica i dispositivi a blocchi da collegare a un'istanza al suo avvio dall'AMI. Per aggiungere ulteriori dispositivi a blocchi a un'AMI devi creare una tua AMI.

Indice

Specificare una mappatura dei dispositivi a blocchi di un'AMI

Ci sono due modi per specificare i volumi oltre al volume root quando crei un'AMI. Se hai già collegato i volumi a un'istanza in esecuzione prima di creare un'AMI dall'istanza, la mappatura dei dispositivi a blocchi dell'AMI includerà gli stessi volumi. Per i volumi EBS, i dati esistenti vengono salvati in una nuova snapshot, che è specificata nella mappatura dei dispositivi a blocchi. Per i volumi instance store, i dati non vengono conservati.

Per un'AMI EBS-backed, puoi aggiungere i volumi EBS e i volumi instance store utilizzando la mappatura dei dispositivi a blocchi. Per un'AMI supportata da instance store, puoi aggiungere volumi instance store solo modificando le voci della mappatura dei dispositivi a blocchi nel file manifest di immagine al momento della registrazione dell'immagine.

> **Note**
>
> Per le istanze M3, devo specificare i volumi instance store nella mappatura dei dispositivi a blocchi dell'istanza quando la avvii. Quando avvii un'istanza M3, i volumi instance store specificati nella mappatura dei dispositivi a blocchi dell'AMI potrebbero venire ignorati se non sono stati specificati come parte della mappatura.

Console

Per aggiungere volumi a un'AMI tramite la console

1. Aprire la console Amazon EC2.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare un'istanza e scegliere Actions (Operazioni), Image and templates (Immagine e modelli), Create image (Crea immagine).
4. Inserire un nome e una descrizione per l'immagine.
5. I volumi di istanza vengono visualizzati in Instance volumes (Volumi istanza). Per aggiungere un altro volume, scegliere Add volume (Aggiungi volume).
6. Per Volume type (Tipo di volume), scegliere il tipo di volume. Per Device (Dispositivo), scegliere il nome del dispositivo. Per un volume EBS, è possibile specificare dettagli aggiuntivi, ad esempio uno snapshot, la dimensione del volume, il tipo di volume, lo IOPS e lo stato di crittografia.
7. Scegliere Create Image (Crea immagine).

Command line

Per aggiungere volumi a un'AMI tramite la riga di comando

Utilizza il AWS CLI comando create-image per specificare una mappatura dei dispositivi a blocchi per un'AMI supportata da EBS. Utilizza il AWS CLI comando register-image per specificare una mappatura dei dispositivi a blocchi per un'AMI basata su store-backed di istanze.

Specificare la mappatura dei dispositivi a blocchi utilizzando il parametro `--block-device-mappings`. Gli argomenti codificati in JSON possono essere forniti direttamente sulla riga di comando o per riferimento in una file:

```
--block-device-mappings [mapping, ...]
--block-device-mappings [file://mapping.json]
```

Per aggiungere un volume instance store, utilizzare la mappatura seguente:

```
{
    "DeviceName": "device_name",
    "VirtualName": "ephemeral0"
}
```

Per aggiungere un volume gp2 di 100 GiB vuoto, utilizzare la seguente mappatura:

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Per aggiungere un volume EBS basato su uno snapshot, utilizzare la seguente mappatura:

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "SnapshotId": "snap-xxxxxxxx"
    }
}
```

Per omettere la mappatura per un dispositivo, utilizzare la seguente mappatura:

```
{
    "DeviceName": "device_name",
    "NoDevice": ""
}
```

In alternativa, si può utilizzare il parametro `-BlockDeviceMapping` con i seguenti comandi (AWS Tools for Windows PowerShell):

- New-EC2Image
- Register-EC2Image

Visualizzazione dei volumi EBS nella mappatura dei dispositivi a blocchi di un'AMI

Puoi enumerare facilmente i volumi EBS nella mappatura dei dispositivi a blocchi dell'AMI.

Console

Per visualizzare i volumi EBS di un'AMI tramite la console

1. Aprire la console Amazon EC2.

2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Scegliere EBS images (Immagini EBS) nell'elenco Filter (Filtro) per ottenere un elenco di AMI EBS-backed.
4. Selezionare l'AMI desiderata e controllare la scheda Details (Dettagli). Per il dispositivo root sono disponibili almeno le seguenti informazioni:

   - Root Device Type (Tipo dispositivo root (`ebs`)
   - Root Device Name (Nome dispositivo root) (ad esempio, `/dev/sda1`)
   - Block Devices (Dispositivi a blocchi) (ad esempio, `/dev/sda1=snap-1234567890abcdef0:8:true`)

   Se l'AMI è stata creata con volumi EBS aggiuntivi tramite la mappatura dei dispositivi a blocchi, nel campo Block Devices (Dispositivi a blocchi) viene visualizzata anche la mappatura di tali volumi aggiuntivi (Questa schermata non visualizza i volumi instance store).

Command line

Per visualizzare i volumi EBS di un'AMI tramite la riga di comando

Utilizzate il comando describe-images (AWS CLI) o il comando Get-EC2Image(AWS Tools for Windows PowerShell) per enumerare i volumi EBS nella mappatura dei dispositivi a blocchi per un'AMI.

Mappatura dei dispositivi a blocchi delle istanze

Per impostazione predefinita, un'istanza avviata include eventuali dispositivi di archiviazione specificati nella mappatura dei dispositivi a blocchi di un'AMI da cui l'istanza è stata avviata. Puoi specificare le modifiche alle mappatura dei dispositivi a blocchi di un'istanza quando la avvii; tali aggiornamenti sostituiscono la mappatura dei dispositivi a blocchi dell'AMI o si uniscono a essa.

Limitazioni

- Per il volume root, puoi solo modificare: le dimensioni, il tipo e il contrassegno È possibile modificare il Delete on Termination (Elimina al termine).
- Quando modifichi un volume EBS non puoi ridurne le dimensioni, pertanto devi specificare una snapshot le cui dimensioni siano uguali o maggiori di quelle della snapshot specificata nella mappatura dei dispositivi a blocchi dell'AMI.

Indice

Aggiornamento della mappatura dei dispositivi a blocchi all'avvio di un'istanza

Puoi aggiungere volumi EBS e volumi instance store a un'istanza al momento del suo avvio. Tieni presente che l'aggiornamento della mappatura dei dispositivi a blocchi di un'istanza non comporta una modifica permanente della mappatura dell'AMI da cui l'istanza è stata avviata.

Console

Per aggiungere volumi a un'istanza tramite la console

1. Aprire la console Amazon EC2.
2. Dal pannello di controllo, selezionare Launch Instance (Avvia istanza).
3. Nella pagina Choose an Amazon Machine Image (AMI) (Scegli Amazon Machine Image (AMI)), scegliere Community AMIs (AMI della community).
4. Segui le istruzioni della procedura guidata per completare le pagine Choose an Instance Type (Scegli il tipo di istanza) e Configure Instance Details (Configura i dettagli dell'istanza).
5. Nella pagina Add Storage (Aggiungi archiviazione), puoi modificare il volume root, i volumi EBS e i volumi instance store nel modo seguente:
   - Per modificare le dimensioni del volume root, individuare il volume Root nella colonna Type (Tipo) e modificarne il campo Size (Dimensioni).
   - Per eliminare un volume EBS specificato dalla mappatura dei dispositivi a blocchi dell'AMI utilizzata per l'avvio dell'istanza, individuare il volume e fare clic sula relativa icona Delete (Elimina).
   - Per aggiungere un volume EBS, scegli Add New Volume (Aggiungi nuovo volume), EBS nell'elenco Type (Tipo), quindi completa i campi (Device (dispositivo), Snapshot e così via).
   - Per eliminare un volume instance store specificato dalla mappatura dei dispositivi a blocchi dell'AMI utilizzata per l'avvio dell'istanza, individuare il volume e scegliere la relativa icona Delete (Elimina).

- Per aggiungere un volume instance store, scegliere Add New Volume (Aggiungi nuovo volume), selezionare Instance Store dall'elenco Type (Tipo) e selezionare il nome di un dispositivo da Device (Dispositivo).

6. Completare le restanti pagine della procedura guidata e scegliere Launch (Avvia).

Command line

Per aggiungere volumi a un'istanza utilizzando AWS CLI

Utilizzate il AWS CLI comando run-instances con l'`--block-device-mapping`opzione di specificare una mappatura dei dispositivi a blocchi per un'istanza al momento del lancio.

Ad esempio, supponiamo che un'AMI supportata da EBS specifichi la seguente mappatura dei dispositivi a blocchi per un'istanza Linux:

- `/dev/sdb` = `ephemeral0`
- `/dev/sdh` = `snap-1234567890abcdef0`
- `/dev/sdj` = `100`

Per evitare che `/dev/sdj` venga collegato a un'istanza avviata da questa AMI, utilizzare la mappatura seguente.

```
{
    "DeviceName": "/dev/sdj",
    "NoDevice": ""
}
```

Per aumentare la dimensione di to, specifica la seguente `/dev/sdh` `300 GiB` mappatura. Si noti che non occorre specificare l'ID della snapshot per `/dev/sdh` poiché per individuare il volume è sufficiente specificare il nome del dispositivo.

```
{
    "DeviceName": "/dev/sdh",
    "Ebs": {
      "VolumeSize": 300
    }
}
```

Per aumentare la dimensione del volume root all'avvio dell'istanza, chiama prima describe-images con l'ID dell'AMI per verificare il nome del dispositivo del volume root. Ad esempio, `"RootDeviceName": "/dev/xvda"`. Per sovrascrivere la dimensione del volume root, specifica il nome del dispositivo root utilizzato dall'AMI e la nuova dimensione del volume.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Per collegare un volume instance store aggiuntivo, `/dev/sdc`, specificare la seguente mappatura. Se il tipo di istanza non supporta più volumi instance store, la mappatura non ha effetto. Se i volumi di instance store NVMe sono supportati dall'istanza, vengono enumerati automaticamente e viene assegnato loro un nome di dispositivo NVMe.

```
{
    "DeviceName": "/dev/sdc",
    "VirtualName": "ephemeral1"
}
```

Per aggiungere volumi a un'istanza utilizzando il AWS Tools for Windows PowerShell

Utilizzate il `-BlockDeviceMapping` parametro con il New-EC2Instancecomando (AWS Tools for Windows PowerShell).

Aggiornamento della mappatura dei dispositivi a blocchi di un'istanza in esecuzione

È possibile utilizzare il modify-instance-attribute AWS CLI comando per aggiornare la mappatura dei dispositivi a blocchi di un'istanza in esecuzione. Non è necessario arrestare l'istanza prima di cambiare questo attributo.

```
aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings
 file://mapping.json
```

Ad esempio, per conservare il volume root al momento dell'interruzione dell'istanza, specificare quanto segue in `mapping.json`:

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

In alternativa, è possibile utilizzare il `-BlockDeviceMapping` parametro con il Edit-EC2InstanceAttributecomando (AWS Tools for Windows PowerShell).

Visualizzazione dei volumi EBS nella mappatura dei dispositivi a blocchi di un'istanza

Puoi enumerare facilmente i volumi EBS mappati a un'istanza.

> **Note**
>
> Per le istanze avviate prima del rilascio dell'API 2009-10-31, non è AWS possibile visualizzare la mappatura dei dispositivi a blocchi. È necessario scollegare e ricollegare i volumi in modo da poter visualizzare la mappatura dei dispositivi a blocchi. AWS

Console

Per visualizzare i volumi EBS di un'istanza tramite la console

1. Aprire la console Amazon EC2.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Nella barra di ricerca, digitare Root Device Type (Tipo di dispositivo root), quindi scegliere EBS. Viene visualizzato un elenco delle istanze supportate da EBS.
4. Selezionare l'istanza desiderata ed esaminare i dettagli visualizzati nella scheda Storage (Archiviazione). Per il dispositivo root sono disponibili almeno le seguenti informazioni:
   - Tipo di dispositivo root (ad esempio, EBS)
   - Nome dispositivo root (ad esempio, `/dev/xvda`)
   - Dispositivi a blocchi (ad esempio, `/dev/xvda`, `/dev/sdf` e `/dev/sdj`)

Se l'istanza è stata avviata con volumi EBS aggiuntivi utilizzando una mappatura di dispositivi a blocchi, questi vengono visualizzati in Block devices (Dispositivi a blocchi). Qualsiasi volume dell'instance store non viene visualizzato in questa scheda.

5. Per visualizzare ulteriori informazioni su un volume EBS, scegliere il relativo ID volume per andare alla pagina del volume.

Command line

Per visualizzare i volumi EBS di un'istanza utilizzando la riga di comando

Utilizzate il comando describe-instances (AWS CLI) o Get-EC2Instanceil comando () per enumerare i AWS Tools for Windows PowerShell volumi EBS nella mappatura dei dispositivi a blocchi per un'istanza.

Visualizzazione della mappatura dei dispositivi a blocchi di un'istanza per i volumi instance store

Il tipo di istanza determina il numero e il tipo di volumi di Instance Store disponibili per l'istanza. Se il numero di volumi instance store in una mappatura dei dispositivi a blocchi supera il numero disponibile di volumi instance store per un'istanza, i volumi vengono ignorati. Per visualizzare i volumi di Instance Store per la tua istanza, esegui il lsblk comando (istanze Linux) o apri Windows Disk Management (istanze Windows). Per sapere quanti volumi di Instance Store sono supportati da ciascun tipo di istanza, consulta le specifiche del tipo di istanza Amazon EC2.

Quando visualizzi la mappatura dei dispositivi a blocchi della tua istanza, puoi vedere solo i volumi EBS e non i volumi instance store. Il metodo utilizzato per visualizzare i volumi dell'archivio istanza per l'istanza dipende dal tipo di volume.

Volumi di archivio istanza NVMe

Istanze Linux

È possibile utilizzare il pacchetto della riga di comando NVMe, nvme-cli, per eseguire query sui volumi dell'archivio istanza NVMe nella mappatura dei dispositivi a blocchi. Scarica e installa il pacchetto sull'istanza, quindi emetti il seguente comando.

```
[ec2-user ~]$ sudo nvme list
```

Di seguito è riportato un esempio di output per un'istanza. Il testo nella colonna Modello indica se il volume è un volume EBS o un volume dell'archivio istanza. In questo esempio, entrambi `/dev/nvme1n1` e `/dev/nvme2n1` sono volumi dell'archivio istanza.

```
Node             SN                   Model
 Namespace
---------------- -------------------- ----------------------------------------
 ---------
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store               1

/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage         1

/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage         1
  ...
```

Istanze Windows

Puoi utilizzare Disk Management o PowerShell elencare sia i volumi EBS che quelli di Instance Store NVMe. Per ulteriori informazioni, consulta the section called “Elencare i volumi NVMe”.

Volumi di archivio istanza HDD o SSD

È possibile utilizzare i metadati dell'istanza per effettuare query sui volumi dell'archivio istanza HDD o SSD nella mappatura dei dispositivi a blocchi. I volumi dell'instance store NVMe non sono inclusi nella mappatura dei dispositivi a blocchi.

L'URI di base di tutte le richieste dei metadati dell'istanza è `http://169.254.169.254/latest/`. Per ulteriori informazioni, consulta Utilizzo dei metadati delle istanze.

Istanze Linux

Innanzitutto connettiti all'istanza in esecuzione, quindi da essa utilizza questa query per ottenere la relativa mappatura dei dispositivi a blocchi.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

La risposta include i nomi dei dispositivi a blocchi dell'istanza. Ad esempio, l'output di un'istanza `m1.small` supportata da archivio istanza somiglia a quello seguente.

```
ami
ephemeral0
root
swap
```

Il dispositivo `ami` è il dispositivo root come visto dall'istanza. I volumi instance store sono denominati `ephemeral[0-23]`. Il dispositivo `swap` è destinato al file di paging. Se hai mappato anche i volumi EBS, questi appariranno come `ebs1`, `ebs2` e così via.

Per ottenere i dettagli su un singolo dispositivo a blocchi nella mappatura dei dispositivi a blocchi, aggiungi il suo nome alla query precedente, come mostrato.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Istanze Windows

Innanzitutto connettiti all'istanza in esecuzione, quindi da essa utilizza questa query per ottenere la relativa mappatura dei dispositivi a blocchi.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/
```

La risposta include i nomi dei dispositivi a blocchi dell'istanza. Ad esempio, l'output di un'istanza `m1.small` supportata da archivio istanza somiglia a quello seguente.

```
ami
ephemeral0
root
swap
```

Il dispositivo `ami` è il dispositivo root come visto dall'istanza. I volumi instance store sono denominati `ephemeral[0-23]`. Il dispositivo `swap` è destinato al file di paging. Se hai mappato anche i volumi EBS, questi appariranno come `ebs1`, `ebs2` e così via.

Per ottenere i dettagli su un singolo dispositivo a blocchi nella mappatura dei dispositivi a blocchi, aggiungi il suo nome alla query precedente, come mostrato.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Mappare i dischi ai volumi nell'istanza Windows

> **Note**
>
> Questo argomento si applica solo alle istanze di Windows.

La tua istanza Windows include un volume EBS che funge da volume root. Se l'istanza Windows utilizza driver AWS PV o Citrix PV, è possibile aggiungere facoltativamente fino a 25 volumi, per un totale di 26 volumi. Per ulteriori informazioni, consulta Limiti dei volumi delle istanze.

A seconda del tipo di istanza della tua istanza, avrai da 0 a 24 volumi di instance store disponibili possibili per l'istanza. Per utilizzare qualsiasi dei volumi di instance store disponibili per l'istanza, è necessario specificarli alla creazione dell'AMI o all'avvio dell'istanza. Puoi inoltre aggiungere volumi EBS alla creazione dell'AMI o all'avvio dell'istanza o collegarli durante l'esecuzione dell'istanza.

Quando aggiungi un volume all'istanza, è necessario specificare il nome del dispositivo utilizzato da Amazon EC2. Per ulteriori informazioni, consulta Nomi dei dispositivi sulle istanze Amazon EC2.

AWS Le Amazon Machine Image (AMI) di Windows contengono un set di driver utilizzati da Amazon EC2 per mappare volume di archivio istanza e EBS ai dischi Windows e alle lettere di unità. Se si avvia un'istanza da un'AMI Windows che utilizza driver AWS PV o Citrix PV, è possibile utilizzare le relazioni descritte in questa pagina per mappare i dischi Windows all'instance store e ai volumi EBS. Se la tua AMI Windows utilizza driver Red Hat PV, puoi aggiornare l'istanza per utilizzare i driver Citrix. Per ulteriori informazioni, consulta the section called “Aggiornamento dei driver PV”.

Indice

Elencare i volumi NVMe

Puoi individuare i dischi sull'istanza Windows tramite Disk Management (Gestione disco) o Powershell.

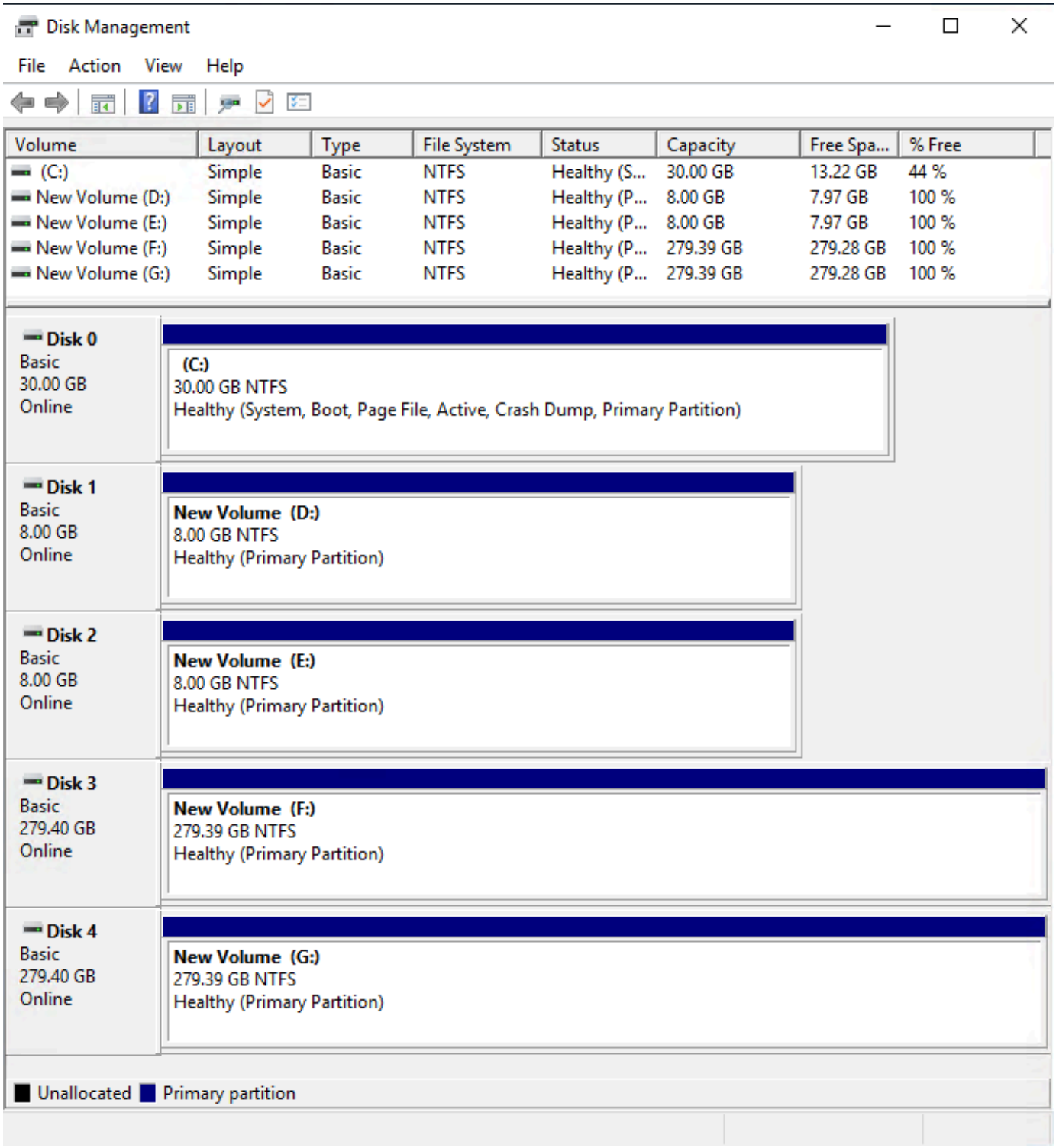
Elencare i dischi NVMe utilizzando Gestione disco

Puoi individuare i dischi sull'istanza Windows tramite Disk Management (Gestione disco).

Individuazione dei dischi sulla tua istanza Windows

1. Accedere all'istanza Windows tramite Remote Desktop. Per ulteriori informazioni, consulta Connettiti all'istanza Windows .
2. Avviare l'utilità Disk Management (Gestione disco).
3. Esamina i dischi. Il volume root è un volume EBS montato come `C:\`. Se non sono visualizzati altri dischi, significa che non hai specificato volumi aggiuntivi alla creazione dell'AMI o all'avvio dell'istanza.

Di seguito è riportato un esempio che mostra i dischi disponibili se si avvia un'istanza `r5d.4xlarge` con due volumi EBS aggiuntivi.



Elenca i dischi NVMe utilizzando PowerShell

PowerShell Lo script seguente elenca ogni disco con il nome e il volume del dispositivo corrispondenti. È destinato all'uso con istanze basate sul sistema AWS Nitro, che utilizzano NVMe EBS e volumi di Instance Store.

Connect all'istanza di Windows ed esegui il comando seguente per abilitare l'esecuzione PowerShell dello script.

```
Set-ExecutionPolicy RemoteSigned
```

Copiare lo script seguente e salvarlo come `mapping.ps1` nell'istanza Windows.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
       $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device  = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
     else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
```

```
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber =  (Get-Disk -Path $Path).Number
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber

}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId  = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
      Disk          = $Disk
      Partitions    = $Partition
      DriveLetter   = $DriveLetter
      EbsVolumeId   = $EbsVolumeId
      Device        = $Device
      VirtualDevice = $VirtualDevice
      VolumeName= $VolumeName
    }
```

```
 $Report += $Disk
}

$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Eseguire lo script come segue:

```
PS C:\> .\mapping.ps1
```

Di seguito è riportato un output di esempio per un'istanza con un volume root, due volumi EBS e due volumi instance store.

```
Disk Partitions DriveLetter EbsVolumeId           Device    VirtualDevice VolumeName
---- ---------- ----------- -----------           ------    ------------- ----------
   0          1 C           vol-03683f1d861744bc7 /dev/sda1 root
   1          1 D           vol-082b07051043174b9 xvdb      N/A
   2          1 E           vol-0a4064b39e5f534a2 xvdc      N/A
   3          1 F           AWS-6AAD8C2AEEE1193F0 Ephemeral N/A           Temporary
 Storage
   4          1 G           AWS-13E7299C2BD031A28 Ephemeral N/A           Temporary
 Storage
```

Se non hai configurato le credenziali per Tools for Windows PowerShell sull'istanza Windows, lo script non può ottenere l'ID del volume EBS e utilizza N/A nella colonna. `EbsVolumeId`

Mappare i volumi EBS NVMe

Con le istanze basate sul sistema AWS Nitro, i volumi EBS vengono esposti come dispositivi NVMe. È possibile utilizzare il comando Get-Disk per mappare numeri di dischi Windows a ID di volumi EBS.

```
PS C:\> Get-Disk
Number Friendly Name Serial Number                    HealthStatus
 OperationalStatus      Total Size Partition

                      Style
------ ------------ -------------                    ------------
 -----------------      ---------- ----------
3      NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.   Healthy              Online
              279.4 GB MBR
4      NVMe Amazo... AWS13E7299C2BD031A28_00000001.   Healthy              Online
              279.4 GB MBR
```

```
2      NVMe Amazo... vol0a4064b39e5f534a2_00000001.   Healthy              Online
                8 GB MBR
0      NVMe Amazo... vol03683f1d861744bc7_00000001.   Healthy              Online
               30 GB MBR
1      NVMe Amazo... vol082b07051043174b9_00000001.   Healthy              Online
                8 GB MBR
```

È anche possibile eseguire il comando ebsnvme-id per eseguire la mappatura dei numeri del disco NVMe con gli ID volume EBS e i nomi dei dispositivi.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Elencare i volumi

Puoi individuare i dischi sull'istanza Windows tramite Disk Management (Gestione disco) o Powershell.

Elencare i dischi utilizzando Gestione disco

Puoi individuare i dischi sull'istanza Windows tramite Disk Management (Gestione disco).

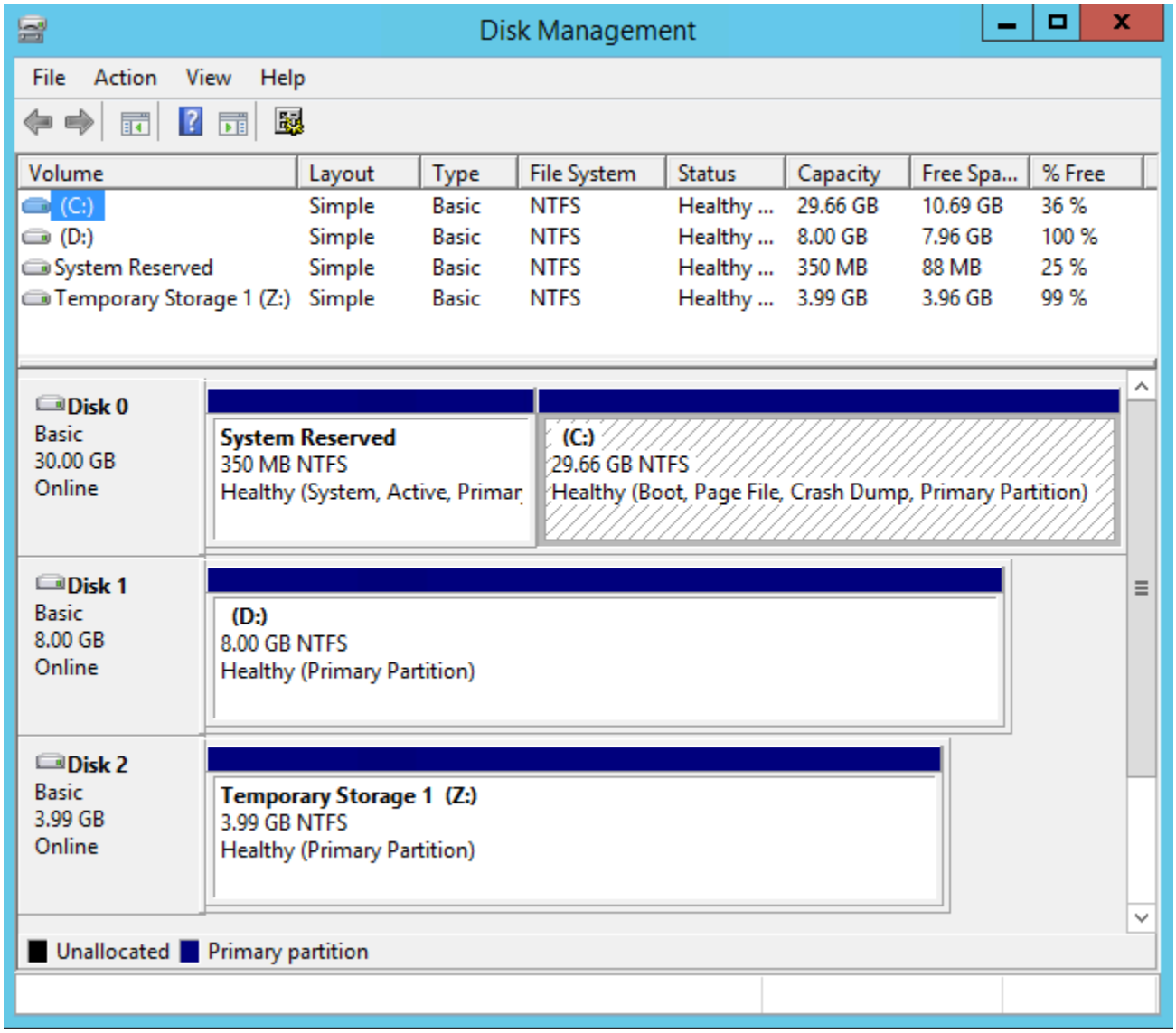
Individuazione dei dischi sulla tua istanza Windows

1. Accedere all'istanza Windows tramite Remote Desktop. Per ulteriori informazioni, consulta Connettiti all'istanza Windows .
2. Avviare l'utilità Disk Management (Gestione disco).

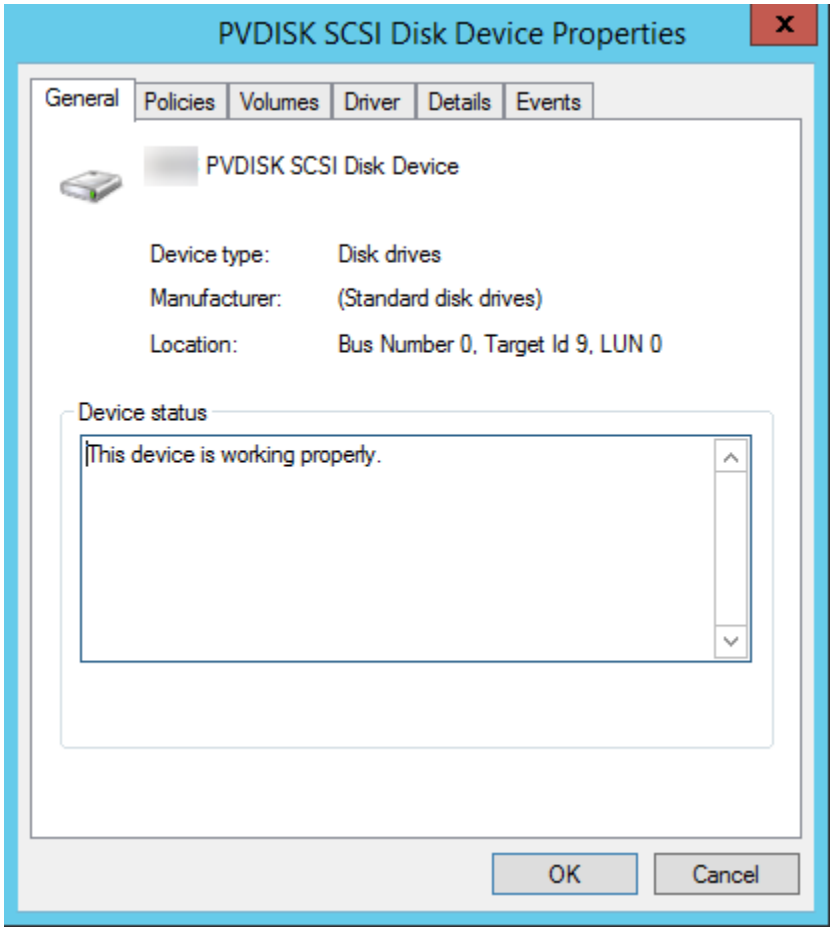
   Sulla barra delle applicazioni, fai clic con il pulsante destro del mouse sul logo di Windows, quindi scegli Gestione disco.

3. Esamina i dischi. Il volume root è un volume EBS montato come `C:\`. Se non sono visualizzati altri dischi, significa che non hai specificato volumi aggiuntivi alla creazione dell'AMI o all'avvio dell'istanza.

   Nell'esempio riportato di seguito sono illustrati i dischi disponibili lanciando un'istanza `m3.medium` con un volume instance store (Disco 2) e un volume EBS aggiuntivo (Disco 1).



4. Fai clic con il pulsante destro del mouse sul riquadro grigio con l'etichetta Disco 1, quindi seleziona Properties (Proprietà). Prendi nota del valore di Location (Ubicazione) e cercalo nelle tabelle in Mappare i dispositivi disco ai nomi dei dispositivi. Ad esempio, il disco seguente presenta l'ubicazione Bus Number 0, Target Id 9, LUN 0. In base alla tabella dei volumi EBS, il nome del dispositivo di questa ubicazione è `xvdj`.



Mappare i dispositivi disco ai nomi dei dispositivi

Il driver del dispositivo a blocchi dell'istanza assegna i nomi del volume effettivi durante il montaggio dei volumi.

Mappature

- Volumi di archivio dell'istanza
- Volumi EBS

Volumi di archivio dell'istanza

La tabella seguente descrive come i driver Citrix PV e AWS PV mappano i volumi di istanze non NVMe ai volumi Windows. Il numero di volumi instance store disponibili è determinato dal tipo di istanza. Per ulteriori informazioni, consulta Volumi di archivio dell'istanza.

Ubicazione	Nome dispositivo
Bus Number 0, Target ID 78, LUN 0	xvdca
Bus Number 0, Target ID 79, LUN 0	xvdcb
Bus Number 0, Target ID 80, LUN 0	xvdcc
Bus Number 0, Target ID 81, LUN 0	xvdcd
Bus Number 0, Target ID 82, LUN 0	xvdce
Bus Number 0, Target ID 83, LUN 0	xvdcf
Bus Number 0, Target ID 84, LUN 0	xvdcg
Bus Number 0, Target ID 85, LUN 0	xvdch
Bus Number 0, Target ID 86, LUN 0	xvdci
Bus Number 0, Target ID 87, LUN 0	xvdcj
Bus Number 0, Target ID 88, LUN 0	xvdck
Bus Number 0, Target ID 89, LUN 0	xvdcl

Volumi EBS

La tabella seguente descrive come i driver Citrix PV e AWS PV mappano i volumi EBS non NVMe ai volumi Windows.

Ubicazione	Nome dispositivo
Bus Number 0, Target ID 0, LUN 0	/dev/sda1
Bus Number 0, Target ID 1, LUN 0	xvdb
Bus Number 0, Target ID 2, LUN 0	xvdc
Bus Number 0, Target ID 3, LUN 0	xvdd

Ubicazione	Nome dispositivo
Bus Number 0, Target ID 4, LUN 0	xvde
Bus Number 0, Target ID 5, LUN 0	xvdf
Bus Number 0, Target ID 6, LUN 0	xvdg
Bus Number 0, Target ID 7, LUN 0	xvdh
Bus Number 0, Target ID 8, LUN 0	xvdi
Bus Number 0, Target ID 9, LUN 0	xvdj
Bus Number 0, Target ID 10, LUN 0	xvdk
Bus Number 0, Target ID 11, LUN 0	xvdl
Bus Number 0, Target ID 12, LUN 0	xvdm
Bus Number 0, Target ID 13, LUN 0	xvdn
Bus Number 0, Target ID 14, LUN 0	xvdo
Bus Number 0, Target ID 15, LUN 0	xvdp
Bus Number 0, Target ID 16, LUN 0	xvdq
Bus Number 0, Target ID 17, LUN 0	xvdr
Bus Number 0, Target ID 18, LUN 0	xvds
Bus Number 0, Target ID 19, LUN 0	xvdt
Bus Number 0, Target ID 20, LUN 0	xvdu
Bus Number 0, Target ID 21, LUN 0	xvdv
Bus Number 0, Target ID 22, LUN 0	xvdw
Bus Number 0, Target ID 23, LUN 0	xvdx

Ubicazione	Nome dispositivo
Bus Number 0, Target ID 24, LUN 0	xvdy
Bus Number 0, Target ID 25, LUN 0	xvdz

Elenca i dischi utilizzando PowerShell

PowerShell Lo script seguente elenca ogni disco con il nome e il volume del dispositivo corrispondenti.

Requisiti e limitazioni

- Richiede Windows Server 2012 o versione successiva.
- Richiede le credenziali per ottenere l'ID del volume EBS. Puoi configurare un profilo utilizzando gli strumenti per PowerShell o assegnare un ruolo IAM all'istanza.
- Non supporta volumi NVMe.
- Non supporta dischi dinamici.

Connect all'istanza di Windows ed esegui il comando seguente per abilitare l'esecuzione PowerShell dello script.

```
Set-ExecutionPolicy RemoteSigned
```

Copiare lo script seguente e salvarlo come `mapping.ps1` nell'istanza Windows.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
  param([int]$SCSITargetId)
  If ($SCSITargetId -eq 0) {
    return "sda1"
  }
  $deviceName = "xvd"
  If ($SCSITargetId -gt 25) {
    $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
  }
  $deviceName += [char](0x61 + $SCSITargetId % 26)
  return $deviceName
}
```

```
[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
  $array1 += $_.Name
  $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
  $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).SerialNumber) -
replace "_[^ ]*$" -replace "vol", "vol-"
  $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).FriendlyName)
  $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
  $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
  $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -ExpandProperty
 SystemName
}
Catch {
  Write-Host "Could not access the instance Metadata using AWS Get-EC2InstanceMetadata
 CMDLet.
Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and Metadata
 is enabled for this instance." -ForegroundColor Yellow
}
Try {
  $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
 $InstanceId).Instances.BlockDeviceMappings
  $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
  Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys or assigned an IAM role with adequate
 permissions." -ForegroundColor Yellow
}
```

```
Get-disk | ForEach-Object {
  $DriveLetter = $null
  $VolumeName = $null
  $VirtualDevice = $null
  $DeviceName = $_.FriendlyName

  $DiskDrive = $_
  $Disk = $_.Number
  $Partitions = $_.NumberOfPartitions
  $EbsVolumeID = $_.SerialNumber -replace "_[^ ]*$" -replace "vol", "vol-"
  if ($Partitions -ge 1) {
    $PartitionsData = Get-Partition -DiskId $_.Path
    $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
 $null) }
    $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
 @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
  }
  If ($DiskDrive.path -like "*PROD_PVDISK*") {
    $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
 Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
 $DiskDrive.Number) }).SCSITargetId)
    $BlockDeviceName = "/dev/" + $BlockDeviceName
    $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*" +
 $_.DeviceName + "*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
 $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").ephemeral((Get-WmiObject -Class Win32_Diskdrive | Where-Object
 { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)
    $BlockDevice = $null
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
 $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
```

```
        $i ++
      }
    }
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
   }
   ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
   }
   Else {
    $BlockDeviceName = $null
    $BlockDevice = $null
   }
   New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else
 { $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName    = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
   }
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions, DriveLetter,
 EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName
```

Eseguire lo script come segue:

```
PS C:\> .\mapping.ps1
```

Di seguito è riportato un output di esempio.

```
Disk  Partitions  DriveLetter   EbsVolumeId             Device      VirtualDevice
 DeviceName              VolumeName
----  ----------  -----------   -----------             ------      -------------
 ----------              ----------
   0           1             C   vol-0561f1783298efedd   /dev/sda1   N/A
 NVMe Amazon Elastic B   N/A
   1           1             D   vol-002a9488504c5e35a   xvdb        N/A
 NVMe Amazon Elastic B   N/A
   2           1             E   vol-0de9d46fcc907925d   xvdc        N/A
 NVMe Amazon Elastic B   N/A
```

Se non sono state fornite le credenziali sull'istanza Windows, lo script non può ottenere l'ID del volume EBS e utilizza N/A nella colonna `EbsVolumeId`.

Snapshot Amazon EBS basati su Windows VSS coerenti con le applicazioni

> **Note**
>
> Le istantanee basate su Windows VSS coerenti con l'applicazione sono supportate solo con le istanze Windows.

Puoi scattare istantanee coerenti con l'applicazione di tutti i volumi Amazon EBS collegati alle istanze Windows di Amazon EC2 utilizzando Run Command.AWS Systems Manager Il processo di creazione di snapshot utilizza il servizio Windows Volume Shadow Copy Service (VSS) per eseguire backup a livello di volume EBS compatibili con VSS. Gli snapshot includono dati delle transazioni in sospeso tra queste applicazioni e il disco. Non è necessario arrestare le istanze o scollegarle per eseguire il backup di tutti i volumi collegati.

Non sono previsti costi aggiuntivi per l'utilizzo di snapshot EBS basati su VSS. Paghi solo gli snapshot EBS creati dal processo di backup. Per ulteriori informazioni, consulta Come mi vengono fatturati i miei snapshot Amazon EBS EBS?

Indice

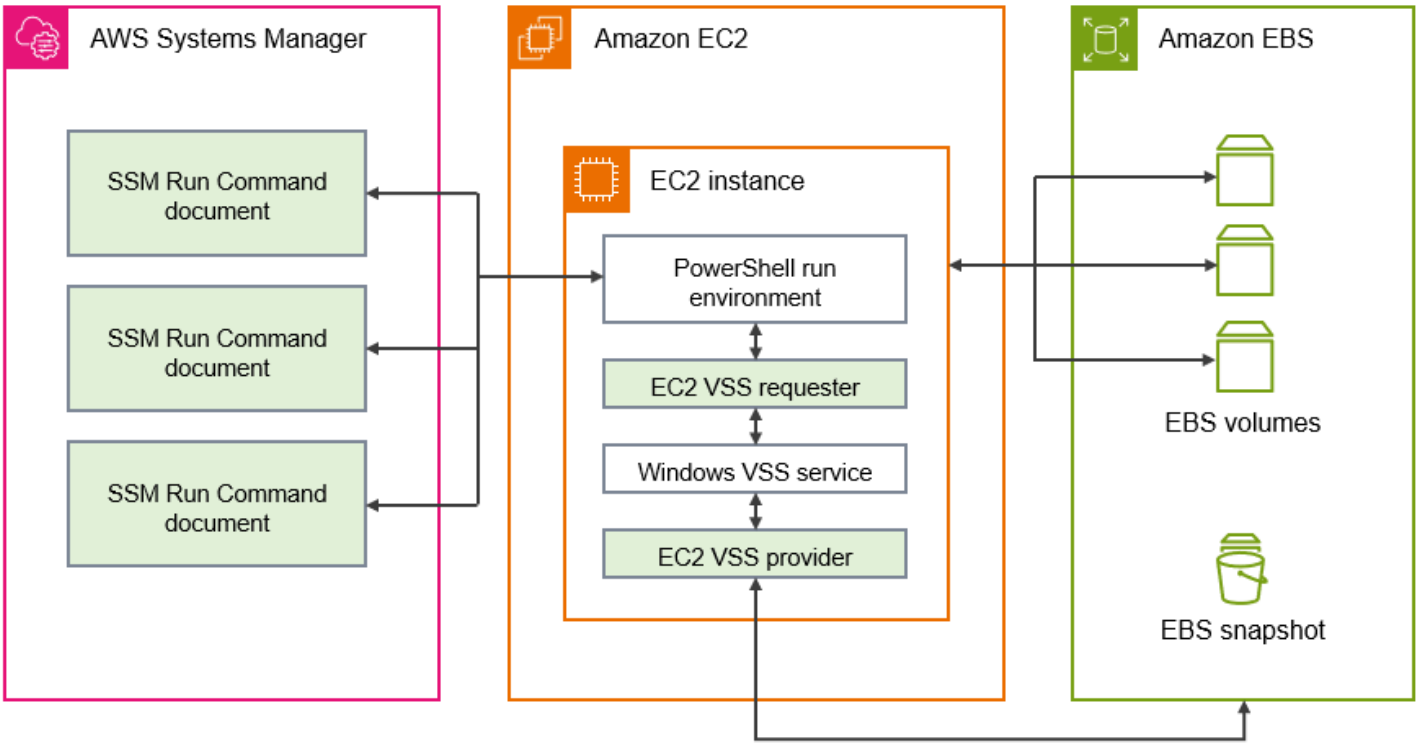
Cos'è VSS?

Volume Snapshot Copy Service (VSS) è una tecnologia di backup e ripristino inclusa in Microsoft Windows. Può creare copie di backup, o snapshot, di file o volumi di computer mentre sono in uso. Per ulteriori informazioni, consulta la pagina Volume Shadow Copy Service.

Per creare uno snapshot coerente con l'applicazione, sono necessari i seguenti componenti software.

- Servizio VSS: parte del sistema operativo Windows
- Richiedente VSS: il software che richiede la creazione di copie shadow
- Scrittore VSS: in genere fornito come parte di un'applicazione, come SQL Server, per garantire la coerenza del set di dati di cui eseguire il backup
- Fornitore VSS: il componente che crea le copie shadow dei volumi sottostanti

La soluzione snapshot Amazon EBS basata su Windows VSS è composta da più documenti Systems Manager (SSM) Run Command che facilitano la creazione di backup e da un pacchetto Systems Manager Distributor, chiamato*`AwsVssComponents`*, che include un richiedente VSS EC2 e un provider VSS EC2. Per acquisire snapshot dei volumi EBS coerenti con l'applicazione, sulle istanze Windows di EC2 deve essere installato il pacchetto `AwsVssComponents`. Il diagramma seguente illustra la relazione tra questi componenti software.



Come funziona la soluzione di snapshot Amazon EBS basata su VSS

Il processo per creare script di snapshot EBS coerenti con l'applicazione e basati su VSS prevede i seguenti passaggi.

1. Completa Prerequisiti.
2. Inserire i parametri per il documento SSM `AWSEC2-VssInstallAndSnapshot` per poi eseguirlo tramite Run Command. Per ulteriori informazioni, consulta Esegui il documento a AWSEC 2 comandi (consigliato) VssInstallAndSnapshot .
3. Il servizio VSS di Windows sull'istanza coordina tutte le operazioni di I/O in corso per l'esecuzione delle applicazioni.
4. Il sistema svuota i buffer di I/O e sospende temporaneamente tutte le operazioni di I/O. La sospensione dura al massimo dieci secondi.
5. In questo lasso di tempo, il sistema crea gli snapshot di tutti i volumi associati all'istanza.
6. Al termine della sospensione, viene recuperata l'operatività di I/O.
7. Il sistema aggiunge tutti gli snapshot appena creati all'elenco degli snapshot di EBS. Il sistema contrassegna tutte le istantanee EBS abilitate per VSS create con successo da questo processo con:true. AppConsistent

8. Se è necessario eseguire il ripristino da uno snapshot, è possibile utilizzare il processo EBS standard di creazione di un volume da uno snapshot. In alternativa, è possibile ripristinare tutti i volumi su un'istanza utilizzando uno script di esempio, illustrato in Ripristino di volumi EBS da snapshot EBS abilitati per VSS.

Prerequisiti

Puoi creare istantanee EBS basate su VSS con Systems Manager Run Command o Amazon Data AWS Backup Lifecycle Manager. I seguenti prerequisiti si applicano a tutte le soluzioni.

Prerequisiti

- Requisiti di sistema
- Autorizzazioni IAM
- Componenti VSS

Requisiti di sistema

Installazione dell'agente Systems Manager

VSS è orchestrato da (Systems AWS Systems Manager Manager) utilizzando. PowerShell Assicurati di aver installato la versione dell'agente SSM `3.0.502.0` o successiva sull'istanza EC2. Se utilizzi una versione obsoleta dell'agente SSM, puoi effettuare l'aggiornamento tramite Run Command. Per ulteriori informazioni, consulta le pagine Setting up Systems Manager for Amazon EC2 instances e Working with SSM Agent on Amazon EC2 instances for Windows Server della Guida per l'utente di AWS Systems Manager .

Requisiti di un'istanza Windows di Amazon EC2

Le istantanee EBS basate su VSS sono supportate per le istanze che eseguono Windows Server 2012 e versioni successive. Per le versioni precedenti di Windows, consulta la tabella di supporto delle versioni di Windows in AWS Cronologia delle versioni della soluzione VSS.

Versione .NET Framework

Il pacchetto `AwsVssComponents` richiede .NET Framework versione `4.6` o successive. Le versioni del sistema operativo Windows precedenti a Windows Server 2016 utilizzano per impostazione predefinita una versione precedente di.NET Framework. Se l'istanza utilizza una versione precedente di.NET Framework, è necessario installare la versione `4.6` o una versione successiva utilizzando Windows Update.

AWS Tools for Windows PowerShell versione

Assicurati che sull'istanza sia in esecuzione AWS Tools for Windows PowerShell la versione `3.3.48.0` o successiva. Per verificare la tua versione, esegui il seguente comando nel PowerShell terminale dell'istanza.

```
C:\> Get-AWSPowerShellVersion
```

Se devi aggiornare AWS Tools for Windows PowerShell la tua istanza, consulta Installazione di AWS Tools for Windows PowerShell nella Guida per l'AWS Tools for Windows PowerShell utente.

PowerShell Versione per Windows

Assicurati che sull'istanza sia in esecuzione la versione PowerShell principale di Windows `3`4, oppure`5`. Per verificare la tua versione, esegui il comando seguente in un PowerShell terminale sull'istanza.

```
C:\> $PSVersionTable.PSVersion
```

PowerShell modalità lingua

Assicurati che la modalità di PowerShell lingua dell'istanza sia impostata su`FullLanguage`. Per ulteriori informazioni, consulta la pagina about_Language_Modes nella documentazione di Microsoft.

Autorizzazioni IAM

Il ruolo IAM collegato alla tua istanza Amazon EC2 Windows deve avere l'autorizzazione a creare snapshot coerenti con l'applicazione con VSS. Per concedere le autorizzazioni necessarie, puoi allegare la policy al profilo della tua istanza. `AWSEC2VssSnapshotPolicy`

La policy consente a Systems Manager di eseguire le seguenti azioni:

- Crea e contrassegna istantanee EBS
- Creare ed etichettare Amazon Machine Images (AMI)
- Allega i metadati, come l'ID del dispositivo, ai tag snapshot predefiniti creati da VSS.

Argomenti

- Allega la policy di snapshot abilitata da VSS al profilo della tua istanza

- Policy gestita per creare istantanee VSS
- Politica precedente (non più supportata)

Allega la policy di snapshot abilitata da VSS al profilo della tua istanza

Per concedere le autorizzazioni per le istantanee abilitate a VSS per la tua istanza, alleghi la policy AWSEC2VssSnapshotPolicy gestita al ruolo del profilo dell'istanza come segue. È importante assicurarsi che l'istanza soddisfi tutti i requisiti. Requisiti di sistema

> **Note**
>
> Per utilizzare la policy gestita, sull'istanza deve essere installata la versione del `AwsVssComponents` pacchetto `2.3.1` o una versione successiva. Per la cronologia delle versioni, consultaAwsVssComponents versioni del pacchetto.
> Se sull'istanza è installata una versione precedente del `AwsVssComponents` pacchetto, consultaPolitica precedente.

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Ruoli per visualizzare un elenco di ruoli IAM a cui hai accesso.
3. Seleziona il link al nome del ruolo associato alla tua istanza. Si apre la pagina dei dettagli del ruolo.
4. Per allegare la policy gestita, scegli Aggiungi autorizzazioni, che si trova nell'angolo in alto a destra del pannello dell'elenco. Quindi seleziona Allega politiche dall'elenco a discesa.
5. Per semplificare i risultati, inserisci il nome della policy nella barra di ricerca ()`AWSEC2VssSnapshotPolicy`.
6. Seleziona la casella di controllo accanto al nome della politica da allegare e scegli Aggiungi autorizzazioni.

Policy gestita per creare istantanee VSS

Una politica AWS gestita è una politica autonoma che Amazon fornisce ai AWS clienti. AWS le politiche gestite sono progettate per concedere autorizzazioni per casi d'uso comuni. Non è possibile modificare le autorizzazioni definite nelle politiche AWS gestite. Tuttavia, puoi copiare la policy e utilizzarla come base per una policy gestita dai clienti specifica per il tuo caso d'uso.

Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella Guida per l'utente IAM.

Per utilizzare la AWSEC2VssSnapshotPolicypolicy, la policy gestita, puoi collegarla al ruolo IAM collegato alle tue istanze EC2 Windows. Questa policy consente alla soluzione VSS EC2 di creare e aggiungere tag ad Amazon Machine Images (AMI) e agli snapshot EBS. Per allegare la policy, consulta. Allega la policy di snapshot abilitata da VSS al profilo della tua istanza

Autorizzazioni concesse da AWSEC2VssSnapshotPolicy

La AWSEC2VssSnapshotPolicypolicy include le seguenti autorizzazioni Amazon EC2:

- ec2: CreateTags — Aggiungi tag agli snapshot e alle AMI EBS per identificare e classificare le risorse.
- ec2: DescribeInstanceAttribute — Recupera i volumi EBS e le corrispondenti mappature dei dispositivi a blocchi collegati all'istanza di destinazione.
- ec2: CreateSnapshots — Crea istantanee dei volumi EBS.
- ec2: CreateImage — Crea un AMI da un'istanza EC2 in esecuzione.
- ec2: DescribeImages — Recupera le informazioni per le AMI e le istantanee EC2.
- ec2: DescribeSnapshots — Determina l'ora e lo stato di creazione delle istantanee per verificare la coerenza dell'applicazione.

Esempio di politica

Di seguito è riportato un esempio della AWSEC2VssSnapshotPolicy policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DescribeInstanceInfo",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstanceAttribute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
```

```
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AwsVssConfig": "*"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsAccessInstance",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsAccessVolume",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
```

```
        {
            "Sid": "CreateImageWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AwsVssConfig": "*"
                }
            }
        },
        {
            "Sid": "CreateImageAccessInstance",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateTagsOnResourceCreation",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateImage",
                        "CreateSnapshots"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "CreateTagsAfterResourceCreation",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/AwsVssConfig": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AppConsistent",
                        "Device"
                    ]
                }
            }
        },
        {
            "Sid": "DescribeImagesAndSnapshots",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Semplifica le autorizzazioni per casi d'uso specifici (avanzato)

La policy `AWSEC2VssSnapshotPolicy` gestita include le autorizzazioni per tutti i modi in cui è possibile creare istantanee abilitate per VSS. È possibile creare una politica personalizzata che includa solo le autorizzazioni necessarie.

Caso d'uso: creazione di AMI, caso d'uso: AWS Backup servizio di utilizzo

Se si utilizza esclusivamente l'`CreateAmi`opzione o se si creano istantanee abilitate per VSS solo tramite il AWS Backup servizio, è possibile semplificare le dichiarazioni politiche come segue.

- Omettete le dichiarazioni politiche identificate dai seguenti ID di dichiarazione (SID):
  - `CreateSnapshotsWithTag`
  - `CreateSnapshotsAccessInstance`
  - `CreateSnapshotsAccessVolume`
- Modificate la `CreateTagsOnResourceCreation` dichiarazione come segue:
  - Rimuovi `arn:aws:ec2:*:*:snapshot/*` dalle risorse.
  - Rimuovi `CreateSnapshots` dalla `ec2:CreateAction` condizione.
- Modifica l'`CreateTagsAfterResourceCreation`istruzione per rimuoverla `arn:aws:ec2:*:*:snapshot/*` dalle risorse.
- Modifica l'`DescribeImagesAndSnapshots`istruzione per rimuoverla `ec2:DescribeSnapshots` dall'azione dell'istruzione.

Caso d'uso: solo snapshot

Se non si utilizza l'`CreateAmi`opzione, è possibile semplificare le dichiarazioni politiche come segue.

- Omettete le dichiarazioni politiche identificate dai seguenti ID di dichiarazione (SID):
  - `CreateImageAccessInstance`
  - `CreateImageWithTag`
- Modificate la `CreateTagsOnResourceCreation` dichiarazione come segue:
  - Rimuovi `arn:aws:ec2:*:*:image/*` dalle risorse.
  - Rimuovi `CreateImage` dalla `ec2:CreateAction` condizione.
- Modifica l'`CreateTagsAfterResourceCreation`istruzione per rimuoverla `arn:aws:ec2:*:*:image/*` dalle risorse.
- Modifica l'`DescribeImagesAndSnapshots`istruzione per rimuoverla `ec2:DescribeImages` dall'azione dell'istruzione.

> **Note**
>
> Per garantire che la politica personalizzata funzioni come previsto, si consiglia di rivedere e incorporare regolarmente gli aggiornamenti alla politica gestita.

Politica precedente (non più supportata)

La policy legacy che concede l'autorizzazione per le istantanee abilitate a VSS include le autorizzazioni IAM consigliate prima del rilascio della policy gestita. `AWSEC2VssSnapshotPolicy`

Se hai configurato un ruolo di istanza con la policy legacy, puoi continuare a utilizzarlo. Tuttavia, per garantire che la tua policy rimanga aggiornata con le più recenti best practice di IAM e applichi di conseguenza le dichiarazioni sulle policy, ti consigliamo di sostituire la policy legacy con la policy `AWSEC2VssSnapshotPolicy` gestita.

Esempio di policy

Il seguente esempio di policy utilizza `ec2:DescribeInstanceAttribute` ciò che è supportato nelle versioni `AwsVssComponents` del pacchetto 2.2.1 e successive. Se è installata una versione precedente del `AwsVssComponents` pacchetto, è necessario sostituirla con l'`ec2:DescribeInstances`azione.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ec2:CreateTags",
   "Resource": [
    "arn:aws:ec2:*::snapshot/*",
    "arn:aws:ec2:*::image/*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstanceAttribute",
    "ec2:CreateSnapshot",
    "ec2:CreateSnapshots",
    "ec2:CreateImage",
```

```
    "ec2:DescribeImages",
    "ec2:DescribeSnapshots"
   ],
   "Resource": "*"
  }
 ]
}
```

Per ulteriori informazioni sulle policy gestite da IAM, consulta le policy AWS gestite nella IAM User Guide.

Componenti VSS

Per creare snapshot coerenti a livello di applicazione sui sistemi operativi Windows, il pacchetto `AwsVssComponents` deve essere installato nell'istanza. Il pacchetto contiene un agente VSS su istanza EC2 che funge da richiedente VSS e un fornitore VSS di EC2 per i volumi EBS.

È possibile installare il componente in un'istanza esistente in diversi modi:

- (Consigliato) Esegui il documento a AWSEC 2 comandi (consigliato) VssInstallAndSnapshot . In questo modo il componente si installa o si aggiorna automaticamente a ogni esecuzione.
- Installazione manuale dei componenti VSS su un'istanza.
- Aggiornamento dei componenti VSS sulle istanze in una pianificazione.

È anche possibile creare un'AMI con EC2 Image Builder che utilizzi il componente gestito `aws-vss-components-windows` per installare il pacchetto `AwsVssComponents` per l'immagine. Il componente gestito utilizza AWS Systems Manager Distributor per installare il pacchetto. Dopo la creazione dell'immagine con Image Builder, ogni istanza avviata dall'AMI associata avrà il pacchetto VSS installato. Per ulteriori informazioni su come creare un'AMI con installato il pacchetto VSS, consulta Distributor package managed components for Windows nella Guida per l'utente di EC2 Image Builder.

Indice

Installazione manuale dei componenti VSS su un'istanza

L'istanza Windows di EC2 deve avere installati i componenti VSS prima di poter creare snapshot coerenti a livello di applicazione con Systems Manager. Se non si esegue il documento di comando `AWSEC2-VssInstallAndSnapshot` per installare o aggiornare il pacchetto ogni volta che si creano snapshot coerenti a livello di applicazione, è necessario installare manualmente il pacchetto.

È necessario eseguire l'installazione manuale anche se si prevede di utilizzare uno dei seguenti metodi per creare snapshot coerenti a livello di applicazione dall'istanza EC2.

- Crea istantanee VSS utilizzando AWS Backup
- Creazione di snapshot VSS mediante Amazon Data Lifecycle Manager

Se devi eseguire un'installazione manuale, ti consigliamo di utilizzare il pacchetto di componenti AWS VSS più recente per migliorare l'affidabilità e le prestazioni delle istantanee coerenti con le applicazioni sulle istanze EC2 Windows.

> **Note**
>
> Per installare o aggiornare automaticamente il pacchetto `AwsVssComponents` ogni volta che si creano snapshot coerenti con l'applicazione, si consiglia di utilizzare Systems Manager per eseguire il documento `AWSEC2-VssInstallAndSnapshot`. Per ulteriori informazioni, consulta Esegui il documento a AWSEC 2 comandi (consigliato) VssInstallAndSnapshot .

Per installare i componenti VSS su un'istanza Windows di Amazon EC2, segui i passaggi per il tuo ambiente preferito.

Console

Installazione dei componenti VSS utilizzando SSM Distributor

1. Apri la console all'indirizzo https://console.aws.amazon.com/systems-manager/. AWS Systems Manager
2. Nel riquadro di navigazione selezionare Run Command.
3. Selezionare Run command.
4. Per il documento Command, scegli il pulsante accanto a AWS-Configure AWSPackage.
5. In Command parameters (Parametri di comando), effettuare le seguenti operazioni:

a. Verificare che Action (Operazione) sia impostata su Install (Installa).

b. In Name (Nome), immettere `AwsVssComponents`.

c. In Versione, lascia vuoto il campo per consentire a Systems Manager di installare l'ultima versione.

6. In Targets (Destinazioni), identificare le istanze in cui si desidera eseguire questa operazione specificando i tag o selezionando le istanze manualmente.

> **Note**
>
> Se scegli di selezionare manualmente le istanze e l'istanza prevista non è inclusa nell'elenco, consulta Dove sono le mie istanze? nella Guida per l'utente di AWS Systems Manager per suggerimenti sulla risoluzione dei problemi.

7. In Other parameters (Altri parametri):

- (Opzionale) In Comment (Commento) digitare le informazioni su questo comando.
- In Timeout (seconds) (Timeout [secondi]), specificare il numero di secondi che il sistema dovrà aspettare prima di generare un errore per l'intera esecuzione del comando.

8. (Facoltativo) In Rate control (Controllo velocità):

- In Concurrency (Simultaneità), specificare un numero o una percentuale di istanze su cui eseguire contemporaneamente il comando.

> **Note**
>
> Se le destinazioni sono state selezionate scegliendo i tag Amazon EC2 e non si conosce il numero di istanze utilizzate dai tag selezionati, limitare il numero di istanze che possono eseguire il documento contemporaneamente specificando una percentuale.

- In Error threshold (Soglia di errore) specificare quando interrompere l'esecuzione del comando sulle altre istanze dopo un errore su un numero o una percentuale di istanze. Se ad esempio si specificano 3 errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche le istanze che elaborano ancora il comando potrebbero inviare errori.

9. (Opzionale) Nella sezione Output options (Opzioni di output), se si desidera salvare l'output del comando in un file, selezionare la casella accanto a Enable writing to an S3 bucket (Abilita la scrittura in un bucket S3). Specificare i nomi del bucket e (opzionale) del prefisso (cartella).

   > **Note**
   >
   > Le autorizzazioni S3 che assegnano la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza e non quelle dell'utente che esegue questa attività. Per ulteriori informazioni, consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager .

10. (Opzionale) Specificare le opzioni per SNS notifications (Notifiche SNS).

    Per informazioni sulla configurazione di notifiche Amazon SNS per Run Command, consultare Configurazione delle notifiche Amazon SNS per AWS Systems Manager.

11. Seleziona Esegui.

AWS CLI

La seguente procedura consente di scaricare e installare il pacchetto `AwsVssComponents` sulle istanze utilizzando Run Command da AWS CLI. Il pacchetto installa due componenti: un richiedente VSS e un provider VSS. Il sistema copia questi componenti su una directory dell'istanza, poi registra il DLL del provider come provider VSS.

Per installare il pacchetto VSS utilizzando il AWS CLI

- Esegui il comando seguente per scaricare e installare i componenti VSS necessari per Systems Manager.

```
aws ssm send-command \
  --document-name "AWS-ConfigureAWSPackage" \
  --instance-ids "i-01234567890abcdef" \
  --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Utilizzare la procedura seguente per scaricare e installare il `AwsVssComponents` pacchetto sulle istanze utilizzando Esegui comando dagli strumenti per Windows. PowerShell Il pacchetto installa due componenti: un richiedente VSS e un provider VSS. Il sistema copia questi componenti su una directory dell'istanza, poi registra il DLL del provider come provider VSS.

Per installare il pacchetto VSS utilizzando il AWS Tools for Windows PowerShell

- Esegui il comando seguente per scaricare e installare i componenti VSS necessari per Systems Manager.

```
Send-SSMCommand -DocumentName AWS-ConfigureAWSPackage -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'action'='Install';'name'='AwsVssComponents'}
```

Verificare la firma sui componenti AWS VSS

Utilizza la procedura seguente per verificare la firma sul pacchetto `AwsVssComponents`.

1. Connettersi all'istanza Windows. Per ulteriori informazioni, consulta Connettiti all'istanza Windows .
2. Vai a C:\Program Files\ Amazon\AwsVssComponents.
3. Apri il menu contestuale (tasto destro del mouse) di `ec2-vss-agent.exe`, quindi seleziona Proprietà.
4. Vai alla scheda Firme digitali e verifica che il nome del firmatario sia Amazon Web Services Inc.
5. Utilizza i passaggi precedenti per verificare la firma su `Ec2VssInstaller` e `Ec2VssProvider.dll`.

Aggiornamento dei componenti VSS sulle istanze in una pianificazione

Ti consigliamo di mantenere sempre aggiornato il componente VSS all'ultima versione consigliata. Quando viene rilasciata una nuova versione del pacchetto `AwsVssComponents`, è possibile aggiornare i componenti in diversi modi.

Metodi di aggiornamento

- È possibile ripetere i passaggi descritti in Installazione manuale dei componenti VSS su un'istanza Quando viene rilasciata una nuova versione dei componenti AWS VSS.
- È possibile configurare un'associazione State Manager di Systems Manager per scaricare e installare automaticamente nuovi componenti VSS quando il pacchetto `AwsVssComponents` diventa disponibile.
- Quando si utilizza Systems Manager per eseguire il documento `AWSEC2-VssInstallAndSnapshot`, è possibile installare o aggiornare automaticamente il pacchetto `AwsVssComponents` ogni volta che si creano snapshot coerenti con l'applicazione.

> **Note**
>
> Consigliamo di utilizzare Systems Manager per eseguire il documento del comando `AWSEC2-VssInstallAndSnapshot` che installa o aggiorna automaticamente il pacchetto `AwsVssComponents` prima di creare gli snapshot coerenti con l'applicazione. Per ulteriori informazioni, consulta Esegui il documento a AWSEC 2 comandi (consigliato) VssInstallAndSnapshot .

Per creare un'associazione Systems Manager State Manager, completa le operazioni per il tuo ambiente preferito.

Console

Creazione di un'associazione di State Manager utilizzando la console

1. Aprire la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, seleziona State Manager.

   Oppure, se la home page di Systems Manager si apre per prima, apri il riquadro di navigazione e scegli State Manager.
3. Selezionare Create association (Crea associazione).
4. Nel campo Name (Nome), immettere un nome descrittivo.
5. Nell'elenco Documento, scegli AWS-Configure AWSPackage.

6. Nella sezione Parameters (Parametri), scegliere Install (Installa) dall'elenco di operazioni.
7. In Installation type (Tipo di installazione), scegliere Uninstall and reinstall (Disinstalla e reinstalla).
8. Nel campo Name (Nome), inserire `AwsVssComponents`. Puoi mantenere vuoti i campi Version (Versione) e Additional Arguments (Argomenti aggiuntivi).
9. Nella sezione Targets (Destinazioni), scegliere un'opzione.

> **Note**
>
> Se si sceglie di definire come target le istanze mediante i tag e si specificano tag che mappano per istanze di Linux, l'associazione va a buon fine sull'istanza di Windows, ma non sulle istanze di Linux. Lo stato globale dell'associazione mostra Failed (Non riuscito).

10. Scegliere una tra le opzioni disponibili in Specify schedule (Specifica la pianificazione).
11. Nella sezione Advanced options (Opzioni avanzate), per Compliance severity (Gravità conformità), scegliere un livello di gravità per l'associazione. Per ulteriori informazioni, consulta la pagina About State Manager association compliance. In Calendari di modifica, seleziona un calendario di modifica preconfigurato. Per ulteriori informazioni, consulta la pagina AWS Systems Manager Change Calendar.
12. In Controllo della velocità, procedi come segue:
    - In Concurrency (Simultaneità), specificare un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.
    - Per Error threshold (Soglia di errore) specificare quando interrompere l'esecuzione del comando sulle altri nodi gestiti dopo un errore su un numero o una percentuale di nodi.
13. (Facoltativo) In Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Abilita scrittura dell'output in S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.
14. Selezionare Create association (Crea associazione), poi Close (Chiudi). Il sistema tenta di creare l'associazione sulle istanze e di applicare immediatamente lo stato.

> **Note**
>
> Se le istanze EC2 per Windows Server mostrano lo stato Failed, verifica che l'agente SSM sia in esecuzione sull'istanza e verifica che l'istanza sia configurata con un ruolo

AWS Identity and Access Management (IAM) per Systems Manager. Per ulteriori informazioni, consulta Configurazione. AWS Systems Manager

AWS CLI

È possibile eseguire il AWS CLI comando create-association per aggiornare un pacchetto Distributor in base a una pianificazione senza mettere offline l'applicazione associata. Vengono sostituiti solo i file nuovi o aggiornati nel pacchetto.

Per creare un'associazione State Manager utilizzando il AWS CLI

1. Installa e configura AWS CLI, se non l'hai già fatto. Per informazioni, consulta la pagina Install or update the latest version of the AWS CLI.
2. Esegui il comando seguente per creare un'associazione. Il valore `--name`, ossia il nome del documento, è sempre `AWS-ConfigureAWSPackage`. Il comando seguente utilizza la chiave `InstanceIds` per specificare le istanze di destinazione.

```
aws ssm create-association \
 --name "AWS-ConfigureAWSPackage" \
 --parameters '{"action":["Install"],"installationType":["Uninstall and
 reinstall"],"name":["AwsVssComponents"]}' \
 --targets [{\"Key\":\"InstanceIds\",\"Values\":[\"i-01234567890abcdef\",
\"i-000011112222abcde\"]}]
```

Per informazioni sulle altre opzioni che è possibile utilizzare con il `create-association` comando, consulta create-association nella AWS Systems Manager sezione del AWS CLI Command Reference.

Creazione di snapshot EBS con tecnologia VSS

In questa sezione viene descritto come creare snapshot EBS abilitati per VSS.

È possibile creare snapshot EBS abilitati per VSS dei volumi EBS collegati alle istanze EC2. Prima di provare a creare uno snapshot abilitato per VSS, assicurati che i Prerequisiti siano soddisfatti.

Argomenti

- Creazione di snapshot VSS con documenti di comando AWS Systems Manager

- Crea istantanee VSS utilizzando AWS Backup
- Creazione di snapshot VSS mediante Amazon Data Lifecycle Manager

Creazione di snapshot VSS con documenti di comando AWS Systems Manager

È possibile utilizzare i documenti di AWS Systems Manager comando per creare istantanee compatibili con VSS. Il seguente contenuto introduce i documenti di comando disponibili e i parametri di runtime utilizzati dai documenti per creare gli snapshot.

Prima di utilizzare uno dei documenti di comando di Systems Manager, assicurati di aver soddisfatto tutti i Prerequisiti.

Argomenti

- Parametri per i documenti Systems Manager per snapshot VSS
- Esecuzione dei documenti di comando Systems Manager per snapshot VSS

Parametri per i documenti Systems Manager per snapshot VSS

I documenti Systems Manager che creano snapshot VSS utilizzano tutti i seguenti parametri, eccetto dove segnalato:

ExcludeBootVolume(stringa, opzionale)

Questa impostazione esclude i volumi di avvio dal processo di backup se si creano snapshot. Per escludere i volumi di avvio dalle istantanee, imposta ExcludeBootVolumesu `True` e CreateAmisu`False`.

Se si crea un'AMI per il backup, questo parametro deve essere impostato su `False`. Il valore predefinito per questo parametro è `False`.

NoWriters(stringa, opzionale)

Per escludere i writer VSS dell'applicazione dal processo di snapshot, imposta questo parametro su`True`. L'esclusione dei writer VSS dell'applicazione può aiutarti a risolvere i conflitti con componenti di backup VSS di terze parti. Il valore predefinito per questo parametro è `False`.

CopyOnly(stringa, opzionale)

Se si utilizza il backup nativo di SQL Server oltre a AWS VSS, l'esecuzione di un backup di sola copia impedisce a AWS VSS di interrompere la catena di backup differenziale nativa. Per eseguire un'operazione di backup di sola copia, imposta questo parametro su `True`.

Il valore predefinito per questo parametro è`False`, che fa sì che AWS VSS esegua un'operazione di backup completa.

CreateAmi(stringa, opzionale)

Per creare un'Amazon Machine Image (AMI) abilitata per VSS per il backup dell'istanza, imposta questo parametro su `True`. Il valore predefinito per questo parametro è `False`, che esegue invece il backup dell'istanza con uno snapshot EBS.

Per ulteriori informazioni sulla creazione di un'AMI da un'istanza, consulta la pagina Crea un'AMI supportata da Amazon EBS.

AmiName(stringa, opzionale)

Se l'CreateAmiopzione è impostata su`True`, specifica il nome dell'AMI creato dal backup.

description (stringa, facoltativo)

Specifica una descrizione per gli snapshot o l'immagine creata da questo processo.

tags (stringa, facoltativo)

Si consiglia di etichettare le istantanee e le immagini per facilitare l'individuazione e la gestione delle risorse, ad esempio per ripristinare i volumi da un elenco di istantanee. Il sistema aggiunge la `Name` chiave, con un valore vuoto in cui è possibile specificare il nome che si desidera applicare alle istantanee o alle immagini di output.

Se desideri specificare tag aggiuntivi, separali con un punto e virgola in mezzo. Ad esempio, `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

Per impostazione predefinita, il sistema aggiunge i seguenti tag riservati per istantanee e immagini compatibili con VSS.

- Dispositivo: per le istantanee abilitate per VSS, questo è il nome del dispositivo del volume EBS acquisito dall'istantanea.
- AppConsistent— Questo tag indica la corretta creazione di un'istantanea o di un AMI abilitato per VSS.
- AwsVssConfig— Identifica le istantanee e le AMI create con VSS abilitato. Il tag include meta-informazioni come la versione. `AwsVssComponents`

> **Warning**
>
> La specificazione di uno di questi tag riservati nell'elenco dei parametri causerà un errore.

executionTimeout (stringa, facoltativo)

Specifica il tempo massimo in secondi per eseguire il processo di creazione degli snapshot sull'istanza o per creare un'AMI dall'istanza. L'aumento di questo timeout consente al comando di attendere più a lungo l'avvio del blocco da parte di VSS e di completare il tagging delle risorse create. Questo timeout si applica solo alle fasi di creazione degli snapshot o dell'AMI. Il passaggio iniziale per installare o aggiornare il pacchetto `AwsVssComponents` non è incluso nel timeout.

CollectDiagnosticLogs(stringa, opzionale)

Per raccogliere ulteriori informazioni durante le fasi di creazione di istantanee e AMI, imposta questo parametro su "`True`». Il valore predefinito per questo parametro è "`False`». I log di diagnostica consolidati vengono salvati come archivio in `.zip` formato nella seguente posizione sull'istanza:

`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`

VssVersion(stringa, opzionale)

Solo per il documento `AWSEC2-VssInstallAndSnapshot`, puoi specificare il parametro `VssVersion` per installare una versione specifica del pacchetto `AwsVssComponents` sull'istanza. Lascia vuoto questo parametro per installare la versione predefinita consigliata.

Se la versione specificata del pacchetto `AwsVssComponents` è già installata, lo script salta la fase di installazione e passa alla fase di backup. Per un elenco delle versioni del pacchetto `AwsVssComponents` e del supporto operativo, consulta AWS Cronologia delle versioni della soluzione VSS.

Esecuzione dei documenti di comando Systems Manager per snapshot VSS

È possibile creare istantanee EBS compatibili con VSS con AWS Systems Manager documenti di comando come segue.

Esegui il documento a AWSEC 2 comandi (consigliato) VssInstallAndSnapshot

Quando si utilizza AWS Systems Manager per eseguire il `AWSEC2-VssInstallAndSnapshot` documento, lo script esegue i seguenti passaggi.

1. Lo script installa o aggiorna innanzitutto il pacchetto `AwsVssComponents` sull'istanza, a seconda che sia già installato.

2. Lo script crea snapshot coerenti con l'applicazione dopo il completamento del primo passaggio.

Per eseguire il documento `AWSEC2-VssInstallAndSnapshot`, segui i passaggi relativi al tuo ambiente preferito.

Console

Creazione di snapshot EBS abilitati per VSS dalla console

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, seleziona Esegui comando. Questo mostra un elenco di comandi correntemente in esecuzione nel tuo account, se applicabile.
3. Seleziona Run command (Esegui comando). Si apre un elenco di documenti di comando a cui si ha accesso.
4. Seleziona `AWSEC2-VssInstallAndSnapshot` dall'elenco dei documenti di comando. Per semplificare i risultati, puoi inserire tutto o parte del nome del documento. Puoi anche filtrare per proprietario, per tipo di piattaforma o per tag.

   Quando si seleziona un documento di comando, i dettagli vengono inseriti sotto l'elenco.
5. Seleziona `Default version at runtime` dall'elenco delle versioni del documento.
6. Configura i parametri del comando per definire come `AWSEC2-VssInstallAndSnapshot` installerà il pacchetto `AwsVssComponents` ed eseguire il backup con snapshot VSS o un'AMI. Per i dettagli dei parametri, consulta Parametri per i documenti Systems Manager per snapshot VSS.
7. In Selezione della destinazione, specifica i tag o seleziona manualmente le istanze per identificare le istanze su cui eseguire questa operazione.

   > **Note**
   >
   > Se selezioni manualmente le istanze e l'istanza prevista non è inclusa nell'elenco, consulta Dove sono le mie istanze? per suggerimenti sulla risoluzione dei problemi.
8. Per i parametri aggiuntivi per la definizione del comportamento dei comandi di esecuzione di Systems Manager, ad esempio il controllo della velocità, immetti i valori come descritto in Esecuzione di comandi dalla console.

9. Selezionare Run (Esegui).

   In caso di esito positivo, il comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco degli snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando di Systems Manager. Nel caso in cui l'esecuzione del comando risulti completata con successo, ma non sia riuscito il backup di un determinato volume, è possibile risolvere il problema dall'elenco dei volumi EBS.

AWS CLI

Puoi eseguire i seguenti comandi in AWS CLI per creare istantanee EBS abilitate per VSS e ottenere lo stato della creazione delle istantanee.

Creazione di snapshot EBS con tecnologia VSS

Esegui il comando seguente per creare snapshot EBS con tecnologia VSS. Per creare gli snapshot, devi identificare le istanze con il parametro `--instance-ids`. Per ulteriori informazioni sugli altri parametri che è possibile utilizzare, consulta Parametri per i documenti Systems Manager per snapshot VSS.

```
aws ssm send-command \
 --document-name "AWSEC2-VssInstallAndSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

In caso di esito positivo, il documento di comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco degli snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando.

Ottenere lo stato del comando

Per ottenere lo stato corrente degli snapshot, esegui il comando riportato utilizzando l'ID del comando restituito da send-command.

```
aws ssm get-command-invocation
 --instance-ids "i-01234567890abcdef" \
```

```
 --command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
 --plugin-name "CreateVssSnapshot"
```

PowerShell

Esegui i seguenti comandi con AWS Tools for Windows PowerShell per creare istantanee EBS abilitate per VSS e ottenere lo stato di runtime corrente per la creazione dell'output. Specifica i parametri descritti nell'elenco precedente per modificare il comportamento del processo di snapshot.

Crea istantanee EBS compatibili con VSS con Tools for Windows PowerShell

Esegui il comando riportato per creare snapshot EBS abilitati per VSS o AMI.

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Ottenere lo stato del comando

Per ottenere lo stato corrente degli snapshot, esegui il comando riportato utilizzando l'ID del comando restituito da Send-SSMCommand.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId
 "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

In caso di esito positivo, il comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco degli snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando.

Esegui il documento a 2 comandi AWSEC CreateVssSnapshot

Per eseguire il documento `AWSEC2-CreateVssSnapshot`, segui i passaggi relativi al tuo ambiente preferito.

Console

Creazione di snapshot EBS abilitati per VSS dalla console

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, seleziona Esegui comando. Questo mostra un elenco di comandi correntemente in esecuzione nel tuo account, se applicabile.
3. Seleziona Run command (Esegui comando). Si apre un elenco di documenti di comando a cui si ha accesso.
4. Seleziona `AWSEC2-CreateVssSnapshot` dall'elenco dei documenti di comando. Per semplificare i risultati, puoi inserire tutto o parte del nome del documento. Puoi anche filtrare per proprietario, per tipo di piattaforma o per tag.

   Quando si seleziona un documento di comando, i dettagli vengono inseriti sotto l'elenco.
5. Seleziona `Default version at runtime` dall'elenco delle versioni del documento.
6. Configura i parametri del comando per definire come `AWSEC2-CreateVssSnapshot` eseguirà il backup con snapshot VSS o un'AMI. Per i dettagli dei parametri, consulta Parametri per i documenti Systems Manager per snapshot VSS.
7. In Selezione della destinazione, specifica i tag o seleziona manualmente le istanze per identificare le istanze su cui eseguire questa operazione.

   > **Note**
   >
   > Se selezioni manualmente le istanze e l'istanza prevista non è inclusa nell'elenco, consulta Dove sono le mie istanze? per suggerimenti sulla risoluzione dei problemi.
8. Per i parametri aggiuntivi per la definizione del comportamento dei comandi di esecuzione di Systems Manager, ad esempio il controllo della velocità, immetti i valori come descritto in Esecuzione di comandi dalla console.
9. Selezionare Run (Esegui).

   In caso di esito positivo, il comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco degli snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando di Systems Manager. Nel caso in cui

l'esecuzione del comando risulti completata con successo, ma non sia riuscito il backup di un determinato volume, è possibile risolvere il problema dall'elenco dei volumi EBS.

AWS CLI

Puoi eseguire il seguente comando in AWS CLI per creare istantanee EBS abilitate per VSS.

Creazione di snapshot EBS con tecnologia VSS

Esegui il comando seguente per creare snapshot EBS con tecnologia VSS. Per creare gli snapshot, devi identificare le istanze con il parametro `--instance-ids`. Per ulteriori informazioni sugli altri parametri che è possibile utilizzare, consulta Parametri per i documenti Systems Manager per snapshot VSS.

```
aws ssm send-command \
 --document-name "AWSEC2-CreateVssSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"]}'
```

In caso di esito positivo, il documento di comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco degli snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando.

PowerShell

Esegui il seguente comando con per creare istantanee EBS abilitate AWS Tools for Windows PowerShell per VSS.

Crea istantanee EBS abilitate per VSS con Tools for Windows PowerShell

Esegui il comando seguente per creare snapshot EBS con tecnologia VSS. Per creare gli snapshot, devi identificare le istanze con il parametro `InstanceId`. È possibile specificare più di un'istanza per cui creare snapshot. Per ulteriori informazioni sugli altri parametri che è possibile utilizzare, consulta Parametri per i documenti Systems Manager per snapshot VSS.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value'}
```

In caso di esito positivo, il comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco degli snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando. Nel caso in cui l'esecuzione del comando risulti completata con successo, ma non sia riuscito il backup di un determinato volume, è possibile risolvere il problema dall'elenco degli snapshot EBS.

Esecuzione dei documenti di comando per un cluster di failover Windows con archiviazione EBS condivisa

È possibile utilizzare una qualsiasi delle procedure della linea di comando descritte nella sezione precedente per creare uno snapshot abilitato per VSS. Il documento del comando (`AWSEC2-VssInstallAndSnapshot` o `AWSEC2-CreateVssSnapshot`) deve essere eseguito sul nodo primario del cluster. Il documento avrà esito negativo sui nodi secondari in quanto non hanno accesso ai dischi condivisi. Se il primario e il secondario cambiano dinamicamente, puoi AWS Systems Manager eseguire il documento Run Command su più nodi con l'aspettativa che il comando abbia esito positivo sul nodo primario e abbia esito negativo sui nodi secondari.

Esegui il documento di comando AWSEC ManageVss 2-IO SSM

Con il seguente script e il documento predefinito SSM `AWSEC2-ManageVssIO` è possibile sospendere temporaneamente le operazioni di I/O, creare snapshot EBS con tecnologia VSS e riavviare le operazioni di I/O. Questo processo si verifica nel contesto dell'utente che esegue il comando. Se l'utente dispone di autorizzazioni sufficienti per creare e contrassegnare istantanee, AWS Systems Manager può creare e taggare istantanee EBS abilitate per VSS senza la necessità del ruolo aggiuntivo di snapshot IAM sull'istanza.

Al contrario, il documento del comando (`AWSEC2-VssInstallAndSnapshot` o `AWSEC2-CreateVssSnapshot`) richiede di assegnare il ruolo di snapshot IAM a ogni istanza per cui si intende creare snapshot EBS. Se non si desidera fornire ulteriori autorizzazioni IAM alle istanze per motivi di conformità o di policy, ci si può avvalere del seguente script.

Prima di iniziare

Tieni presenti queste importanti informazioni relative a questo processo:

- Questo processo utilizza uno PowerShell script (`CreateVssSnapshotAdvancedScript.ps1`) per scattare istantanee di tutti i volumi sulle istanze specificate, ad eccezione dei volumi root.

Per acquisire snapshot di volumi root, è necessario utilizzare il documento SSM `AWSEC2-CreateVssSnapshot`.

- Lo script chiama il documento `AWSEC2-ManageVssIO` due volte. La prima volta, con il parametro `Action` impostato su `Freeze`, che sospende tutte le attività di I/O sulle istanze. La seconda volta, il parametro `Action` è impostato su `Thaw`, che forza la ripresa delle attività di I/O.
- Non tentate di utilizzare il `AWSEC2-ManageVssIO` documento senza utilizzare lo CreateVssSnapshotAdvancedScript script.ps1. Il framework VSS di Microsoft prevede che le operazioni `Freeze` e `Thaw` vengano chiamate a non più di dieci secondi di distanza; la chiamata manuale di tali operazioni senza lo script potrebbe generare errori.

Come creare snapshot EBS con tecnologia VSS avvalendosi del documento **`AWSEC2-ManageVssIO`**

1. Scarica il CreateVssSnapshotAdvancedScriptfile.zip ed estrai il contenuto del file.
2. Apri `CreateVssSnapshotAdvancedScript.ps1` in un editor di testo, modifica la chiamata di esempio nella parte inferiore dello script con un ID di istanza EC2 valido, una descrizione dell'istantanea e i valori dei tag desiderati, quindi esegui lo script da. PowerShell

In caso di esito positivo, il comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco degli snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando. Nel caso in cui l'esecuzione del comando sia stata completata con successo, ma non sia riuscito il backup di un determinato volume, è possibile risolvere il problema dall'elenco dei volumi EBS.

> **Note**
>
> Per automatizzare i backup, puoi creare un'attività della finestra di AWS Systems Manager manutenzione che utilizzi il documento. `AWSEC2-VssInstallAndSnapshot` Per ulteriori informazioni, consulta Utilizzo delle finestre di manutenzione (console) nella Guida per l'utente di AWS Systems Manager .

Crea istantanee VSS utilizzando AWS Backup

È possibile creare un backup VSS quando si utilizza AWS Backup abilitando VSS nella console o nella CLI. Assicurati di aver soddisfatto i prerequisiti prima di creare il piano di backup abilitato per

VSS. Per ulteriori informazioni, consulta la pagina Creating Windows VSS backups della Guida per gli sviluppatori di AWS Backup .

> **Note**
>
> AWS Backup non installa automaticamente il `AwsVssComponents` pacchetto sulla tua istanza. È necessario eseguire un'installazione manuale sull'istanza. Per ulteriori informazioni, consulta Installazione manuale dei componenti VSS su un'istanza.

Creazione di snapshot VSS mediante Amazon Data Lifecycle Manager

Puoi creare snapshot VSS utilizzando Amazon Data Lifecycle Manager abilitando gli script pre e post nelle policy del ciclo di vita degli snapshot. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/ebs/latest/userguide/automate-app-consistent-backups.html.

> **Note**
>
> Il Sistema di gestione del ciclo di vita dei dati Amazon non installa automaticamente il pacchetto `AwsVssComponents` sull'istanza. È necessario eseguire un'installazione manuale sull'istanza. Per ulteriori informazioni, consulta Installazione manuale dei componenti VSS su un'istanza.

Risolvi i problemi relativi alle istantanee EBS basate su Windows VSS

Prima di provare qualsiasi altra procedura di risoluzione dei problemi, consigliamo di verificare le seguenti informazioni.

- Assicurati di aver soddisfatto tutti i Prerequisiti.
- Verifica di utilizzare la Supporto della versione del sistema operativo Windows più recente del pacchetto `AwsVssComponents` per il sistema operativo. Il problema riscontrato potrebbe essere stato risolto nelle versioni più recenti.

Argomenti

- Controlla i file di registro
- Raccogli registri diagnostici aggiuntivi

- Utilizza VSS su istanze con proxy configurato
- Errore: timeout della connessione del thaw pipe, errore sul thaw, timeout in attesa di VSS Freeze o altri errori di timeout
- Errore: impossibile richiamare il metodo. L'invocazione del metodo è supportata solo sui tipi principali in questa modalità di linguaggio

Controlla i file di registro

Se si verificano problemi o si ricevono messaggi di errore durante la creazione di istantanee EBS abilitate per VSS, è possibile visualizzare l'output del comando nella console Systems Manager.

Per i documenti Systems Manager che creano istantanee VSS, è possibile impostare il `CollectDiagnosticLogs` parametro su "`True`" in fase di esecuzione. Quando il `CollectDiagnosticLogs` parametro è impostato su "`True`«, VSS raccoglie registri aggiuntivi per facilitare il debug. Per ulteriori informazioni, consulta Raccogli registri diagnostici aggiuntivi.

Se raccogli registri di diagnostica, il documento Systems Manager li memorizza sulla tua istanza nella seguente posizione:`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`. L'impostazione predefinita per il `CollectDiagnosticLogs` parametro è "`False`».

> **Note**
>
> Per ulteriore assistenza sul debug, puoi inviare il `.zip` file a. AWS Support

Sono disponibili i seguenti registri aggiuntivi, indipendentemente dal fatto che vengano raccolti o meno registri di diagnostica:

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stdout`
- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stderr`

È inoltre possibile aprire l'applicazione Visualizzatore eventi di Windows e scegliere Registri di Windows, Applicazione per visualizzare i registri aggiuntivi. Per visualizzare gli eventi specificatamente dal provider VSS Windows EC2 e dal servizio Copia shadow del volume, filtrare in base all' origine con i termini **`Ec2VssSoftwareProvider`** e **`VSS`**.

Se utilizzi Systems Manager con endpoint VPC e l'azione dell'SendCommandAPI Systems Manager (Esegui comando nella console) non è riuscita, verifica di aver configurato correttamente il seguente endpoint: com.amazonaws. ***regione .ec2.***

Senza l'endpoint Amazon EC2 definito, la chiamata per enumerare i volumi EBS collegati ha esito negativo, causando il fallimento del comando Systems Manager. Per ulteriori informazioni sulla configurazione degli endpoint VPC con Systems Manager, consulta Creazione di un endpoint VPC nella AWS Systems Manager Guida per l'utente di .

Raccogli registri diagnostici aggiuntivi

Per raccogliere registri diagnostici aggiuntivi quando si utilizza il comando send di Systems Manager per eseguire il documento snapshot VSS, impostare il parametro di `CollectDiagnosticLogs` input su "`True`" in fase di esecuzione. Si consiglia di impostare questo parametro su "`True`" durante la risoluzione dei problemi.

Per vedere un esempio di riga di comando, seleziona una delle seguenti schede.

AWS CLI

L'esempio seguente esegue il documento `AWSEC2-CreateVssSnapshot` Systems Manager in AWS CLI:

```
aws ssm send-command \
--document-name "AWSEC2-CreateVssSnapshot" \
--instance-ids "i-1234567890abcdef0" \
--parameters '{"description":["Example - create diagnostic logs at
 runtime."],"tags":["Key=tag_name,Value=tag_value"],"CollectDiagnosticLogs":
["True"]}'
```

PowerShell

L'esempio seguente esegue il documento `AWSEC2-CreateVssSnapshot` Systems Manager in PowerShell:

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-1234567890abcdef0" -Parameter @{'description'='Example - create diagnostic logs
 at runtime.';'tags'='Key=tag_name,Value=tag_value';'CollectDiagnosticLogs'='True'}
```

Utilizza VSS su istanze con proxy configurato

Se riscontri problemi durante la creazione di snapshot EBS compatibili con VSS su istanze che utilizzano un proxy per raggiungere gli endpoint EC2, assicurati di quanto segue:

- Il proxy è configurato in modo che gli endpoint del servizio EC2 nella regione e nell'IMDS dell'istanza siano raggiungibili eseguendo come SYSTEM. AWS Tools for Windows PowerShell
- È installato `AwsVssComponents` versione 2.0.1 o successiva. A partire da `AwsVssComponents` versione 2.0.1, il provider VSS EC2 supporta l'utilizzo del proxy WinHTTP configurato dal sistema. Per ulteriori informazioni sulla configurazione del proxy WinHTTP, consulta la pagina Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP) sul sito web di Microsoft.

Errore: timeout della connessione del thaw pipe, errore sul thaw, timeout in attesa di VSS Freeze o altri errori di timeout

Il provider VSS Windows EC2 potrebbe scadere a causa di attività o servizi sull'istanza che impediscono agli snapshot abilitati per VSS di procedere in modo tempestivo. Il framework VSS Windows fornisce una finestra di 10 secondi non configurabile durante la quale la comunicazione con il file system viene sospesa. Durante questo periodo, `AWSEC2-CreateVssSnapshot` crea gli snapshot dei volumi.

I seguenti problemi possono causare il superamento dei limiti di tempo da parte del provider VSS Windows EC2 durante uno snapshot:

- I/O eccessivo per un volume
- Reattività lenta dell'API EC2 sull'istanza
- Volumi frammentati
- Incompatibilità con alcuni software antivirus
- Problemi con un autore di applicazioni VSS
- Quando il Module Logging è abilitato per un gran numero di PowerShell moduli, ciò può causare un rallentamento dell'esecuzione degli script PowerShell

La maggior parte dei problemi che si verificano quando si esegue il documento di comando `AWSEC2-CreateVssSnapshot` è legata a un carico di lavoro eccessivamente elevato sull'istanza al momento del backup. Le seguenti azioni consentono di eseguire con successo lo snapshot:

- Riprovare a eseguire il comando `AWSEC2-CreateVssSnapshot` per verificare se il tentativo di snapshot ha esito positivo. Se in alcuni casi il tentativo ha esito positivo, la riduzione del carico dell'istanza potrebbe rendere più efficace gli snapshot.
- Attendere che il carico di lavoro sull'istanza diminuisca e riprovare a eseguire il comando `AWSEC2-CreateVssSnapshot`. In alternativa, è possibile scattare gli snapshot quando si è certi che l'istanza è in una fase di carico ridotto.
- Provare a scattare gli snapshot VSS dopo avere disattivato il software antivirus del sistema. Se questo risolve il problema, fare riferimento alle istruzioni del software antivirus e configurarlo per consentire gli snapshot VSS.
- Se nell'account è presente un volume elevato di chiamate API Amazon EC2 nella stessa regione in cui si esegue uno snapshot, la limitazione (della larghezza di banda della rete) delle API può ritardare le operazioni di snapshot. Per ridurre l'impatto della limitazione, utilizzare la versione più recente del pacchetto `AwsVssComponents` (versione 2.1.0 e successive, con autorizzazioni di prerequisito). Questo pacchetto utilizza l'operazione API `CreateSnapshots` di EC2 per ridurre il numero di operazioni mutevoli, come la creazione e l'applicazione di tag per volume.
- Se vi sono più script di comando `AWSEC2-CreateVssSnapshot` in esecuzione contemporaneamente, è possibile seguire questa procedura per ridurre i problemi di simultaneità.
  - Valutare la possibilità di programmare gli snapshot durante periodi di minore attività delle API.
  - Se si utilizza Run Command nella console Systems Manager (oppure SendCommand nell'API) per eseguire lo script di comando, è possibile utilizzare i controlli di velocità di Systems Manager per ridurre la simultaneità.

    È inoltre possibile utilizzare i controlli di frequenza di Systems Manager per ridurre la concorrenza per servizi come quelli AWS Backup che utilizzano Systems Manager per eseguire lo script di comando.
- Eseguire il comando `vssadmin list writers` in una shell e verificare se segnala eventuali errori nel campo Ultimo errore per tutti gli autori del sistema. Se un autore segnala un errore di timeout, è consigliabile scattare nuovi snapshot quando l'istanza è sotto un carico minore.
- Quando si utilizzano tipi di istanza più piccoli, come *`t2 | t3 | t3a`*.nano o *`t2 | t3 | t3a`*-micro, possono verificarsi timeout dovuti a limiti di memoria e CPU. Le seguenti operazioni potrebbero contribuire a ridurre i problemi di timeout.
  - Provare a chiudere le applicazioni con un uso intensivo di memoria e CPU prima di acquisire snapshot.
  - Provare ad acquisire snapshot durante i periodi di minore attività dell'istanza.

Errore: impossibile richiamare il metodo. L'invocazione del metodo è supportata solo sui tipi principali in questa modalità di linguaggio

Questo errore si verificherà quando la modalità della PowerShell lingua non è impostata su. `FullLanguage` I documenti `AWSEC2-CreateVssSnapshot` e `AWSEC2-ManageVssIo` SSM devono PowerShell essere configurati in `FullLanguage` modalità.

Per verificare la modalità della lingua, esegui il seguente comando sull'istanza in una PowerShell console:

```
$ExecutionContext.SessionState.LanguageMode
```

Per ulteriori informazioni sulle modalità di linguaggio, consulta about_Language_Modes nella documentazione di Microsoft.

Ripristino di volumi EBS da snapshot EBS abilitati per VSS

È possibile utilizzare lo script `RestoreVssSnapshotSampleScript.ps1` per ripristinare i volumi su un'istanza da snapshot EBS con tecnologia VSS. Questo script esegue le operazioni seguenti:

- Arresta un'istanza
- Rimuove tutte le unità esistenti dall'istanza (eccetto il volume di avvio, se è stato escluso)
- Crea nuovi volumi dagli snapshot
- Collega i volumi all'istanza utilizzando il tag di ID dispositivo sulla snapshot
- Riavvia l'istanza

> **Important**
>
> Lo script seguente scollega tutti i volumi collegati a un'istanza, poi crea nuovi volumi da una snapshot. Accertati di aver correttamente eseguito il backup dell'istanza. I vecchi volumi non vengono eliminati. All'occorrenza, è possibile modificare lo script per eliminare i vecchi volumi.

Per ripristinare volumi da snapshot EBS con tecnologia VSS

1. Scarica il RestoreVssSnapshotSampleScriptfile.zip ed estrai il contenuto del file.

2. Apri `RestoreVssSnapshotSampleScript.ps1` in un editor di testo e modifica la chiamata di esempio nella parte inferiore dello script con un ID di istanza EC2 e un ID snapshot EBS validi, quindi esegui lo script da. PowerShell

AWS Cronologia delle versioni della soluzione VSS

Argomenti

AwsVssComponents versioni del pacchetto

La tabella seguente descrive le versioni rilasciate del pacchetto di componenti AWS VSS.

Versione	Dettagli	Data di rilascio
2.3.3	È stato aggiornato l'agente VSS per garantire che `Ec2VssProvider` venga utilizzato durante la creazione di istantanee.	25 giugno 2024
2.3.2	Risolto un caso in cui la registrazione del provider VSS non veniva rimossa durante la disinstallazione.	9 maggio 2024
2.3.1	È stato aggiunto un nuovo tag predefinito `AwsVssConfig` per identificare istantanee e AMI create da VSS. AWS	7 marzo 2024
2.2.1	• È stato aggiunto il supporto per l'utilizzo dell'`DescribeInstanceAttribute` API. • Correzioni di bug e miglioramenti dell'affidabilità. • Supporto obsoleto per Windows Server 2012 e 2012 R2. AWS L'installazione dei componenti VSS versione 2.2.1 su Windows Server 2012 e 2012 R2 avrà esito negativo. AWS	18 gennaio 2024

Versione	Dettagli	Data di rilascio
	La versione 2.1.0 dei componenti VSS è l'ultima versione a supportare Windows Server 2012 e 2012 R2.	
2.1.0	È stato aggiunto il supporto per l'utilizzo dell'`CreateSnapshots` API.	6 novembre 2023
2.0.1	È stato aggiunto il supporto per l'utilizzo delle impostazioni del proxy WinHTTP.	26 ottobre 2023
2.0.0	È stata aggiunta la funzionalità al componente AWS VSS di creare istantanee e AMI, che consente la compatibilità con le funzionalità di registrazione dei PowerShell moduli, registrazione dei blocchi di script e trascrizione.	28 aprile 2023
1.3.2.0	Risolto un caso in cui l'errore di installazione non è stato segnalato correttamente.	10 maggio 2022
1.3.1.0	• Risolti gli snapshot che non funzionavano sui controller di dominio in relazione a un errore di registrazione del writer VSS NTDS. • Risolto l'errore dell'agente VSS durante la disinstallazione del provider VSS versione 1.0.	6 febbraio 2020

Versione	Dettagli	Data di rilascio
1.3.00	• Registrazione migliorata riducendo la verbosità indesiderata. • Risolti i problemi di regionalizzazione durante l'installazione. • Codici di reso fissi per alcune condizioni di errore di registrazione del provider. • Risolti vari problemi di installazione.	19 marzo 2019
1.2.00	• Aggiunti parametri della riga di comando `-nw` (senza scrittori) e `-copy` (solo copia) all'agente. • Sono stati corretti EventLog gli errori causati da chiamate di allocazione della memoria improprie.	15 novembre 2018
1.1	Risolto il problema con i componenti AWS VSS che venivano utilizzati in modo errato come provider predefinito di Windows Backup and Restore.	12 dicembre 2017
1	Versione iniziale.	20 novembre 2017

Supporto della versione del sistema operativo Windows

La tabella seguente mostra quali versioni della soluzione AWS VSS è necessario eseguire su ciascuna versione di Windows Server su Amazon EC2.

Versione di Windows Server	AwsVssComponents versione	AWSECnor della VssInstallAndSnapshot versione 2	AWSECnor della CreateVssSnapshot versione 2	AWSEC2-Nome della versione ManageVssIO
Windows Server 2022	default	default	default	default
Windows Server 2019	default	default	default	default
Windows Server 2016	default	default	default	default
Windows Server 2012 R2	2.1.0	non supportato	2012R2	2012R2
Windows Server 2012	2.1.0	non supportato	2012R2	2012R2
Windows Server 2008 R2	1.3.1.0	non supportato	2008R2	2008R2

Prevenzione della scrittura anomala per le istanze Linux

> **Note**
>
> La prevenzione della scrittura tornizzata è supportata solo con le istanze Linux.

Torn write prevention è una funzionalità di storage a blocchi progettata per migliorare le prestazioni dei carichi di lavoro dei database relazionali AWS a uso intensivo di I/O e ridurre la latenza senza influire negativamente sulla resilienza dei dati. I database relazionali che utilizzano InnoDB o XtraDB come motore di database, come MySQL e MariaDB, trarranno vantaggio dalla prevenzione delle distorsioni di scrittura.

In genere, i database relazionali che utilizzano pagine più grandi dell'atomicità in caso di interruzione dell'alimentazione del dispositivo di archiviazione utilizzano meccanismi di registrazione dei dati per proteggersi dalle distorsioni di scrittura. MariaDB e MySQL utilizzano un file buffer di doppia scrittura per registrare i dati prima di scriverli nelle tabelle di dati. In caso di scritture incomplete o errate a causa di arresti anomali del sistema operativo o di interruzione dell'alimentazione durante le transazioni di scrittura, il database può recuperare i dati dal buffer di doppia scrittura. Il sovraccarico di I/O aggiuntivo associato alla scrittura nel buffer di doppia scrittura influisce sulle prestazioni del database e sulla latenza delle applicazioni e riduce il numero di transazioni che possono essere elaborate al secondo. Per ulteriori informazioni sul buffer di doppia scrittura, consulta la documentazione di MariaDB e MySQL.

Con Torn Write Prevention, i dati vengono scritti nell'archivio in transazioni di scrittura, eliminando così la necessità di utilizzare il buffer di all-or-nothingscrittura doppia. Ciò impedisce che dati parziali o incompleti vengano scritti nell'archivio in caso di arresti anomali del sistema operativo o di interruzione dell'alimentazione durante le transazioni di scrittura. È possibile aumentare il numero di transazioni elaborate al secondo fino a un massimo del 30 percento e ridurre la latenza di scrittura fino a un massimo del 50 percento senza compromettere la resilienza dei carichi di lavoro.

Prezzi

L'utilizzo della prevenzione delle distorsioni di scrittura non prevede costi aggiuntivi.

Dimensioni dei blocchi supportate e allineamenti dei limiti dei blocchi

La prevenzione delle distorsioni di scrittura supporta operazioni di scrittura per blocchi di dati da 4 KiB, 8 KiB e 16 KiB. L'indirizzo del blocco logico (LBA) di inizio del blocco di dati deve essere

allineato alla rispettiva dimensione del limite del blocco di 4 KiB, 8 KiB o 16 KiB. Ad esempio, per le operazioni di scrittura da 16 KiB, l'LBA di inizio del blocco di dati deve essere allineato a una dimensione del limite del blocco di 16 KiB.

La tabella seguente mostra il supporto per tutti i tipi di archiviazione e di istanza.

	Blocchi da 4 KiB	Blocchi da 8 KiB	Blocchi da 16 KiB
Volumi di archivio dell'istanza	Tutti i volumi di archivio dell'istanza NVMe collegati a istanze della famiglia I della generazione corrente.	Istanze I4i, Im4gn e IS4gen supportate da Nitro SSD. AWS	
Volumi Amazon EBS	Tutti i volumi Amazon EBS collegati a istanze basate sul sistema AWS Nitro.		

Per verificare se l'istanza e il volume supportano la prevenzione delle distorsioni di scrittura, esegui una query per verificare se l'istanza supporta la funzionalità e altri dettagli, come le dimensioni dei blocchi e dei limiti supportate. Per ulteriori informazioni, consulta Verifica del supporto e della configurazione della prevenzione delle distorsioni di scrittura.

Requisiti

Affinché la prevenzione delle distorsioni di scrittura funzioni correttamente, un'operazione di I/O deve soddisfare i requisiti di dimensione, allineamento e limiti, come specificato nei campi `NTWPU`, `NTWGU` e `NTWBU`. È necessario configurare il sistema operativo in modo da evitare che il sottosistema di archiviazione specifico (file system, LVM, RAID, ecc.) modifichi le proprietà di I/O lungo lo stack di archiviazione, comprese le unioni e le divisioni di blocchi o il trasferimento degli indirizzi dei blocchi, prima dell'invio al dispositivo.

La prevenzione delle distorsioni di scrittura è stata testata con la seguente configurazione:

- Un tipo di istanza e un tipo di archiviazione che supportano la dimensione del blocco richiesta.
- Amazon Linux 2 con versione del kernel 5.10 o successiva.
- ext4 con la funzione `bigalloc` abilitata, una dimensione del cluster di 16 KiB e le utilità ext4 più recenti (e2fsprogs 1.46.5 o versioni successive).

- Modalità di accesso ai file `O_DIRECT` per bypassare la cache del buffer del kernel Linux.

> **Note**
>
> Non è necessario disabilitare l'unione I/O per i carichi di lavoro MySQL e MariaDB.

Verifica del supporto e della configurazione della prevenzione delle distorsioni di scrittura

Per verificare se l'istanza e il volume supportano la prevenzione delle distorsioni di scrittura e per visualizzare i dati specifici del fornitore dello spazio dei nomi NVMe che contengono informazioni sulla prevenzione delle distorsioni di scrittura, utilizza il comando seguente.

```
$ sudo nvme id-ns -v device_name
```

> **Note**
>
> Il comando restituisce le informazioni specifiche del fornitore in formato esadecimale con interpretazione ASCII. Nelle applicazioni potrebbe essere necessario creare uno strumento simile a `ebsnvme-id` che sia in grado di leggere e analizzare l'output.

Ad esempio, il comando seguente restituisce i dati specifici del fornitore dello spazio dei nomi NVMe che contengono informazioni sulla prevenzione delle distorsioni di scrittura per `/dev/nvme1n1`.

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Se l'istanza e il volume supportano la prevenzione della scrittura ripetuta, restituiscono le seguenti informazioni sulla prevenzione della scrittura non corretta nei dati AWS specifici del fornitore del namespace NVMe.

> **Note**
>
> I byte nella tabella seguente rappresentano l'offset in byte dall'inizio dei dati specifici del fornitore dello spazio dei nomi NVMe.

Byte	Descrizione
0:31	Il nome del punto di montaggio del dispositivo, ad esempio /dev/xvda . Lo fornisci durante la richiesta di collegamenti al volume e può essere utilizzato dall'istanza Amazon EC2 per creare un collegamento simbolico al dispositivo a blocchi NVMe (nvmeXn1).
32:63	L'ID del volume. Ad esempio, vol01234567890abcdef . Questo campo può essere utilizzato per mappare il dispositivo NVMe al volume collegato.
64:255	Riservato per uso futuro.
256:257	Dimensione dell'unità di prevenzione delle distorsioni di scrittura dello spazio dei nomi (NTWPU). Questo campo indica la dimensione specifica dello spazio dei nomi dell'operazione di scrittura garantita per la scrittura atomica sulla NVM durante un'interruzione di corrente o una condizione di errore. Il campo è specificato in blocchi logici rappresentati in valori a base zero.
258:259	Dimensione della granularità di prevenzione delle distorsioni di scrittura dello spazio dei nomi (NTWPU). Questo campo indica gli increment i di dimensione specifici dello spazio dei nomi al di sotto di NTWPU dell'operazione di scrittura garantita per la scrittura atomica sulla NVM durante un'interruzione di corrente o una condizione di errore. Cioè, la dimensione dovrebbe essere NTWPG * n <= NTWPU dove n è un numero intero positivo. Anche l'offset dell'LBA dell'operazione di scrittura deve essere allineato a questo campo. Il campo è specificato in blocchi logici rappresentati in valori a base zero.
260:263	Dimensione del limite di prevenzione delle distorsioni di scrittura dello spazio dei nomi (NTWPU). Questo campo indica la dimensione del limite atomico per questo spazio dei nomi per il valore NTWPU. Non è garantito che le scritture che superano i limiti atomici su questo spazio dei nomi vengano scritte atomicamente sulla NVM durante un'interr uzione di corrente o una condizione di errore. Il valore di 0h indica che non esistono limiti atomici per le interruzioni di corrente o le condizioni di

Byte	Descrizione
	errore. Tutti gli altri valori specificano una dimensione in termini di blocchi logici utilizzando la stessa codifica del campo NTWPU.

Configurazione dello stack software per la prevenzione delle distorsioni di scrittura

La prevenzione delle distorsioni di scrittura è abilitata per impostazione predefinita sui tipi di istanze supportati con volumi supportati. Non è necessario abilitare alcuna impostazione aggiuntiva per abilitare la prevenzione delle distorsioni di scrittura sul volume o sull'istanza.

> **Note**
>
> Non vi è alcun impatto sulle prestazioni dei carichi di lavoro che non supportano la prevenzione delle distorsioni di scrittura. Non è necessario apportare modifiche per questi carichi di lavoro.
> I carichi di lavoro che supportano la prevenzione delle distorsioni di scrittura ma non sono configurati per utilizzarla continuano a utilizzare il buffer di doppia scrittura e non ottengono alcun vantaggio in termini di prestazioni.

Per configurare lo stack software MySQL o MariaDB in modo da disabilitare il buffer di doppia scrittura e utilizzare la prevenzione delle distorsioni di scrittura, completa i seguenti passaggi:

1. Configura il volume per utilizzare il file system ext4 con l' BigAlloc opzione e imposta la dimensione del cluster su 4 KiB, 8 KiB o 16 KiB. L'utilizzo BigAlloc con una dimensione del cluster di 4 KiB, 8 KiB o 16 KiB garantisce che il file system allochi i file in linea con il rispettivo limite.

   ```
   $  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
   ```

   > **Note**
   >
   > Per MySQL e MariaDB, è necessario utilizzare `-C 16384` per eguagliare la dimensione della pagina del database. L'impostazione della granularità di allocazione su un valore diverso da un multiplo della dimensione della pagina può comportare allocazioni che

potrebbero non corrispondere ai limiti di prevenzione delle distorsioni di scrittura del dispositivo di archiviazione.

Per esempio:

```
$  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
```

2. Configura InnoDB per l'utilizzo del metodo di svuotamento `O_DIRECT` e disattiva la doppia scrittura di InnoDB. Utilizza un editor di testo per aprire `/etc/my.cnf` e modifica i parametri `innodb_flush_method` e `innodb_doublewrite` come segue:

```
innodb_flush_method=O_DIRECT
innodb_doublewrite=0
```

Important

Se utilizzi Logical Volume Manager (LVM) o un altro livello di virtualizzazione dell'archiviazione, assicurati che gli offset iniziali dei volumi siano allineati su multipli di 16 KiB. Ciò è relativo all'archiviazione NVMe sottostante, che deve tenere conto delle intestazioni dei metadati e dei superblocchi utilizzati dal livello di virtualizzazione dell'archiviazione. L'aggiunta di un offset al volume fisico LVM può causare un disallineamento tra le allocazioni del file system e gli offset del dispositivo NVMe, il che invaliderebbe la prevenzione delle distorsioni di scrittura. Per ulteriori informazioni, consulta la sezione `--dataalignmentoffset` nella pagina del manuale Linux.

Risorse e tag

In Amazon EC2 sono disponibili varie risorse che puoi creare e utilizzare. Alcune di queste risorse includono immagini, istanze, volumi e snapshot. Quando crei una risorsa, assegniamo a tale risorsa un ID risorsa univoco.

Ad alcune risorse puoi assegnare tag con valori definiti per velocizzarne l'organizzazione e l'identificazione.

Gli argomenti seguenti descrivono le risorse e i tag e come puoi utilizzarli.

Indice

Cestino

Il Cestino di riciclaggio è una caratteristica di ripristino dei dati che consente di ripristinare snapshot Amazon EBS e AMI EBS-backed eliminati accidentalmente. Quando si usa il Cestino di riciclaggio, se le risorse vengono eliminate, vengono conservate al suo interno per un periodo di tempo specificato, prima di essere eliminate definitivamente.

Puoi ripristinare una risorsa dal Cestino di riciclaggio in qualsiasi momento, prima della scadenza del periodo di conservazione. Quando ripristini una risorsa dal Cestino di riciclaggio, essa viene rimossa dal Cestino di riciclaggio e puoi usarla nello stesso modo in cui usi qualsiasi altra risorsa dello stesso tipo nel tuo account. Se il periodo di conservazione scade e la risorsa non viene ripristinata, viene eliminata definitivamente dal Cestino di riciclaggio e non è più disponibile per il ripristino.

L'utilizzo del Cestino di riciclaggio contribuisce a garantire la continuità aziendale proteggendo i dati business-critical dall'eliminazione accidentale.

Argomenti

Come funziona?

Per abilitare e utilizzare Recycle Bin, è necessario creare regole di conservazione nelle AWS regioni in cui si desidera proteggere le risorse. Le regole di conservazione specificano le seguenti informazioni:

- Il tipo di risorsa da proteggere.
- Le risorse che vuoi mantenere nel Cestino di riciclaggio quando vengono eliminate.
- Il periodo di conservazione durante il quale mantenere le risorse nel Cestino di riciclaggio prima che vengano eliminate definitivamente.

Con il Cestino di riciclaggio puoi creare due tipi di regole di conservazione:

- Regole di conservazione a livello di tag: una regola di conservazione a livello di tag usa i tag delle risorse per identificare le risorse che devono essere mantenute nel Cestino di riciclaggio. Per ogni regola di conservazione, è necessario specificare una o più coppie di chiavi e valori di tag. Le risorse del tipo specificato taggate con almeno una delle coppie chiave-valore di tag specificate nella regola di conservazione vengono mantenute automaticamente nel Cestino di riciclaggio al momento dell'eliminazione. Puoi usare questo tipo di regola di conservazione se desideri proteggere risorse specifiche nel tuo account in base ai relativi tag.
- Regole di conservazione a livello di Regione: una regola di conservazione a livello di Regione non ha alcun tag di risorsa specificato. Si applica a tutte le risorse del tipo specificato nella regione in

cui viene creata la regola, anche se le risorse non sono taggate. Puoi usare questo tipo di regola di conservazione se desideri proteggere tutte le risorse di un tipo specifico in una Regione specifica.

Mentre una risorsa si trova nel Cestino di riciclaggio, puoi ripristinarla per l'uso in qualsiasi momento.

La risorsa rimane nel Cestino di riciclaggio fino a quando non si verifica una delle seguenti situazioni:

- È possibile ripristinarlo manualmente per l'uso. Quando ripristini una risorsa dal Cestino di riciclaggio, viene rimossa dal Cestino di riciclaggio e diventa immediatamente disponibile per l'uso. Puoi usare le risorse ripristinate nello stesso modo in cui usi qualsiasi altra risorsa dello stesso tipo nel tuo account.
- Il periodo di conservazione scade. Se il periodo di conservazione scade e la risorsa non è stata ripristinata dal Cestino di riciclaggio, viene eliminata definitivamente dal Cestino di riciclaggio e non può più essere visualizzata o ripristinata.

Risorse supportate

Il Cestino di riciclaggio supporta i tipi di risorse seguenti:

- Snapshot Amazon EBS

> **Important**
>
> Le regole di conservazione del cestino si applicano anche agli snapshot archiviati nel livello di archiviazione archivio. Se elimini uno snapshot archiviato corrispondente a una regola di conservazione, lo snapshot viene mantenuto nel cestino per il periodo definito nella regola di conservazione. Gli snapshot archiviati vengono fatturati alla tariffa per gli snapshot archiviati mentre si trovano nel Cestino di riciclaggio.

- Amazon Machine Image (AMI) Amazon EBS-backed

> **Note**
>
> Le regole di conservazione si applicano anche alle AMI disabilitate.

Considerazioni

Le considerazioni seguenti si applicano quando si usano il Cestino di riciclaggio e le regole di conservazione.

Considerazioni generali

- **Important**

  Quando crei la prima regola di conservazione, possono essere necessari fino a 30 minuti prima che diventi attiva e inizi a mantenere le risorse. Dopo aver creato la prima regola di conservazione, le regole di conservazione successive diventano attive e iniziano a mantenere le risorse quasi immediatamente.

- Se una risorsa corrisponde a più di una regola di conservazione al momento dell'eliminazione, la regola di conservazione con il periodo di conservazione più lungo ha la precedenza.
- Non puoi eliminare manualmente una risorsa dal Cestino di riciclaggio. La risorsa verrà eliminata automaticamente allo scadere del periodo di conservazione.
- Mentre una risorsa si trova nel Cestino di riciclaggio, puoi visualizzarla, ripristinarla o modificarne i tag. Per usare la risorsa in qualsiasi altro modo, è necessario prima ripristinarla.
- Se qualcuno Servizio AWS, ad esempio AWS Backup o Amazon Data Lifecycle Manager, elimina una risorsa che corrisponde a una regola di conservazione, tale risorsa viene automaticamente conservata da Recycle Bin.
- Quando una risorsa viene inviata al Cestino di riciclaggio, le viene assegnato il seguente tag generato dal sistema:
  - Chiave tag: `aws:recycle-bin:resource-in-bin`
  - Valore tag: `true`

  Non è possibile modificare o eliminare manualmente questo tag. Quando la risorsa viene ripristinata dal Cestino di riciclaggio, il tag viene rimosso automaticamente.

Considerazioni sugli snapshot

- **Important**

  Se disponi di regole di conservazione per le AMI e per gli snapshot associati, è possibile rendere il periodo di conservazione degli snapshot uguale o superiore al periodo di

conservazione per le AMI. Ciò garantisce che il Cestino di riciclaggio non elimini gli snapshot associati a un'AMI prima di eliminare l'AMI stessa, poiché in quel caso l'AMI non può più essere recuperata.

- Se uno snapshot è abilitato per il ripristino rapido degli snapshot quando viene eliminato, il ripristino rapido degli snapshot viene disabilitato automaticamente poco dopo l'invio dello snapshot al Cestino di riciclaggio.
  - Se si ripristina lo snapshot prima che il ripristino rapido dello snapshot sia disabilitato, lo snapshot rimane abilitato.
  - Se si ripristina lo snapshot dopo che il ripristino rapido degli snapshot è stato disattivato, rimarrà disabilitato. Se necessario, si dovrà riabilitare manualmente il ripristino rapido degli snapshot.
- Se uno snapshot viene condiviso quando viene eliminato, la condivisione viene annullata automaticamente quando viene inviato al Cestino di riciclaggio. Se si ripristina lo snapshot, tutte le autorizzazioni di condivisione precedenti saranno ripristinate automaticamente.
- Se un'istantanea creata da un altro AWS servizio, ad esempio, AWS Backup viene inviata al Cestino e successivamente la ripristini dal Cestino, non viene più gestita dal servizio che l'ha creata. AWS Se non è più necessario, occorre eliminare manualmente lo snapshot.

Considerazioni per le AMI

- Sono supportate solo le AMI Amazon EBS-backed.
- **Important**

  Se disponi di regole di conservazione per le AMI e per gli snapshot associati, è possibile rendere il periodo di conservazione degli snapshot uguale o superiore al periodo di conservazione per le AMI. Ciò garantisce che il Cestino di riciclaggio non elimini gli snapshot associati a un'AMI prima di eliminare l'AMI stessa, poiché in quel caso l'AMI non può più essere recuperata.
- Se un'AMI viene condivisa quando viene eliminata, la condivisione viene annullata automaticamente quando viene inviata al Cestino di riciclaggio. Se si ripristina l'AMI, tutte le autorizzazioni di condivisione precedenti vengono ripristinate automaticamente.
- Prima di poter ripristinare un'AMI dal Cestino di riciclaggio, è necessario innanzitutto ripristinare tutti gli snapshot associati dal Cestino di riciclaggio e assicurarsi che abbiano lo stato `available`.

- Se le istantanee associate all'AMI vengono eliminate dal Cestino di riciclaggio, l'AMI non può più essere recuperata. L'AMI verrà eliminata alla scadenza del periodo di conservazione.
- Se un'AMI creata da un altro AWS servizio, ad esempio AWS Backup, viene inviata al Cestino e successivamente si ripristina tale AMI dal Cestino, non viene più gestita dal AWS servizio che l'ha creata. Se non è più necessaria, occorre eliminare manualmente l'AMI.

Considerazioni sulle policy per gli snapshot di Sistema di gestione del ciclo di vita dei dati Amazon

- Se Sistema di gestione del ciclo di vita dei dati Amazon elimina uno snapshot che corrisponde a una regola di conservazione, tale snapshot viene mantenuto automaticamente dal cestino.
- Se Amazon Data Lifecycle Manager elimina uno snapshot e lo invia al Cestino di riciclaggio quando viene raggiunta la soglia di conservazione della policy e si ripristina manualmente lo snapshot dal Cestino di riciclaggio, è necessario eliminare manualmente tale snapshot quando non è più necessario. Amazon Data Lifecycle Manager non gestirà più lo snapshot.
- Se si elimina manualmente uno snapshot creato da una policy e tale snapshot si trova nel Cestino di riciclaggio quando viene raggiunta la soglia di conservazione della policy, Amazon Data Lifecycle Manager non eliminerà lo snapshot. Amazon Data Lifecycle Manager non gestisce gli snapshot mentre sono archiviati nel Cestino di riciclaggio

  Se lo snapshot viene ripristinato dal Cestino di riciclaggio prima che venga raggiunta la soglia di conservazione della policy, Amazon Data Lifecycle Manager eliminerà lo snapshot quando viene raggiunta la soglia di conservazione della policy.

  Se lo snapshot viene ripristinato dal Cestino di riciclaggio dopo che venga raggiunta la soglia di conservazione della policy, Amazon Data Lifecycle Manager non provvederà più ad eliminare lo snapshot. Lo snapshot che non è più necessario deve essere eliminato manualmente.

Considerazioni per AWS il Backup

- Se AWS Backup elimina un'istantanea che corrisponde a una regola di conservazione, tale istantanea viene automaticamente conservata dal Cestino.

Considerazioni sugli snapshot archiviati

- Le regole di conservazione del cestino si applicano anche agli snapshot archiviati nel livello di archiviazione archivio. Se elimini uno snapshot archiviato corrispondente a una regola di

conservazione, lo snapshot viene mantenuto nel cestino per il periodo definito nella regola di conservazione.

Gli snapshot archiviati vengono fatturati alla tariffa per gli snapshot archiviati mentre si trovano nel Cestino di riciclaggio.

In altre parole, se una regola di conservazione elimina uno snapshot archiviato dal cestino prima del periodo di archivio minimo di 90 giorni, ti vengono addebitati i costi per i giorni rimanenti. Per ulteriori informazioni, consulta i prezzi e la fatturazione degli snapshot archiviati nella Guida per l'utente di Amazon EBS.

Per utilizzare uno snapshot archiviato che si trova nel cestino, è necessario prima recuperarlo dal cestino, quindi ripristinarlo dal livello archivio nel livello standard.

Quote

Le quote seguenti si applicano al Cestino di riciclaggio.

Quota	Quota predefinita			
Regole di conservazione per regione	250			
Coppie di chiavi e valori di tag per regola di conservazione	50			

Servizi correlati

Il Cestino di riciclaggio funziona con i seguenti servizi:

- AWS CloudTrail — Consente di registrare eventi che si verificano nel Cestino di riciclaggio. Per ulteriori informazioni, consulta Monitora Recycle Bin utilizzando AWS CloudTrail.

Prezzi

Le risorse nel Cestino di riciclaggio vengono fatturate in base alle tariffe standard. Non sono previsti costi aggiuntivi per l'utilizzo di Cestino di riciclaggio e regole di conservazione. Per ulteriori informazioni, consulta Prezzi di Amazon EBS.

> **Note**
>
> Alcune risorse potrebbero ancora apparire nella console Recycle Bin o nell'output dell'API AWS CLI e per un breve periodo dopo la scadenza dei rispettivi periodi di conservazione e l'eliminazione definitiva. Queste risorse non vengono fatturate. La fatturazione si interrompe non appena il periodo di conservazione scade.

È possibile utilizzare i seguenti tag di allocazione dei costi AWS generati per il monitoraggio e l'allocazione dei costi durante l'utilizzo. AWS Billing and Cost Management

- Chiave: `aws:recycle-bin:resource-in-bin`
- Valore: `true`

Per ulteriori informazioni, consulta la pagina Tag di allocazione dei costi generati da AWS nella Guida per l'utente di AWS Billing and Cost Management .

Autorizzazioni IAM richieste

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per usare il Cestino di riciclaggio, le regole di conservazione o gli snapshot presenti nel Cestino di riciclaggio. Per permettere agli utenti di utilizzare queste risorse, è necessario creare delle policy IAM che forniscano l'autorizzazione per l'uso di risorse e operazioni API specifiche. Dopo aver creato le politiche, è necessario aggiungere le autorizzazioni agli utenti, ai gruppi o ai ruoli.

Argomenti

- Autorizzazioni per usare il Cestino di riciclaggio e le regole di conservazione
- Autorizzazioni per usare le risorse nel Cestino di riciclaggio
- Chiavi di condizione per il Cestino

Autorizzazioni per usare il Cestino di riciclaggio e le regole di conservazione

Per usare il Cestino di riciclaggio e le regole di conservazione, gli utenti devono disporre delle seguenti autorizzazioni.

- `rbin:CreateRule`
- `rbin:UpdateRule`
- `rbin:GetRule`
- `rbin:ListRules`
- `rbin:DeleteRule`
- `rbin:TagResource`
- `rbin:UntagResource`
- `rbin:ListTagsForResource`
- `rbin:LockRule`
- `rbin:UnlockRule`

Per usare la console del Cestino di riciclaggio, gli utenti devono disporre dell'autorizzazione `tag:GetResources`.

Di seguito è riportata una policy IAM di esempio che include l'autorizzazione `tag:GetResources` per gli utenti della console. Se qualche autorizzazione non è necessaria, puoi rimuoverla dalla policy.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "rbin:CreateRule",
            "rbin:UpdateRule",
            "rbin:GetRule",
            "rbin:ListRules",
            "rbin:DeleteRule",
            "rbin:TagResource",
            "rbin:UntagResource",
            "rbin:ListTagsForResource",
            "rbin:LockRule",
            "rbin:UnlockRule",
            "tag:GetResources"
```

```
        ],
        "Resource": "*"
    }]
}
```

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Autorizzazioni per usare le risorse nel Cestino di riciclaggio

Per ulteriori dettagli sulle autorizzazioni IAM necessarie per usare le risorse nel Cestino di riciclaggio, consulta gli argomenti seguenti:

- Autorizzazioni per l'uso degli snapshot nel Cestino di riciclaggio
- Autorizzazioni per l'uso delle AMI nel Cestino di riciclaggio

Chiavi di condizione per il Cestino

Il Cestino definisce le seguenti chiavi di condizione che puoi utilizzare nell'elemento `Condition` di una policy IAM per controllare le condizioni in base alle quali si applica l'istruzione di policy. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

Argomenti

- Chiave di condizione rbin:Request/ResourceType
- Chiave di condizione rbin:Attribute/ResourceType

Chiave di condizione **`rbin:Request/ResourceType`**

La chiave di `rbin:Request/ResourceType` condizione può essere utilizzata per filtrare l'accesso CreateRulee ListRuleslе richieste in base al valore specificato per il parametro di `ResourceType` richiesta.

Esempio 1 - CreateRule

Il seguente esempio di policy IAM consente ai presidi IAM di effettuare CreateRulerichieste solo se il valore specificato per il parametro di `ResourceType` richiesta è `EBS_SNAPSHOT` o`EC2_IMAGE`. Ciò consente al principale di creare nuove regole di conservazione solo per gli snapshot e le AMI.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:CreateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Esempio 2 - ListRules

Il seguente esempio di policy IAM consente ai presidi IAM di effettuare ListRulesrichieste solo se il valore specificato per il parametro di `ResourceType` richiesta è`EBS_SNAPSHOT`. Ciò consente al principale di elencare le regole di conservazione solo per gli snapshot e impedisce loro di elencare le regole di conservazione per qualsiasi altro tipo di risorsa.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:ListRules"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Chiave di condizione **`rbin:Attribute/ResourceType`**

La chiave `rbin:Attribute/ResourceType` condizionale può essere utilizzata per filtrare l'accesso a DeleteRuleGetRule, UpdateRule, LockRule, UnlockRule, TagResourceUntagResource, e ListTagsForResourcele richieste in base al valore dell'`ResourceType`attributo della regola di conservazione.

Esempio 1 - UpdateRule

Il seguente esempio di policy IAM consente ai responsabili IAM di effettuare UpdateRulerichieste solo se l'`ResourceType`attributo della regola di conservazione richiesta è `EBS_SNAPSHOT` o`EC2_IMAGE`. Ciò consente al principale di aggiornare le regole di conservazione solo per gli snapshot e le AMI.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:UpdateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
```

```
                    "rbin:Attribute/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Esempio 2 - DeleteRule

Il seguente esempio di policy IAM consente ai responsabili IAM di effettuare DeleteRulerichieste solo se l'`ResourceType`attributo della regola di conservazione richiesta è`EBS_SNAPSHOT`. Ciò consente al principale di eliminare le regole di conservazione solo per gli snapshot e le AMI.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:DeleteRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Lavorare con le regole di conservazione

Per abilitare e utilizzare Recycle Bin, devi creare regole di conservazione nelle AWS regioni in cui desideri proteggere le tue risorse. Le regole di conservazione specificano le seguenti informazioni:

- Il tipo di risorsa da proteggere.
- Le risorse che vuoi mantenere nel Cestino di riciclaggio quando vengono eliminate.
- Il periodo di conservazione durante il quale mantenere le risorse nel Cestino di riciclaggio prima che vengano eliminate definitivamente.

Con il Cestino di riciclaggio puoi creare due tipi di regole di conservazione:

- Regole di conservazione a livello di tag: una regola di conservazione a livello di tag usa i tag delle risorse per identificare le risorse che devono essere mantenute nel Cestino di riciclaggio. Per ogni regola di conservazione, è necessario specificare una o più coppie di chiavi e valori di tag. Le risorse del tipo specificato taggate con almeno una delle coppie chiave-valore di tag specificate nella regola di conservazione vengono mantenute automaticamente nel Cestino di riciclaggio al momento dell'eliminazione. Puoi usare questo tipo di regola di conservazione se desideri proteggere risorse specifiche nel tuo account in base ai relativi tag.
- Regole di conservazione a livello di Regione: una regola di conservazione a livello di Regione non ha alcun tag di risorsa specificato. Si applica a tutte le risorse del tipo specificato nella regione in cui viene creata la regola, anche se le risorse non sono taggate. Puoi usare questo tipo di regola di conservazione se desideri proteggere tutte le risorse di un tipo specifico in una Regione specifica.

Dopo aver creato una regola di conservazione, le risorse che corrispondono ai criteri vengono conservate automaticamente nel Cestino di riciclaggio per il periodo specificato quando vengono eliminate.

Argomenti

Creazione di una regola di conservazione

Quando crei una regola di conservazione, devi specificare i seguenti parametri obbligatori:

- Il tipo di risorsa che deve essere protetto dalla regola di conservazione.

- Le risorse che devono essere protette dalla regola di conservazione. Puoi creare regole di conservazione a livello di tag e a livello di Regione.
  - Per creare una regola di conservazione a livello di tag, specifica i tag delle risorse che identificano le risorse da proteggere. Puoi specificare fino a 50 tag per ogni regola e aggiungere la stessa coppia chiave-valore di tag a un massimo di 5 regole di conservazione.
  - Per creare una regola di conservazione a livello di Regione, non specificare alcuna coppia chiave-valore di tag. In questo caso, tutte le risorse del tipo specificato sono protette.
- Il periodo per il quale conservare le risorse nel cestino dopo l'eliminazione. Il periodo può essere fino a 1 anno (365 giorni).

È inoltre possibile specificare i parametri opzionali seguenti:

- Un nome facoltativo per la regola di conservazione. Il nome può contenere fino a 255 caratteri.
- Una descrizione opzionale per la regola di conservazione. La descrizione può contenere un massimo di 255 caratteri.

> **Note**
>
> Ti consigliamo di non includere informazioni di identificazione personali, riservate o sensibili nella descrizione delle regole di conservazione.

- I tag delle regole di conservazione facoltativi per identificare e organizzare le regole di conservazione. È possibile assegnare fino a 50 tag a ciascuna regola.

È inoltre possibile bloccare le regole di conservazione al momento della creazione. Se blocchi una regola di conservazione al momento della creazione, devi specificare anche il periodo di ritardo dello sblocco, che può essere compreso tra 7 e 30 giorni. Le regole di conservazione rimangono sbloccate per impostazione predefinita, a meno che non vengano bloccate esplicitamente.

Le regole di conservazione funzionano solo nelle regioni in cui sono state create. Se si desidera utilizzare il Cestino di riciclaggio in altre regioni, si dovrà creare regole di conservazione aggiuntive in tali regioni.

È possibile creare una regola di conservazione del Cestino di riciclaggio utilizzando uno dei metodi descritti di seguito.

Recycle Bin console

Come creare una regola di conservazione

1. Aprire la console del Cestino di riciclaggio all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione scegli Retention rules (Regole di conservazione), quindi Create retention rule (Crea regola di conservazione).
3. Nella sezione Rule details (Dettagli regola), completare le seguenti operazioni:
   a. (Facoltativo) Per Retention rule name (Nome regola di conservazione) inserire un nome descrittivo per la regola di conservazione.
   b. (Facoltativo) Per Retention rule description (Descrizione regola di conservazione) inserire una breve descrizione per la regola.
4. Nella sezione Rule settings (Impostazioni regole), procedere nel seguente modo:
   a. Per Resource type (Tipo di risorsa), seleziona il tipo di risorsa per la regola di conservazione da proteggere. La regola di conservazione manterrà solo risorse di questo tipo nel Cestino di riciclaggio.
   b. Esegui una di queste operazioni:
      - Per creare una regola di conservazione a livello di regione che corrisponda a tutte le risorse del tipo specificato eliminate nella Regione, seleziona Apply to all resources (Applica a tutte le risorse). La regola di conservazione manterrà tutte le risorse presenti nel Cestino di riciclaggio al momento dell'eliminazione, anche se non hanno tag.
      - Per creare una regola di conservazione a livello di tag, per Resource tags to match (Tag delle risorse da associare), inserisci le coppie chiave-valore di tag da usare per identificare le risorse del tipo specificato che devono essere conservate nel Cestino di riciclaggio. La regola di conservazione conserverà solo le risorse del tipo specificato che dispongono di almeno una delle coppie chiave-valore di tag specificate.
   c. Per Retention period (Periodo di conservazione), inserire il numero di giorni per i quali la regola di conservazione deve mantenere le risorse nel Cestino di riciclaggio.
5. (Facoltativo) Per bloccare la regola di conservazione, per Rule lock settings (Impostazioni di blocco delle regole), seleziona Lock (Blocca), quindi per Unlock delay period (Periodo di ritardo dello sblocco) specifica il periodo di ritardo dello sblocco in giorni. Una regola di conservazione bloccata non può essere modificata o eliminata. Per modificare o eliminare la

regola, è necessario prima sbloccarla e quindi attendere la scadenza del periodo di ritardo dello sblocco. Per ulteriori informazioni, consulta Blocco delle regole di conservazione

Per lasciare sbloccata la regola di conservazione, per Rule lock settings (Impostazioni di blocco della regola) mantieni selezionata l'opzione Unlock (Sblocca). Una regola di conservazione sbloccata può essere modificata o eliminata in qualsiasi momento. Per ulteriori informazioni, consulta Sblocco delle regole di conservazione.

6. (Facoltativo) Nella sezione Tags (Tag), completare le seguenti operazioni:
   - Per taggare la regola con i tag personalizzati, scegliere Add tag (Aggiungi tag), quindi inserire la coppia chiave-valore del tag.
7. Scegliere Create retention rule (Crea regola di conservazione).

AWS CLI

Come creare una regola di conservazione

Utilizzare il comando create-rule della AWS CLI . Per `--retention-period`, specificare il numero di giorni durante i quali mantenere gli snapshot eliminati nel Cestino di riciclaggio. Per `--resource-type`, specifica `EBS_SNAPSHOT` per gli snapshot o `EC2_IMAGE` per le AMI. Per creare una regola di conservazione a livello di tag, per `--resource-tags`, specificare i tag da utilizzare per identificare gli snapshot che devono essere conservati. Per creare una regola di conservazione a livello di Regione, ometti `--resource-tags`. Per bloccare una regola di conservazione, includi `--lock-configuration` e specifica il periodo di ritardo dello sblocco in giorni.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description" \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

Esempio 1

Il comando di esempio seguente crea una regola di conservazione sbloccata a livello di Regione che conserva tutti gli snapshot eliminati per un periodo di 7 giorni.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots"
```

Esempio 2

Il comando di esempio seguente crea una regola a livello di tag che conserva tutti gli snapshot eliminati taggati con `purpose=production` per un periodo di 7 giorni.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match snapshots with a specific tag" \
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

Esempio 3

Il comando di esempio seguente crea una regola di conservazione bloccata a livello di Regione che conserva tutti gli snapshot eliminati per un periodo di 7 giorni. La regola di conservazione è bloccata con un periodo di ritardo dello sblocco di 7 giorni.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots" \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

Visualizzazione delle regole di conservazione del Cestino di riciclaggio

Puoi visualizzare le regole di conservazione del Cestino di riciclaggio utilizzando uno dei metodi descritti di seguito.

Recycle Bin console

Come visualizzare le regole di conservazione

1. Aprire la console del Cestino di riciclaggio all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegli Retention rules (Regole di conservazione).

3. La griglia elenca tutte le regole di conservazione per la regione selezionata. Per visualizzare ulteriori informazioni su una regola di conservazione specifica, selezionare la regola nella griglia.

AWS CLI

Come visualizzare tutte le regole di conservazione

Usa il comando della AWS CLI list-rules e per `--resource-type` specifica `EBS_SNAPSHOT` per gli snapshot o `EC2_IMAGE` per le AMI.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT|EC2_IMAGE
```

Esempio

Il comando di esempio seguente fornisce un elenco di tutte le regole di conservazione che mantengono gli snapshot.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT
```

Come visualizzare le informazioni per una regola di conservazione specifica

Utilizzate il comando get-rule AWS CLI .

```
aws rbin get-rule --identifier rule_ID
```

Esempio

Il seguente comando di esempio fornisce informazioni sulla regola di conservazione `pwxIkFcvge4`.

```
aws rbin get-rule --identifier pwxIkFcvge4
```

Aggiornamento delle regole di conservazione

È possibile aggiornare la descrizione, i tag delle risorse e il periodo di conservazione di una regola di conservazione non bloccata in qualsiasi momento dopo la creazione. Non è possibile aggiornare il tipo di risorsa o il periodo di ritardo dello sblocco di una regola di conservazione, anche se la regola di conservazione è sbloccata.

Non è possibile aggiornare in alcun modo una regola di conservazione bloccata. Se hai la necessità di modificare una regola di conservazione bloccata, prima devi sbloccarla, dopodiché devi attendere la scadenza del periodo di ritardo dello sblocco.

Se hai la necessità di modificare il periodo di ritardo dello sblocco per una regola di conservazione bloccata, devi sbloccare la regola di conservazione e attendere la scadenza del periodo di ritardo dello sblocco corrente. Quando il periodo di ritardo dello sblocco è scaduto, è necessario bloccare nuovamente la regola di conservazione e specificare il nuovo periodo di ritardo dello sblocco.

> **Note**
>
> Ti consigliamo di non includere informazioni di identificazione personali, riservate o sensibili nella descrizione delle regole di conservazione.

Dopo aver aggiornato una regola di conservazione, le modifiche vengono applicate solo alle nuove risorse conservate. Le modifiche non influiscono sulle risorse inviate precedentemente al Cestino di riciclaggio. Ad esempio, se aggiorni il periodo di conservazione di una regola di conservazione, vengono conservati per il nuovo periodo di conservazione solo gli snapshot eliminati dopo l'aggiornamento. Gli snapshot inviati al Cestino di riciclaggio prima dell'aggiornamento saranno ancora conservati per il periodo di conservazione precedente (vecchio valore).

È possibile aggiornare una regola di conservazione utilizzando uno dei seguenti metodi.

Recycle Bin console

Come aggiornare una regola di conservazione

1. Aprire la console del Cestino di riciclaggio all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegli Retention rules (Regole di conservazione).
3. Nella griglia, selezionare la regola di conservazione da aggiornare e scegliere Actions (Operazioni), Edit retention rule (Modifica regola di conservazione).
4. Nella sezione Rule details (Dettagli regola), aggiornare i campi Retention rule name (Nome regola di conservazione) e Retention rule description (Descrizione regola di conservazione) in base alle necessità.

5. Nella sezione Rule settings (Impostazioni delle regole), aggiorna i campi Resource type (Tipo di risorsa), Resource tags to match (Tag delle risorse da associare) e Retention period (Periodo di conservazione) in base alle tue esigenze.
6. Nella sezione Tags (Tag), aggiungere o rimuovere i tag delle regole di conservazione in base alle necessità.
7. Scegliere Save retention rule (Salva una regola di conservazione).

AWS CLI

Come aggiornare una regola di conservazione

Utilizzare il comando update-rule della AWS CLI . Per `--identifier`, specifica l'ID della regola di conservazione da aggiornare per `--resource-types`, specifica `EBS_SNAPSHOT` per gli snapshot o `EC2_IMAGE` per le AMI.

```
aws rbin update-rule \
--identifier rule_ID \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description"
```

Esempio

Il comando di esempio seguente aggiorna la regola di conservazione `6lsJ2Fa9nh9` in modo da mantenere tutti gli snapshot per 7 giorni e aggiorna la relativa descrizione.

```
aws rbin update-rule \
--identifier 6lsJ2Fa9nh9 \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Retain for three weeks"
```

Blocco delle regole di conservazione

Il cestino consente di bloccare le regole di conservazione a livello di Regione in qualsiasi momento.

> **Note**
>
> Non è possibile bloccare le regole di conservazione a livello di tag.

Una regola di conservazione bloccata non può essere modificata o eliminata, nemmeno dagli utenti che dispongono delle autorizzazioni IAM richieste. Puoi bloccare le regole di conservazione per proteggerle da modifiche ed eliminazioni accidentali o dannose.

Quando blocchi una regola di conservazione, devi specificare un periodo di ritardo dello sblocco. Questo è il periodo di tempo che devi attendere dopo avere sbloccato la regola di conservazione prima di poterla modificare o eliminare. Non è possibile modificare o eliminare la regola di conservazione durante il periodo di ritardo dello sblocco. È possibile modificare o eliminare la regola di conservazione solo dopo la scadenza del periodo di ritardo dello sblocco.

Non è possibile modificare il periodo di ritardo dello sblocco dopo il blocco della regola di conservazione. Se le autorizzazioni del tuo account sono state compromesse, il periodo di ritardo dello sblocco ti offre più tempo per rilevare e rispondere alle minacce alla sicurezza. La durata di questo periodo dovrebbe essere superiore al tempo necessario per identificare e rispondere alle violazioni della sicurezza. Per impostare la durata corretta, puoi esaminare i precedenti incidenti di sicurezza e il tempo che è servito per identificare e porre rimedio a una violazione dell'account.

Ti consigliamo di utilizzare EventBridge le regole di Amazon per notificarti le modifiche allo stato di blocco delle regole di conservazione. Per ulteriori informazioni, consulta Monitora Recycle Bin con Amazon EventBridge.

Considerazioni

- È possibile bloccare solo le regole di conservazione a livello di Regione.
- È possibile bloccare una regola di conservazione sbloccata in qualsiasi momento.
- Il periodo di ritardo dello sblocco deve essere compreso tra 7 e 30 giorni.
- È possibile bloccare nuovamente una regola di conservazione durante il periodo di ritardo dello sblocco. Il nuovo blocco di una regola di conservazione ripristina il periodo di ritardo dello sblocco.

È possibile creare una regola di conservazione a livello di Regione utilizzando uno dei metodi descritti di seguito.

Recycle Bin console

Blocco di una regola di conservazione

1. Apri la console del cestino all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegliere Retention rules (Regole di conservazione).
3. Nella griglia, seleziona la regola di conservazione sbloccata da bloccare e scegli Actions (Operazioni), Edit retention rule lock (Modifica blocco della regola di conservazione).
4. Nella schermata Edit retention rule lock (Modifica blocco della regola di conservazione), scegli Lock (Blocca), quindi per Unlock delay period (Periodo di ritardo dello sblocco) specifica il periodo di ritardo dello sblocco in giorni.
5. Seleziona la casella di controllo I acknowledge that locking the retention rule will prevent it from being modified or deleted (Riconosco che il blocco della regola di conservazione ne impedirà la modifica o l'eliminazione), quindi scegli Save (Salva).

AWS CLI

Blocco di una regola di conservazione sbloccata

Utilizza il comando lock-rule della AWS CLI . Per `--identifier`, specifica l'ID della regola di conservazione da bloccare. Per `--lock-configuration`, specifica il periodo di ritardo dello sblocco in giorni.

```
aws rbin lock-rule \
--identifier rule_ID \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

Esempio

Il seguente comando di esempio blocca la regola di conservazione `6lsJ2Fa9nh9` e imposta il periodo di ritardo dello sblocco su 15 giorni.

```
aws rbin lock-rule \
--identifier 6lsJ2Fa9nh9 \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

Sblocco delle regole di conservazione

Non è possibile eliminare o modificare una regola di conservazione bloccata. Se hai la necessità di modificare una regola di conservazione bloccata, prima devi sbloccarla. Dopo avere sbloccato la regola di conservazione, è necessario attendere la scadenza del periodo di ritardo dello sblocco prima di poterla modificare o eliminare. Non è possibile modificare o eliminare la regola di conservazione durante il periodo di ritardo dello sblocco.

Una regola di conservazione sbloccata può essere modificata ed eliminata in qualsiasi momento da un utente che dispone delle autorizzazioni IAM richieste. Lasciare sbloccate le regole di conservazione potrebbe esporle a modifiche ed eliminazioni accidentali o dannose.

Considerazioni

- È possibile bloccare nuovamente una regola di conservazione durante il periodo di ritardo dello sblocco.
- È possibile bloccare nuovamente una regola di conservazione dopo la scadenza del periodo di ritardo dello sblocco.
- Non è possibile aggirare il periodo di ritardo dello sblocco.
- Non è possibile modificare il periodo di ritardo dello sblocco dopo il blocco iniziale.

Ti consigliamo di utilizzare EventBridge le regole di Amazon per notificarti le modifiche allo stato di blocco delle regole di conservazione. Per ulteriori informazioni, consulta Monitora Recycle Bin con Amazon EventBridge.

È possibile sbloccare una regola di conservazione bloccata a livello di Regione utilizzando uno dei metodi descritti di seguito.

Recycle Bin console

Sblocco di una regola di conservazione

1. Apri la console del cestino all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegliere Retention rules (Regole di conservazione).
3. Nella griglia, seleziona la regola di conservazione bloccata da sbloccare e scegli Actions (Operazioni), Edit retention rule lock (Modifica blocco della regola di conservazione).
4. Nella schermata Edit retention rule lock (Modifica blocco della regola di conservazione), scegli Unlock (Sblocca), quindi scegli Save (Salva).

AWS CLI

Sblocco di una regola di conservazione bloccata

Utilizza il comando unlock-rule della AWS CLI . Per `--identifier`, specifica l'ID della regola di conservazione da sbloccare.

```
aws rbin unlock-rule \
--identifier rule_ID
```

Esempio

Il seguente comando di esempio sblocca la regola di conservazione `6lsJ2Fa9nh9`.

```
aws rbin unlock-rule \
--identifier 6lsJ2Fa9nh9
```

Regole di conservazione dei tag

È possibile assegnare tag personalizzati alle tue regole di conservazione in modo da categorizzarle in diversi modi, ad esempio a seconda dello scopo, del proprietario o dell'ambiente. Questa procedura ti aiuta a trovare in modo efficiente una regola di conservazione specifica grazie ai tag personalizzati che hai assegnato.

È possibile assegnare un tag a una regola di conservazione utilizzando uno dei seguenti metodi.

Recycle Bin console

Come aggiungere un tag a una regola di conservazione

1. Aprire la console del Cestino di riciclaggio all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegli Retention rules (Regole di conservazione).
3. Selezionare la regola di conservazione da taggare, scegliere la scheda Tags (Tag), quindi scegliere Manage tags (Gestisci tag).
4. Selezionare Aggiungi tag. In Key (Chiave), inserire il nome della chiave. In Value (Valore), inserire il valore del tag.
5. Scegliere Save (Salva).

AWS CLI

Come aggiungere un tag a una regola di conservazione

Usa il comando tag-resource AWS CLI . Per `--resource-arn`, specificare il nome della risorsa Amazon (ARN) della regola di conservazione da taggare e per `--tags`, specificare la coppia chiave-valore di tag.

```
aws rbin tag-resource \
--resource-arn retention_rule_arn \
--tags key=tag_key,value=tag_value
```

Esempio

Il seguente comando di esempio aggiunge alla regola di conservazione `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3` il tag `purpose=production`.

```
aws rbin tag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3 \
--tags key=purpose,value=production
```

Visualizzazione dei tag delle regole di conservazione

È possibile visualizzare i tag assegnati a una regola di conservazione utilizzando uno dei seguenti metodi.

Recycle Bin console

Come visualizzare i tag per una regola di conservazione

1. Aprire la console del Cestino di riciclaggio all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegli Retention rules (Regole di conservazione).
3. Seleziona la regola di conservazione per cui visualizzare i tag, quindi scegli la scheda Tags (Tag).

AWS CLI

Come visualizzare i tag assegnati a una regola di conservazione

Utilizza il comando list-tags-for-resource. AWS CLI Per `--resource-arn`, specificare l'ARN della regola di conservazione.

```
aws rbin list-tags-for-resource \
--resource-arn retention_rule_arn
```

Esempio

L'esempio seguente di comando elenca i tag per la regola di conservazione `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3`.

```
aws rbin list-tags-for-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3
```

Rimozione di tag dalle regole di conservazione

È possibile rimuovere i tag da una regola di conservazione utilizzando uno dei metodi descritti di seguito.

Recycle Bin console

Come rimuovere un tag da una regola di conservazione

1. Aprire la console del Cestino di riciclaggio all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegli Retention rules (Regole di conservazione).
3. Selezionare la regola di conservazione da cui rimuovere il tag, scegli la scheda Tags (Tag), quindi scegli Manage tags (Gestisci tag).
4. Scegliere Remove (Rimuovi) accanto al tag da rimuovere.
5. Scegliere Save (Salva).

AWS CLI

Come rimuovere un tag da una regola di conservazione

Utilizzare il comando untag-resource della AWS CLI . Per `--resource-arn`, specificare l'ARN della regola di conservazione. Per `--tagkeys`, specificare le chiavi di tag dei tag da rimuovere.

```
aws rbin untag-resource \
--resource-arn retention_rule_arn \
--tagkeys tag_key
```

Esempio

Il seguente comando di esempio rimuove i tag con una chiave tag `purpose` dalla regola di conservazione `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3`.

```
aws rbin untag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tagkeys purpose
```

Eliminazione delle regole di conservazione del Cestino di riciclaggio

È possibile eliminare una regola di conservazione in qualsiasi momento. Quando elimini una regola di conservazione, questa non conserva più le nuove risorse nel Cestino dopo la loro eliminazione. Le risorse inviate al Cestino di riciclaggio prima dell'eliminazione della regola di conservazione continueranno a essere conservate nel Cestino di riciclaggio in base al periodo di conservazione definito nella regola. Quando il periodo scade, la risorsa viene eliminata definitivamente dal Cestino di riciclaggio.

È possibile eliminare una regola di conservazione utilizzando uno dei seguenti metodi.

Recycle Bin console

Come eliminare una regola di conservazione

1. Aprire la console del Cestino di riciclaggio all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegli Retention rules (Regole di conservazione).
3. Nella griglia, seleziona la regola di conservazione da eliminare e scegli Actions (Operazioni), Delete retention rule (Elimina regola di conservazione).
4. Quando richiesto, inserire il messaggio di conferma e scegliere Delete retention rule (Elimina regola di conservazione).

AWS CLI

Come eliminare una regola di conservazione

Utilizzare il comando delete-rule della AWS CLI . Per `--identifier`, specificare l'ID della regola di conservazione da eliminare.

```
aws rbin delete-rule --identifier rule_ID
```

Esempio

Il seguente comando di esempio elimina la regola di conservazione `6lsJ2Fa9nh9`.

```
aws rbin delete-rule --identifier 6lsJ2Fa9nh9
```

Utilizzo delle risorse nel Cestino di riciclaggio

Il Cestino di riciclaggio supporta i tipi di risorse seguenti:

- Snapshot Amazon EBS
- Amazon Machine Image (AMI) Amazon EBS-backed

Attività

- Ripristino degli snapshot dal Cestino di riciclaggio
- Ripristino delle AMI dal Cestino di riciclaggio

Ripristino degli snapshot dal Cestino di riciclaggio

Il Cestino di riciclaggio è una caratteristica di ripristino dei dati che consente di ripristinare snapshot Amazon EBS e AMI EBS-backed eliminati accidentalmente. Quando si usa il Cestino di riciclaggio, se le risorse vengono eliminate, vengono conservate al suo interno per un periodo di tempo specificato, prima di essere eliminate definitivamente.

Puoi ripristinare una risorsa dal Cestino di riciclaggio in qualsiasi momento, prima della scadenza del periodo di conservazione. Quando ripristini una risorsa dal Cestino di riciclaggio, essa viene rimossa dal Cestino di riciclaggio e puoi usarla nello stesso modo in cui usi qualsiasi altra risorsa dello stesso tipo nel tuo account. Se il periodo di conservazione scade e la risorsa non viene ripristinata, viene eliminata definitivamente dal Cestino di riciclaggio e non è più disponibile per il ripristino.

Gli snapshot nel Cestino di riciclaggio vengono fatturati allo stesso costo dei normali snapshot del tuo account. Non sono previsti costi aggiuntivi per l'utilizzo di Cestino di riciclaggio e regole di conservazione. Per ulteriori informazioni, consulta Prezzi di Amazon EBS.

Per ulteriori informazioni, consulta Cestino.

Argomenti

- Autorizzazioni per l'uso degli snapshot nel Cestino di riciclaggio
- Visualizzazione degli snapshot nel Cestino di riciclaggio
- Ripristino degli snapshot dal Cestino di riciclaggio

Autorizzazioni per l'uso degli snapshot nel Cestino di riciclaggio

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per usare gli snapshot che si trovano nel Cestino di riciclaggio. Per permettere agli utenti di utilizzare queste risorse, è necessario creare delle policy IAM che forniscano l'autorizzazione per l'uso di risorse e operazioni API specifiche. Dopo aver creato le politiche, è necessario aggiungere le autorizzazioni agli utenti, ai gruppi o ai ruoli.

Per visualizzare e ripristinare gli snapshot che si trovano nel Cestino di riciclaggio, gli utenti devono disporre delle autorizzazioni seguenti:

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Per gestire i tag per gli snapshot nel Cestino di riciclaggio, gli utenti hanno bisogno delle seguenti autorizzazioni aggiuntive.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Per usare la console del Cestino di riciclaggio, gli utenti devono disporre dell'autorizzazione `ec2:DescribeTags`.

Di seguito è riportata una policy IAM di esempio. Include l'autorizzazione `ec2:DescribeTags` per gli utenti della console e le autorizzazioni `ec2:CreateTags` e `ec2:DeleteTags` per la gestione dei tag. Se non sono necessarie, puoi rimuovere le autorizzazioni dalla policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListSnapshotsInRecycleBin",
            "ec2:RestoreSnapshotFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
      },

    ]
}
```

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.

- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Per ulteriori informazioni sulle autorizzazioni necessarie per utilizzare il Cestino di riciclaggio, consulta Autorizzazioni per usare il Cestino di riciclaggio e le regole di conservazione.

Visualizzazione degli snapshot nel Cestino di riciclaggio

Mentre uno snapshot si trova nel Cestino di riciclaggio, è possibile visualizzare informazioni limitate su di esso, tra cui:

- L'ID della snapshot.
- La descrizione degli snapshot.
- L'ID del volume da cui è stato creato lo snapshot.
- Data e ora in cui lo snapshot è stato eliminato e inserito nel Cestino di riciclaggio.
- La data e l'ora in cui scade il periodo di conservazione. Lo snapshot verrà eliminato definitivamente dal Cestino di riciclaggio in questo momento.

È possibile visualizzare gli snapshot nel Cestino di riciclaggio utilizzando uno dei metodi descritti di seguito.

Recycle Bin console

Come visualizzare gli snapshot nel Cestino di riciclaggio tramite la console

1. Apri la console del cestino all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegli Recycle Bin (Cestino).
3. La griglia riporta tutti gli snapshot attualmente presenti nel Cestino di riciclaggio. Per visualizzare i dettagli di uno snapshot specifico, selezionarlo nella griglia e scegliere Actions (Operazioni), View details (Visualizza dettagli).

AWS CLI

Per visualizzare le istantanee nel Cestino utilizzando il AWS CLI

Utilizzare il comando list-snapshots-in-recycle-bin AWS CLI . Includere l'opzione `--snapshot-id` per visualizzare uno snapshot specifico. Oppure omettere l'opzione `--snapshot-id` per visualizzare tutti gli snapshot presenti nel Cestino di riciclaggio.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Ad esempio, il comando seguente fornisce informazioni sullo snapshot `snap-01234567890abcdef` nel Cestino di riciclaggio.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Output di esempio:

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

Ripristino degli snapshot dal Cestino di riciclaggio

Non è possibile utilizzare uno snapshot in alcun modo mentre si trova nel Cestino di riciclaggio. Per utilizzare lo snapshot, è necessario prima ripristinarlo. Quando si ripristina uno snapshot dal Cestino di riciclaggio, lo snapshot diventa immediatamente disponibile per l'uso e viene rimosso dal Cestino. Dopo averlo ripristinato, potrà essere utilizzato nello stesso modo in cui qualsiasi altro snapshot viene utilizzato nel proprio account.

È possibile ripristinare uno snapshot dal Cestino di riciclaggio utilizzando uno dei metodi descritti di seguito.

Recycle Bin console

Come ripristinare uno snapshot dal Cestino di riciclaggio tramite la console

1. Apri la console del cestino all'indirizzo https://console.aws.amazon.com/rbin/home/
2. Nel pannello di navigazione, scegli Recycle Bin (Cestino).
3. La griglia riporta tutti gli snapshot attualmente presenti nel Cestino di riciclaggio. Selezionare lo snapshot da ripristinare e scegliere Recover (Recupera).
4. Quando richiesto, scegliere Recover (Ripristino).

AWS CLI

Per ripristinare un'istantanea eliminata dal Cestino utilizzando il AWS CLI

Utilizzare il comando restore-snapshot-from-recycle-bin AWS CLI . Per `--snapshot-id`, specificare l'ID dello snapshot da ripristinare.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Ad esempio, il comando seguente ripristina lo snapshot `snap-01234567890abcdef` dal Cestino di riciclaggio.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

Output di esempio:

```
{
    "SnapshotId": "snap-01234567890abcdef",
    "Description": "Monthly data backup snapshot",
    "Encrypted": false,
    "OwnerId": "111122223333",
    "Progress": "100%",
    "StartTime": "2021-12-01T13:00:00.000000+00:00",
    "State": "recovering",
    "VolumeId": "vol-ffffffff",
    "VolumeSize": 30
}
```

Ripristino delle AMI dal Cestino di riciclaggio

Il Cestino di riciclaggio è una caratteristica di ripristino dei dati che consente di ripristinare snapshot Amazon EBS e AMI EBS-backed eliminati accidentalmente. Quando si usa il Cestino di riciclaggio, se le risorse vengono eliminate, vengono conservate al suo interno per un periodo di tempo specificato, prima di essere eliminate definitivamente.

Puoi ripristinare una risorsa dal Cestino di riciclaggio in qualsiasi momento, prima della scadenza del periodo di conservazione. Quando ripristini una risorsa dal Cestino di riciclaggio, essa viene rimossa dal Cestino di riciclaggio e puoi usarla nello stesso modo in cui usi qualsiasi altra risorsa dello stesso tipo nel tuo account. Se il periodo di conservazione scade e la risorsa non viene ripristinata, viene eliminata definitivamente dal Cestino di riciclaggio e non è più disponibile per il ripristino.

Per le AMI nel Cestino di riciclaggio non sono previsti costi aggiuntivi.

Per ulteriori informazioni, consulta Cestino.

Argomenti

Autorizzazioni per l'uso delle AMI nel Cestino di riciclaggio

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per usare le AMI che si trovano nel Cestino di riciclaggio. Per permettere agli utenti di utilizzare queste risorse, è necessario creare delle policy IAM che forniscano l'autorizzazione per l'uso di risorse e operazioni API specifiche. Dopo aver creato le politiche, è necessario aggiungere le autorizzazioni agli utenti, ai gruppi o ai ruoli.

Per visualizzare e ripristinare le AMI che si trovano nel Cestino di riciclaggio, gli utenti devono disporre delle autorizzazioni seguenti:

- `ec2:ListImagesInRecycleBin`
- `ec2:RestoreImageFromRecycleBin`

Per gestire i tag per le AMI nel Cestino di riciclaggio, gli utenti devono disporre delle autorizzazioni aggiuntive seguenti.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Per usare la console del Cestino di riciclaggio, gli utenti devono disporre dell'autorizzazione `ec2:DescribeTags`.

Di seguito è riportata una policy IAM di esempio. Include l'autorizzazione `ec2:DescribeTags` per gli utenti della console e le autorizzazioni `ec2:CreateTags` e `ec2:DeleteTags` per la gestione dei tag. Se non sono necessarie, puoi rimuovere le autorizzazioni dalla policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListImagesInRecycleBin",
            "ec2:RestoreImageFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region::image/*"
      }
    ]
}
```

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Per ulteriori informazioni sulle autorizzazioni necessarie per utilizzare il Cestino di riciclaggio, consulta Autorizzazioni per usare il Cestino di riciclaggio e le regole di conservazione.

Visualizzazione delle AMI nel Cestino di riciclaggio

Mentre un'AMI si trova nel Cestino di riciclaggio, puoi visualizzare informazioni limitate su di essa, tra cui:

- Nome, descrizione e ID univoco dell'AMI.
- Data e ora in cui l'AMI è stata eliminata e inserita nel Cestino di riciclaggio.
- La data e l'ora in cui scade il periodo di conservazione. L'AMI verrà eliminata definitivamente in questo momento.

Puoi visualizzare le AMI nel Cestino di riciclaggio usando uno dei metodi seguenti.

Recycle Bin console

Per visualizzare le AMI eliminate nel Cestino di riciclaggio tramite la console

1. Apri la console del Cestino di riciclaggio all'indirizzo console.aws.amazon.com/rbin/home/.
2. Nel pannello di navigazione, scegli Recycle Bin (Cestino).
3. Nella griglia sono elencate tutte le risorse che attualmente si trovano nel Cestino di riciclaggio. Per visualizzare i dettagli di un'AMI specifica, selezionala nella griglia e scegli Actions (Operazioni), View details (Visualizza dettagli).

AWS CLI

Per visualizzare le AMI eliminate nel Cestino utilizzando AWS CLI

Utilizzare il comando list-images-in-recycle-bin AWS CLI . Per visualizzare AMI specifiche, includi l'opzione `--image-id` e specifica gli ID delle AMI da visualizzare. Puoi specificare fino a 20 ID in un'unica richiesta.

Per visualizzare tutte le AMI presenti nel Cestino di riciclaggio, ometti l'opzione `--image-id`. Se non specifichi un valore per `--max-items`, il comando restituisce 1.000 elementi per pagina, per impostazione predefinita. Per ulteriori informazioni, consulta Pagination (Paginazione) nella Amazon EC2 API Reference.

```
aws ec2 list-images-in-recycle-bin --image-id ami_id
```

Ad esempio, il comando seguente fornisce informazioni sull'AMI `ami-01234567890abcdef` nel Cestino di riciclaggio.

```
aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

Output di esempio:

```
{
    "Images": [
        {
            "ImageId": "ami-0f740206c743d75df",
            "Name": "My AL2 AMI",
            "Description": "My Amazon Linux 2 AMI",
            "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
            "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
        }
    ]
}
```

> **Important**
>
> Se ricevi il seguente errore, potrebbe essere necessario aggiornare la AWS CLI versione. Per ulteriori informazioni, consulta la sezione Errori di comando non trovato.

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

Ripristino delle AMI dal Cestino di riciclaggio

Non puoi usare un'AMI in alcun modo mentre si trova nel Cestino di riciclaggio. Per usare l'AMI, devi prima ripristinarla. Quando ripristini un'AMI dal Cestino di riciclaggio, essa diventa immediatamente disponibile per l'uso e viene rimosso dal Cestino di riciclaggio. Puoi usare un'AMI ripristinata nello stesso modo in cui usi qualsiasi altra AMI nel tuo account.

Puoi ripristinare un'AMI dal Cestino di riciclaggio usando uno dei metodi descritti di seguito.

Recycle Bin console

Per ripristinare un'AMI dal Cestino di riciclaggio tramite la console

1. Apri la console del Cestino di riciclaggio all'indirizzo console.aws.amazon.com/rbin/home/.
2. Nel pannello di navigazione, scegli Recycle Bin (Cestino).
3. Nella griglia sono elencate tutte le risorse che attualmente si trovano nel Cestino di riciclaggio. Seleziona l'AMI da ripristinare e scegli Recover (Ripristina).
4. Quando richiesto, scegliere Recover (Ripristino).

AWS CLI

Per ripristinare un AMI eliminato dal Cestino utilizzando AWS CLI

Utilizzare il comando restore-image-from-recycle-bin. AWS CLI Per `--image-id`, specifica l'ID dell'AMI da ripristinare.

```
aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

Ad esempio, il comando seguente ripristina l'AMI `ami-01234567890abcdef` dal Cestino di riciclaggio.

```
aws ec2 restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

Se il comando viene eseguito correttamente, non restituisce alcun output.

> **Important**
>
> Se ricevi il seguente errore, potrebbe essere necessario aggiornare la AWS CLI versione. Per ulteriori informazioni, consulta la sezione Errori di comando non trovato.
>
> ```
> aws.exe: error: argument operation: Invalid choice, valid choices are: ...
> ```

Monitoraggio del cestino

È possibile utilizzare le seguenti funzionalità per monitorare il cestino.

Argomenti

- Monitora Recycle Bin con Amazon EventBridge
- Monitora Recycle Bin utilizzando AWS CloudTrail

Monitora Recycle Bin con Amazon EventBridge

Recycle Bin invia eventi ad Amazon EventBridge per le azioni eseguite sulle regole di conservazione. Con EventBridge, puoi stabilire regole che avviano azioni programmatiche in risposta a questi eventi. Ad esempio, è possibile creare una EventBridge regola che invii una notifica alla posta elettronica quando una regola di conservazione viene sbloccata e entra nel periodo di ritardo dello sblocco. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi.

Gli eventi in EventBridge sono rappresentati come oggetti JSON. I campi univoci per l'evento sono contenuti nella sezione `detail` dell'oggetto JSON. Il campo `event` contiene il nome dell'evento. Il campo `result` contiene lo stato completato dell'operazione che ha attivato l'evento. Per ulteriori informazioni, consulta i modelli di EventBridge eventi di Amazon nella Amazon EventBridge User Guide.

Per ulteriori informazioni su Amazon EventBridge, consulta What Is Amazon EventBridge? nella Amazon EventBridge User Guide.

Eventi

- RuleLocked
- RuleChangeAttempted

- RuleUnlockScheduled
- RuleUnlockingNotice
- RuleUnlocked

RuleLocked

Di seguito è riportato un esempio di evento generato dal cestino quando una regola di conservazione viene bloccata correttamente. Questo evento può essere generato da CreateRulee LockRulerichieste. L'API che ha generato l'evento è indicata nel campo `api-name`.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Locked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "CreateRule"
  }
}
```

RuleChangeAttempted

Di seguito è riportato un esempio di evento generato dal cestino per i tentativi non riusciti di modificare o eliminare una regola bloccata. Questo evento può essere generato da DeleteRulee UpdateRulerichieste. L'API che ha generato l'evento è indicata nel campo `api-name`.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
```

```
  "detail-type": "Recycle Bin Rule Change Attempted",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "DeleteRule"
  }
}
```

RuleUnlockScheduled

Di seguito è riportato un esempio di evento generato dal cestino quando una regola di conservazione viene sbloccata e inizia il relativo periodo di ritardo dello sblocco.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlock Scheduled",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z",
  }
}
```

RuleUnlockingNotice

Di seguito è riportato un esempio di evento generato quotidianamente dal cestino durante il periodo di ritardo dello sblocco di una regola di conservazione fino al giorno prima della scadenza di tale periodo.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocking Notice",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

RuleUnlocked

Di seguito è riportato un esempio di evento generato dal cestino quando il periodo di ritardo dello sblocco di una regola di conservazione scade e la regola di conservazione può essere modificata o eliminata.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
```

```
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

Monitora Recycle Bin utilizzando AWS CloudTrail

Il servizio Recycle Bin è integrato con AWS CloudTrail. CloudTrail è un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio. CloudTrail acquisisce tutte le chiamate API eseguite in Recycle Bin come eventi. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon Simple Storage Service (Amazon S3). Se non configuri un percorso, puoi comunque visualizzare gli eventi di gestione più recenti nella CloudTrail console nella cronologia degli eventi. È possibile utilizzare le informazioni raccolte da CloudTrail per determinare la richiesta effettuata a Recycle Bin, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni in merito CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Informazioni sul cestino in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di evento supportata in Recycle Bin, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Recycle Bin, crea un percorso. Un trail consente di CloudTrail inviare file di registro a un bucket S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il percorso registra gli eventi di tutte le regioni della AWS partizione e consegna i file di registro al bucket S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consultare Panoramica della creazione di un percorso nella Guida per l'utente di AWS CloudTrail .

Operazioni API supportate

Per Recycle Bin, è possibile utilizzare CloudTrail per registrare le seguenti azioni API come eventi di gestione.

- CreateRule
- UpdateRule
- GetRules
- ListRule
- DeleteRule
- TagResource
- UntagResource
- ListTagsForResource
- LockRule
- UnlockRule

Per ulteriori informazioni sulla registrazione degli eventi di gestione, vedere Registrazione degli eventi di gestione dei percorsi nella Guida per l'CloudTrail utente.

Informazioni sull'identità

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta la CloudTrail userIdentityElement.

Informazioni sulle voci dei file di log del Cestino

Un trail è una configurazione che consente la consegna di eventi come file di registro in un bucket S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di

registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Di seguito sono riportati alcuni esempi di voci di CloudTrail registro.

CreateRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:22Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "CreateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
```

```
  },
  "responseElements": {
    "identifier": "jkrnexample"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

GetRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
```

```
  "eventTime": "2021-08-02T21:45:33Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "GetRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

ListRules

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
```

```
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:44:37Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListRules",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "resourceTags": [
      {
        "resourceTagKey": "test",
        "resourceTagValue": "test"
      }
    ]
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


UpdateRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
```

```
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:03Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UpdateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample",
    "retentionPeriod": {
      "retentionPeriodValue": 365,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
```

```
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

DeleteRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:25Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "DeleteRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
```

```
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

TagResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:43:15Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "TagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
```

```
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tags": [
      {
        "key": "purpose",
        "value": "production"
      }
    ]
  },
  "responseElements": null,
  "requestID": "examplee-7962-49ec-8633-795efexample",
  "eventID": "example4-6826-4c0a-bdec-0bab1example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

UntagResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
```

```
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:44:16Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UntagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tagKeys": [
      "purpose"
    ]
  },
  "responseElements": null,
  "requestID": "example7-6c1e-4f09-9e46-bb957example",
  "eventID": "example6-75ff-4c94-a1cd-4d5f5example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

ListTagsForResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
```

```
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:42:31Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListTagsForResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
  },
  "responseElements": null,
  "requestID": "example8-10c7-43d4-b147-3d9d9example",
  "eventID": "example2-24fc-4da7-a479-c9748example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

LockRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-25T00:45:19Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "LockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {
    "identifier": "jkrnexample",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    }
  },
  "responseElements": {
    "identifier": "jkrnexample",
    "description": "",
    "resourceType": "EBS_SNAPSHOT",
```

```
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "resourceTags": [],
    "status": "available",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    },
    "lockState": "locked"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

UnlockRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
```

```
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-25T00:46:17Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UnlockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": {
    "identifier": "jkrnexample",
    "description": "",
    "resourceType": "EC2_IMAGE",
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "resourceTags": [],
    "status": "available",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    },
    "lockState": "pending_unlock",
    "lockEndTime": "Nov 1, 2022, 12:46:17 AM"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
```

```
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

Posizioni delle risorse

Le risorse Amazon EC2 sono specifiche per la AWS regione o la zona di disponibilità in cui risiedono.

Risorsa	Tipo	Descrizione
Identificatori di risorse Amazon EC2	Pool di risorse	Ogni identificatore di risorsa, ad esempio un ID AMI, ID istanza, ID volume EBS o ID snapshot EBS, è associato alla relativa regione e può essere utilizzat o solo nella regione in cui hai creato la risorsa.
Nomi di risorsa forniti dall'utente	Pool di risorse	Ogni nome di risorsa, ad esempio un nome di gruppo di sicurezza o un nome di coppia di chiavi, è associato alla relativa regione e può essere utilizzat o solo nella regione in cui hai creato la risorsa. Anche se puoi creare risorse con lo stesso nome in più regioni, tali risorse non saranno correlate tra loro.
AMI	Pool di risorse	Un'AMI è associata alla regione in cui si trovano i relativi file all'interno di Amazon S3. Puoi copiare un'AMI da una regione all'altra. Per ulteriori informazioni, consultare Copiare un'AMI.
Snapshot EBS	Pool di risorse	Uno snapshot EBS è associato alla relativa regione e può essere utilizzato solo per creare volumi nella stessa regione. Puoi copiare uno snapshot da una regione all'altra.

Risorsa	Tipo	Descrizione
Volumi EBS	Zona di disponibilità	Un volume Amazon EBS è associato alla relativa zona di disponibilità e può essere collegato solo alle istanze nella stessa zona di disponibilità.
Indirizzi IP elastici	Pool di risorse	Un indirizzo IP elastico è associato a una regione e può essere collegato solo a un'istanza nella stessa regione.
Istanze	Zona di disponibilità	Un'istanza è associata alle zone di disponibilità in cui la hai avviata. Tuttavia, il relativo ID istanza è associato alla regione.
Key pairs (Coppie di chiavi)	Globale o regionale	Le coppie di chiavi create utilizzando Amazon EC2 sono associate alla regione in cui le hai create. Puoi creare una coppia di chiavi RSA specifica e caricarla nella regione in cui vuoi utilizzarla. Puoi impostare la coppia di chiavi in modo che sia disponibile a livello globale caricandola in ogni regione. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.
Gruppi di sicurezza	Pool di risorse	Un gruppo di sicurezza è associato a una regione e può essere collegato solo alle istanze nella stessa regione. Non puoi abilitare la comunicazione tra un'istanza e un'istanza esterna alla relativa regione utilizzando le regole del gruppo di sicurezza. Il traffico da un'istanza che si trova in un'altra regione viene considerato larghezza di banda WAN.

ID risorsa

Quando le risorse vengono create, assegniamo a ciascuna risorsa un ID univoco. Un ID risorsa ha il formato di un identificatore di risorsa (ad esempio `snap` per uno snapshot) seguito da un trattino e da una combinazione univoca di lettere e numeri.

Ogni identificatore di risorsa, ad esempio un ID AMI, ID istanza, ID volume EBS o ID snapshot EBS, è associato alla relativa regione e può essere utilizzato solo nella regione in cui hai creato la risorsa.

Puoi utilizzare gli ID risorsa per cercare le risorse nella console Amazon EC2. Se stai utilizzando uno strumento a riga di comando o l'API Amazon EC2 in combinazione con Amazon EC2, l'uso degli ID risorsa è obbligatorio per determinati comandi. Ad esempio, se utilizzi il AWS CLI comando stop-instances per arrestare un'istanza, devi specificare l'ID dell'istanza nel comando.

Lunghezza dell'ID risorsa

Prima di gennaio 2016, gli ID assegnati alle risorse appena create di alcuni tipi di risorse utilizzavano 8 caratteri dopo il trattino (ad esempio, i-1a2b3c4d). Da gennaio 2016 a giugno 2018, sono stati modificati gli ID di questi tipi di risorse per utilizzare 17 caratteri dopo il trattino (ad esempio, `i-1234567890abcdef0`). A seconda del momento in cui è stato creato l'account, potresti disporre di risorse esistenti con ID brevi, tuttavia, tutte le nuove risorse riceveranno ID più lunghi.

Elencare e filtrare le risorse

Puoi ottenere un elenco di alcuni tipi di risorse tramite la console Amazon EC2. Puoi ottenere un elenco di ciascun tipo di risorsa tramite il comando o l'operazione API corrispondente. Se disponi di molte risorse, puoi filtrare i risultati in modo da includere o escludere solo le risorse che corrispondono a determinati criteri.

Indice

Elencare e filtrare le risorse utilizzando la console

Indice

Elencare le risorse mediante la console

Puoi visualizzare i tipi di risorse Amazon EC2 più frequenti tramite la console. Per visualizzare risorse aggiuntive, utilizza l'interfaccia a riga di comando o le operazioni API.

Per elencare le risorse EC2 tramite la console

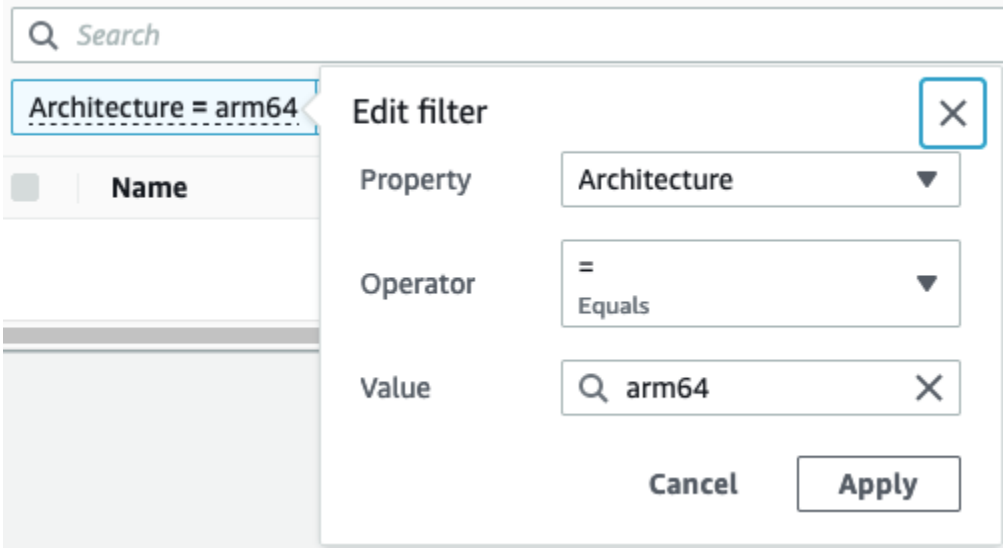
1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere l'opzione corrispondente al tipo di risorsa. Ad esempio, per elencare le istanze, scegliere Instances (Istanze).

   Nella pagina vengono visualizzate tutte le risorse del tipo di risorsa selezionato.

Filtrare le risorse mediante la console

Per filtrare un elenco di risorse

1. Nel riquadro di navigazione selezionare un tipo di risorsa, ad esempio Instances (Istanze).
2. Selezionare il campo di ricerca.
3. Selezionare il filtro dall'elenco.
4. Selezionare un operatore, ad esempio = (uguale a). Per alcuni attributi è possibile selezionare più operatori. Nota: non tutte le schermate supportano la selezione di un operatore.
5. Seleziona un valore di filtro.
6. Per modificare un filtro selezionato, scegli il token del filtro (casella blu), apporta le modifiche richieste e quindi scegli Apply (Applica). Nota: non tutte le schermate supportano la modifica del filtro selezionato.



7. Al termine, rimuovere il filtro.

Filtri supportati

La console Amazon EC2 supporta due tipi di filtraggio.

- Il filtro API viene applicato sul lato server. Il filtro viene applicato alla chiamata API e riduce il numero di risorse restituite dal server. Consente un filtraggio rapido tra grandi insiemi di risorse e può ridurre i tempi e i costi di trasferimento dei dati tra il server e il browser. Il filtro API supporta gli operatori = (uguale a) e : (contiene) e fa sempre distinzione tra maiuscole e minuscole.
- Il filtro client avviene sul lato client. Consente di filtrare i dati già disponibili nel browser (in altre parole, i dati che sono già stati restituiti dall'API). Il filtro client funziona bene in combinazione con un filtro API per filtrare set di dati più piccoli nel browser. Oltre agli operatori = (uguale a) e : (contiene), il filtro client può anche supportare gli operatori di intervallo, come >= (maggiore o uguale a) e gli operatori di negazione (inverso) come != (non è uguale).

La console Amazon EC2 supporta i seguenti tipi di ricerche:

Ricerca per parola chiave

La ricerca per parola chiave è una ricerca a testo libero che consente di cercare un valore in tutti gli attributi o i tag delle risorse, senza specificare una chiave di attributo o di tag da cercare.

> **Note**
>
> Tutte le ricerche per parole chiave utilizzano il filtro client.

Per eseguire la ricerca per parola chiave, digita o incolla quello che stai cercando nel campo di ricerca, quindi scegli Enter (Invia). Ad esempio, la ricerca `123` corrisponde a tutte le istanze che hanno 123 in uno qualsiasi dei relativi attributi, ad esempio un indirizzo IP, un ID istanza, un ID VPC o un ID AMI, o in uno qualsiasi dei relativi tag, come il Nome. Se la ricerca a testo libero restituisce corrispondenze impreviste, applica filtri aggiuntivi.

Ricerca per attributo

La ricerca per attributo consente di cercare un attributo specifico in tutte le risorse.

> **Note**
>
> Le ricerche degli attributi utilizzano filtri API o filtri client, a seconda dell'attributo selezionato. Quando si esegue una ricerca di attributi, gli attributi vengono raggruppati di conseguenza.

Ad esempio puoi cercare nell'attributo Instance state (Stato istanza) tutte le istanze in modo da restituire solo le istanze che si trovano nello stato `stopped`. Per farlo:

1. Nel campo di ricerca nella schermata Instances (Istanze), inizia a immettere `Instance state`. Quando si immettono i caratteri, vengono visualizzati i due tipi di filtri per Instance state (Stato istanza): API filters (Filtri API) e Client filters (Filtri client).
2. Per eseguire la ricerca sul lato server, scegli Instance state (Stato istanza) in API filters (Filtri API). Per eseguire la ricerca sul lato client, scegli Instance state (client) (Stato istanza) (client) in Client filters (Filtri client).

   Viene visualizzato un elenco di possibili operatori per l'attributo selezionato.
3. Scegli l'operatore = (uguale a).

   Viene visualizzato un elenco di possibili valori per l'attributo e l'operatore selezionati.
4. Seleziona Stopped (Interrotto) dall'elenco.

Ricerca per tag

La ricerca per tag consente di filtrare le risorse nella tabella attualmente visualizzata in base a una chiave di tag o un valore di tag.

Le ricerche per tag utilizzano il filtro API o il filtro client, a seconda delle impostazioni nella finestra Preferences (Preferenze).

Per utilizzare il filtro API per i tag

1. Apri la finestra Preferenze.
2. Deseleziona la casella di controllo Use regular expression matching (Usa corrispondenza espressioni regolari). Se questa casella di controllo è selezionata, viene applicato il filtro client.
3. Seleziona la casella di controllo Use case sensitive matching (Usa corrispondenza tra maiuscole e minuscole). Se questa casella di controllo è deselezionata, viene applicato il filtro client.
4. Scegli Conferma.

Quando si esegue una ricerca per tag, è possibile utilizzare i valori seguenti:

- (empty) (vuoto): trova tutte le risorse con la chiave di tag specificata, ma non deve essere presente alcun valore di tag.
- All values (Tutti i valori): trova tutte le risorse con la chiave di tag specificata e qualsiasi valore di tag.
- Senza tag: trova tutte le risorse che non hanno la chiave di tag specificata.
- Il valore visualizzato: trova tutte le risorse con la chiave di tag specificata e il valore di tag specificato.

È possibile utilizzare le seguenti tecniche per migliorare o perfezionare le ricerche:

Ricerca inversa

Le ricerche inverse consentono di cercare risorse che non corrispondono a un valore specificato. Nelle schermate Instances (Istanze) e AMI, le ricerche inverse vengono eseguite selezionando l'operatore != (non è uguale) o !: (non contiene) e successivamente selezionando un valore. In altre schermate, le ricerche inverse vengono eseguite aggiungendo un prefisso carattere punto esclamativo (!) alla parola chiave di ricerca.

> **Note**
>
> La ricerca inversa è supportata solo con le ricerche di parole chiave e attributi nei filtri client. Non è supportato con le ricerche di attributi nei filtri API.

Ad esempio puoi cercare nell'attributo Instance state (Stato istanza) tutte le istanze in modo da escludere le istanze che si trovano nello stato `terminated`. Per farlo:

1. Nel campo di ricerca nella schermata Instances (Istanze), inizia a immettere `Instance state`. Quando si immettono i caratteri, vengono visualizzati i due tipi di filtri per Instance state (Stato istanza): API filters (Filtri API) e Client filters (Filtri client).
2. In Client filters (Filtri client), scegli Instance state (client) (Stato istanza (client)). La ricerca inversa è supportata solo sui filtri client.

   Viene visualizzato un elenco di possibili operatori per l'attributo selezionato.
3. Scegli != (non è uguale), quindi scegli terminated (terminato).

Per filtrare le istanze in base a un attributo di stato dell'istanza, è inoltre possibile utilizzare le icone di ricerca
()
nella colonna Instance state (Stato istanza). L'icona di ricerca con un segno più (+) visualizza tutte le istanze corrispondenti a tale attributo. L'icona di ricerca con un segno meno (-) esclude tutte le istanze corrispondenti a tale attributo.

Ecco un altro esempio di utilizzo della ricerca inversa: per elencare tutte le istanze a cui non è assegnato il gruppo di sicurezza denominato `launch-wizard-1`, in Client filters, (Filtri client), esegui la ricerca in base all'attributo Security group name (Nome gruppo di sicurezza), scegli != e inserisci la parola chiave `launch-wizard-1` nella barra di ricerca.

Ricerca parziale

Con le ricerche parziali, è possibile cercare valori di stringa parziali. Per eseguire una ricerca parziale, immettere solo una parte della parola chiave da cercare. Nelle schermate Instances (Istanze) e AMI, le ricerche parziali possono essere eseguite solo con l'operatore : (contiene). In altre schermate, è possibile selezionare l'attributo del filtro client e inserire immediatamente solo una parte della parola chiave che si desidera cercare. Ad esempio, nella schermata Instance type (Tipo di istanza), per cercare tutte le istanze `t2.micro`, `t2.small` e `t2.medium` è possibile

eseguire la ricerca in base all'attributo Instance Type (Tipo di istanza) e inserire la parola chiave `t2`.

Ricerca di espressioni regolari

Per utilizzare le ricerche con espressioni regolari, è necessario selezionare la casella di controllo Use regular expression matching (Usa corrispondenza espressioni regolari) nella finestra Preferenze.

Le espressioni regolari sono utili quando devi far corrispondere i valori in un campo con un modello specifico. Ad esempio, per cercare un valore che inizia con `s`, cercare `^s`. Per cercare un valore che termina con `xyz`, cercare `xyz$`. Oppure per cercare un valore che inizia con un numero seguito da uno o più caratteri, cercare `[0-9]+.*`.

> **Note**
>
> La ricerca con espressioni regolari è supportata solo con ricerche per parole chiave e ricerche di attributi nei filtri client. Non è supportato con le ricerche di attributi nei filtri API.

Ricerca con distinzione tra maiuscole e minuscole

Per utilizzare le ricerche con distinzione tra maiuscole e minuscole, è necessario selezionare la casella di controllo Use case sensitive matching (Usa corrispondenza tra maiuscole e minuscole) nella finestra Preferences (Preferenze). Questa preferenza si applica solo ai filtri client e tag.

> **Note**
>
> I filtri API fanno sempre distinzione tra maiuscole e minuscole.

Ricerca con caratteri jolly

Utilizzare il carattere jolly `*` per abbinare zero o più caratteri. Utilizzare il carattere jolly `?` per corrispondere a zero o a un carattere. Ad esempio, se si dispone di un set di dati con i valori `prod`, `prods` e `production`, la ricerca di `prod*` corrisponde a tutti i valori, mentre `prod?` corrisponde solo a `prod` e `prods`. Per utilizzare i valori letterali, utilizzare il carattere escape barra rovesciata (\). Ad esempio, "`prod\*`" corrisponde a `prod*`.

> **Note**
>
> La ricerca con caratteri jolly è supportata solo con le ricerche di attributi e tag nei filtri API. Non è supportata con le ricerche per parole chiave e con le ricerche di attributi e tag nei filtri client.

Combinazione di ricerche

In generale, più filtri con lo stesso attributo vengono automaticamente uniti con `OR`. Ad esempio, la ricerca `Instance State : Running` e `Instance State : Stopped` restituisce tutte le istanze in esecuzione O arrestate. Per unire la ricerca con `AND`, cerca tra diversi attributi. Ad esempio, la ricerca `Instance State : Running` e `Instance Type : c4.large` restituisce solo le istanze di tipo `c4.large` E che si trovano in stato di esecuzione.

Elencare e filtrare tramite la CLI e l'API

Ogni tipo di risorsa ha un comando CLI o un'operazione API corrispondente per elencare le risorse di quel tipo. Gli elenchi di risorse risultanti possono essere lunghi, quindi può essere più veloce e più utile filtrare i risultati in modo da includere solo le risorse corrispondenti a criteri specifici.

Considerazioni sui filtri

- Puoi specificare fino a 50 filtri e fino a 200 valori per filtro in una singola richiesta.
- Le stringhe di filtro possono avere una lunghezza massima di 255 caratteri.
- Puoi anche utilizzare caratteri jolly con i valori di filtro. Un asterisco (*) corrisponde a 0 o più caratteri, mentre un punto interrogativo (?) corrisponde a 0 o un carattere.
- I valori di filtro fanno distinzione tra maiuscole e minuscole.
- La ricerca può includere i valori letterali dei caratteri jolly; basta inserirli come caratteri escape con una barra rovesciata prima del carattere. Ad esempio, un valore di `\*amazon\?\\` ricerca la stringa letterale `*amazon?\`.

Filtri supportati

Per visualizzare i filtri supportati per ogni risorsa Amazon EC2, vedere la seguente documentazione:

- AWS CLI: i comandi `describe` in Riferimento ai comandi AWS CLI -Amazon EC2.

- Strumenti per Windows PowerShell: `Get` i comandi del AWS Tools for PowerShell Cmdlet Reference-Amazon EC2.
- Query API: le operazioni API `Describe` in Riferimenti API Amazon EC2.

Example Esempio: specificare un singolo filtro

È possibile elencare le istanze Amazon EC2 utilizzando describe-instances. Senza filtri, la risposta contiene informazioni su tutte le tue risorse. È possibile utilizzare il comando seguente per includere solo le istanze in esecuzione nell'output.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running
```

Per elencare solo gli ID di istanza per le istanze in esecuzione, aggiungere il parametro `--query` come indicato di seguito.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running --query
 "Reservations[*].Instances[*].InstanceId" --output text
```

Di seguito è riportato un output di esempio.

```
i-0ef1f57f78d4775a4
i-0626d4edd54f1286d
i-04a636d18e83cfacb
```

Example Esempio: specificare più filtri o valori filtro

Se si specificano più filtri o più valori filtro, la risorsa deve corrispondere a tutti i filtri da includere nei risultati.

È possibile utilizzare il comando seguente per elencare tutte le istanze il cui tipo è `m5.large` o `m5d.large`.

```
aws ec2 describe-instances --filters Name=instance-type,Values=m5.large,m5d.large
```

È possibile utilizzare il comando seguente per elencare tutte le istanze interrotte il cui tipo è `t2.micro`.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=stopped
 Name=instance-type,Values=t2.micro
```

Example Esempio: utilizzare caratteri jolly in un valore di filtro

Se si specifica il `database` come valore del filtro per il filtro `description` quando si descrivono gli snapshot EBS utilizzando describe-snapshots, il comando restituisce solo gli snapshot la cui descrizione è "database".

```
aws ec2 describe-snapshots --filters Name=description,Values=database
```

Il carattere jolly * corrisponde a zero o più caratteri. Se si specifica `*database*` come valore del filtro, il comando restituisce solo snapshot la cui descrizione include la parola database.

```
aws ec2 describe-snapshots --filters Name=description,Values=*database*
```

Il carattere jolly ? corrisponde esattamente a 1 carattere. Se si specifica `database?` come valore del filtro, il comando restituisce solo snapshot la cui descrizione è "database" o "database" seguito da un carattere.

```
aws ec2 describe-snapshots --filters Name=description,Values=database?
```

Se si specifica `database????`, il comando restituisce solo snapshot la cui descrizione è "database" seguito da un massimo di quattro caratteri. Esclude le descrizioni con "database" seguite da cinque o più caratteri.

```
aws ec2 describe-snapshots --filters Name=description,Values=database????
```

Example Esempio: filtro in base alla data

Con AWS CLI, puoi utilizzare JMESPath per filtrare i risultati utilizzando le espressioni. *Ad esempio, il describe-snapshotscomando seguente visualizza gli ID di tutte le istantanee create dall'utente Account AWS (rappresentato da 123456789012) prima della data specificata (rappresentata dal 31/03/2020).* Se non si specifica il proprietario, i risultati includono tutti gli snapshot pubblici.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

Il comando seguente visualizza gli ID di tutti gli snapshot creati nell'intervallo di date specificato.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]" --
output text
```

Filtra in base ai tag

Per esempi su come filtrare un elenco di risorse in base ai relativi tag, consulta Utilizzo dei tag tramite la riga di comando.

Visualizzazione delle risorse in tutte le regioni utilizzando Amazon EC2 Global View

Amazon EC2 Global View consente di visualizzare e cercare risorse Amazon EC2 e Amazon VPC in AWS una singola regione o in più regioni contemporaneamente in un'unica console. Per ulteriori informazioni, consulta Amazon EC2 Global View.

Amazon EC2 Global View

Amazon EC2 Global View consente di visualizzare alcune delle risorse Amazon EC2 e Amazon VPC in un'unica Regione AWS o in più Regioni in un'unica console. Amazon EC2 Global View fornisce anche la funzionalità di ricerca globale che ti consente di cercare risorse specifiche o tipi di risorse specifici in più Regioni contemporaneamente.

Amazon EC2 Global View non ti consente di modificare le risorse in alcun modo.

Risorse supportate

Utilizzando Amazon EC2 Global View, puoi visualizzare un riepilogo globale delle seguenti risorse in tutte le regioni per le quali Account AWS è abilitato.

- Gruppi Auto Scaling
- Set opzioni DHCP
- Internet Gateway egress-only
- IP elastici
- Servizi endpoint
- Istanze
- Gateway Internet
- Elenchi di prefissi gestiti

- Gateway NAT
- Liste di controllo accessi (ACL) di rete
- Interfacce di rete
- Tabelle di instradamento
- Gruppi di sicurezza
- Sottoreti
- Volumi
- VPC
- Endpoint VPC
- Connessioni in peering di VPC

Autorizzazioni richieste

Per poter utilizzare Amazon EC2 Global View, un utente deve disporre delle autorizzazioni seguenti.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:DescribeRegions",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeAddresses",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribePrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
```

```
    "ec2:DescribeVpcPeeringConnections"
  ],
  "Resource": "*"
  }]
}
```

Per utilizzare Amazon EC2 Global View

Apri la console Amazon EC2 Global View all'indirizzo https://console.aws.amazon.com/ec2globalview/home.

> **Important**
>
> Non è possibile utilizzare una finestra privata in Firefox per accedere ad Amazon EC2 Global View.

La console include i seguenti elementi:

- Region explorer (Explorer Regione): questa scheda include le sezioni seguenti:
  - Riepilogo delle risorse: fornisce una panoramica di alto livello delle risorse in tutte le Regioni.

    Le regioni abilitate indicano il numero di regioni per le quali la tua Account AWS è abilitata. I campi rimanenti indicano il numero di risorse attualmente disponibili in tali Regioni. Scegli uno dei collegamenti per visualizzare le risorse di quel tipo in tutte le Regioni. Ad esempio, se il link sotto l'etichetta Instances (Istanze) è 29 in 10 Regioni, indica che attualmente hai 29 istanze in 10 Regioni. Scegliere il collegamento per visualizzare un elenco di tutte le 29 istanze.
  - Numero di risorse per Regione: elenca tutte le Regioni AWS (incluse quelle per le quali il tuo account non è abilitato) e fornisce i totali di ogni tipo di risorsa per ogni Regione.

    Scegliere il nome di una regione per visualizzare tutte le risorse di tutti i tipi per la regione specifica. Ad esempio, scegli Africa (Città del Capo) af-south-1 per visualizzare tutti i VPC, le sottoreti, le istanze, i gruppi di sicurezza, i volumi e i gruppi con scalabilità automatica di tale regione. In alternativa, selezionare una regione e scegliere View resources for selected Region (Visualizza le risorse per la regione selezionata).

    Scegliere il valore per un tipo di risorsa specifico in una regione specifica per visualizzare solo le risorse di quel tipo in quella regione. Ad esempio, scegliere il valore di Istanze per Africa (Città del Capo) af-south-1 per visualizzare solo le istanze in quella regione.

- Global search (Ricerca globale): questa scheda consente di cercare risorse specifiche o tipi di risorse specifici in una singola regione o in più regioni. Consente inoltre di visualizzare i dettagli per una risorsa specifica.

  Per cercare le risorse, immettere i criteri di ricerca nel campo che precede la griglia. La ricerca può essere eseguita in base alla Regione, al tipo di risorsa e ai tag assegnati alle risorse.

  Per visualizzare i dettagli di una risorsa specifica, selezionala nella griglia. È possibile inoltre scegliere l'ID risorsa di una risorsa per aprirla nella console corrispondente. Ad esempio, scegli un ID istanza per aprire l'istanza nella console Amazon EC2 oppure scegli un ID sottorete per aprire la sottorete nella console Amazon VPC.

> **Tip**
>
> Se utilizzi solo regioni o tipi di risorse specifici, puoi personalizzare Amazon EC2 Global View per visualizzare soltanto tali regioni e tipi di risorse. Per personalizzare le regioni e i tipi di risorse visualizzati, nel pannello di navigazione scegli Impostazioni, quindi nelle schede Risorse e Regioni seleziona le regioni e i tipi di risorse che desideri escludere dalla visualizzazione in Amazon EC2 Global View.

Tagging delle risorse Amazon EC2.

Per semplificare la gestione di istanze, immagini e altre risorse Amazon EC2 puoi decidere di assegnare metadati personalizzati a ogni risorsa sotto forma di tag. I tag consentono di classificare le AWS risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Questa caratteristicaè molto utile quando hai tante risorse dello stesso tipo in quanto puoi rapidamente individuare una risorsa specifica in base ai tag assegnati. Questo argomento descrive i tag e mostra come crearli.

> **Warning**
>
> Le chiavi di tag e i relativi valori vengono restituiti da numerose chiamate API diverse. Negando l'accesso a `DescribeTags` non viene automaticamente negato l'accesso ai tag restituiti da altre API. Come best practice, consigliamo di non includere dati sensibili nei tag.

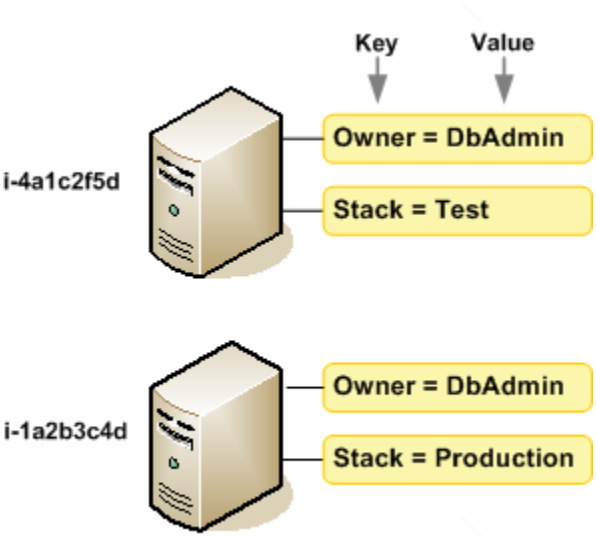
Indice

Nozioni di base sui tag

Un tag è un'etichetta che si assegna a una AWS risorsa. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

I tag consentono di classificare le AWS risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ad esempio, puoi definire un set di tag per le istanze Amazon EC2 del tuo account e monitorare così ogni proprietario dell'istanza e il livello dello stack.

Lo schema seguente illustra il funzionamento del tagging. In questo esempio hai assegnato due tag a ciascuna istanza, un tag con la chiave `Owner` e un altro tag con la chiave `Stack`. A ogni tag è inoltre associato un valore.



Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Con un set di chiavi di tag coerente, la gestione delle risorse risulta semplificata. Puoi cercare e filtrare le risorse in base ai tag aggiunti. Per ulteriori informazioni su come implementare una strategia efficace di etichettatura delle risorse, consulta il white paper sulle migliori pratiche di etichettatura. AWS

I tag non hanno alcun significato semantico per Amazon EC2 e vengono interpretati rigorosamente come una stringa di caratteri. Inoltre, i tag non vengono assegnati automaticamente alle risorse. Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

> **Note**
>
> Dopo aver eliminato una risorsa, i relativi tag potrebbero rimanere visibili nell'output della console, dell'API e della CLI per un breve periodo. Questi tag saranno gradualmente dissociati dalla risorsa e verranno eliminati definitivamente.

Assegnazione di tag alle risorse

Puoi assegnare tag alla maggior parte delle risorse Amazon EC2 già esistenti nel tuo account. Nella tabella seguente sono elencate le risorse che supportano il tagging.

Se utilizzi la console Amazon EC2, puoi applicare tag alle risorse utilizzando la scheda Tag nella schermata delle risorse pertinente oppure puoi utilizzare l'Editor dei tag nella AWS Resource Groups console. Alcune schermate relative alle risorse ti permettono di specificare i tag per una risorsa quando crei la risorsa, ad esempio un tag con la chiave `Name` e un valore specificato. Nella maggior parte dei casi, la console applica i tag subito dopo la creazione della risorsa, anziché durante il processo di creazione. La console può organizzare le risorse in base al relativo tag `Name` ma questo tag non ha un significato semantico per il servizio Amazon EC2.

Se utilizzi l'API Amazon EC2, o un AWS SDK AWS CLI, puoi utilizzare l'azione API `CreateTags` EC2 per applicare tag alle risorse esistenti. Inoltre, alcune operazioni per la creazione di risorse ti consentono di specificare tag per una risorsa durante la sua creazione. Se i tag non possono essere applicati durante la creazione della risorsa, eseguiamo il rollback del processo di creazione della risorsa. Ciò fa sì che le risorse vengano create con i tag oppure che non vengano create affatto, nonché che nessuna risorsa sia mai sprovvista di tag. Il tagging delle risorse in fase di creazione ti

permette di evitare di eseguire script di tagging personalizzati dopo la creazione delle risorse. Per ulteriori informazioni sull'abilitazione agli utenti affinché possano aggiungere tag alle risorse durante la creazione, vedere Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

La tabella seguente descrive le risorse Amazon EC2 che possono essere etichettate e le risorse che possono essere taggate al momento della creazione utilizzando l'API Amazon EC2, o un AWS CLI SDK. AWS

Supporto del tagging per le risorse Amazon EC2

Risorsa	support dei tag	Supporta l'applicazione di tag in fase di creazione
AFI	Sì	Sì
AMI	Sì	Sì
Attività bundle	No	No
Capacity Reservation	Sì	Sì
Gateway carrier	Sì	Sì
Endpoint Client VPN	Sì	Sì
Route Client VPN	No	No
Gateway del cliente	Sì	Sì
Dedicated Host	Sì	Sì
Prenotazione Host dedicato	Sì	Sì
Opzioni DHCP	Sì	Sì
Snapshot EBS	Sì	Sì
Volume EBS	Sì	Sì
EC2 Fleet	Sì	Sì

Risorsa	support dei tag	Supporta l'applicazione di tag in fase di creazione
Gateway Internet Egress-only	Sì	Sì
Indirizzo IP elastico	Sì	Sì
Acceleratore Grafica elastica	Sì	No
Istanza	Sì	Sì
Finestra di eventi istanza	Sì	Sì
Volume di instance store	N/A	N/A
Internet Gateway	Sì	Sì
Pool di indirizzi IP (BYOIP)	Sì	Sì
Coppia di chiavi	Sì	Sì
Modello di lancio	Sì	Sì
Versione del modello di lancio	No	No
Gateway locale	Sì	No
Tabella di routing del gateway locale	Sì	No
Interfaccia virtuale del gateway locale	Sì	No
Gruppo di interfacce virtuali del gateway locale	Sì	No
Associazione VPC della tabella di routing del gateway locale	Sì	Sì

Risorsa	support dei tag	Supporta l'applicazione di tag in fase di creazione
Associazione gruppo di interfacce virtuali della tabella di routing del gateway locale	Sì	No
Gateway NAT	Sì	Sì
Lista di controllo degli accessi di rete	Sì	Sì
Interfaccia di rete	Sì	Sì
Gruppo di collocamento	Sì	Sì
Elenco di prefissi	Sì	Sì
Reserved Instance	Sì	No
Elenco di Istanza riservata	No	No
Tabella di routing	Sì	Sì
Richieste di parchi istanze Spot	Sì	Sì
Richiesta di istanza Spot	Sì	Sì
Gruppo di sicurezza	Sì	Sì
Regola del gruppo di sicurezza	Sì	No
Sottorete	Sì	Sì
Filtro di mirroring del traffico	Sì	Sì
Sessione di mirroring del traffico	Sì	Sì

Risorsa	support dei tag	Supporta l'applicazione di tag in fase di creazione
Destinazione di mirroring del traffico	Sì	Sì
Transit Gateway	Sì	Sì
ID del dominio multicast del Transit Gateway	Sì	Sì
Tabella di routing del Transit Gateway	Sì	Sì
Allegato VPC del Transit Gateway	Sì	Sì
Gateway privato virtuale	Sì	Sì
VPC	Sì	Sì
Endpoint VPC	Sì	Sì
Servizio endpoint VPC	Sì	Sì
Configurazione del servizio endpoint VPC	Sì	Sì
Log di flusso VPC	Sì	Sì
Connessione di peering di VPC	Sì	Sì
Connessione VPN	Sì	Sì

Puoi creare tag per istanze, volumi, grafica elastica, interfacce di rete e richieste di istanze spot in fase di creazione utilizzando la procedura guidata di avvio istanza di Amazon EC2 nella console Amazon EC2. Puoi associare tag a volumi EBS in fase di creazione utilizzando la schermata Volumi o

a snapshot EBS tramite la schermata Snapshots. In alternativa, usa le API Amazon EC2 che creano risorse (ad esempio RunInstances) per applicare i tag durante la creazione della risorsa.

Puoi applicare autorizzazioni basate su tag a livello di risorsa nelle policy IAM alle operazioni dell'API Amazon EC2 che supportano il tagging in fase di creazione per implementare un controllo granulare sugli utenti e sui gruppi che associano tag alle risorse in fase di creazione. Le risorse vengono adeguatamente protette a partire dal momento della creazione, ovvero i tag vengono applicati subito alle risorse. Pertanto qualsiasi autorizzazione basata su tag a livello di risorsa che controlla l'uso delle risorse risulta immediatamente valida. Le risorse possono essere monitorate e segnalate con maggiore precisione. Puoi applicare l'uso del tagging alle nuove risorse e controllare quali chiavi e valori di tag sono impostati per le risorse.

Puoi inoltre applicare autorizzazioni a livello di risorsa alle operazioni `CreateTags` e `DeleteTags` dell'API Amazon EC2 nelle policy IAM per controllare quali chiavi e valori di tag sono impostati sulle risorse esistenti. Per ulteriori informazioni, consulta Esempio: aggiunta di tag alle risorse.

Per ulteriori informazioni sul tagging delle risorse per la fatturazione, consulta Utilizzo di tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per risorsa: 50
- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- Lunghezza massima della chiave: 128 caratteri Unicode in formato UTF-8
- Lunghezza massima del valore: 256 caratteri Unicode in formato UTF-8
- Caratteri consentiti
  - Sebbene EC2 consenta l'uso di qualsiasi carattere nei tag, altri servizi sono più restrittivi. AWS I caratteri consentiti in tutti i AWS servizi sono: lettere (`a-z`,`A-Z`), numeri (`0-9`) e spazi rappresentabili in UTF-8 e i seguenti caratteri:. `+ - = . _ : / @`
  - Se abiliti i tag delle istanze nei metadati delle istanze, per il tag dell'istanza keys puoi usare solo lettere (`a-z`, `A-Z`), numeri (`0-9`) e i seguenti caratteri: `+ - = . , _ : @`. Il tag dell'istanza keys non può contenere spazi o `/` e non può contenere solo `.` (un punto), `..` (due punti) o `_index`. Per ulteriori informazioni, consulta Utilizzo dei tag dell'istanza nei metadati dell'istanza.
- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole.

- Il `aws:` prefisso è riservato all'uso. AWS Se il tag ha una chiave di tag con questo prefisso, non puoi modificare o eliminare la chiave o il valore de tag. I tag con il prefisso `aws:` non vengono conteggiati per il limite del numero di tag per risorsa.

Non puoi interrompere, arrestare o eliminare una risorsa solo sulla base dei relativi tag. Devi specificare il relativo identificatore. Ad esempio, per eliminare gli snapshot associato a una chiave di tag denominata `DeleteMe`, devi utilizzare l'operazione `DeleteSnapshots` con gli identificatori di risorsa degli snapshot, ad esempio `snap-1234567890abcdef0`.

Quando tagghi risorse pubbliche o condivise, i tag che assegni sono disponibili solo per il tuo AWS account; nessun altro AWS account avrà accesso a quei tag. Per il controllo dell'accesso alle risorse condivise basato su tag, ogni AWS account deve assegnare il proprio set di tag per controllare l'accesso alla risorsa.

Non puoi associare tag a tutte le risorse. Per ulteriori informazioni, consulta Supporto del tagging per le risorse Amazon EC2.

Tag e gestione degli accessi

Se utilizzi AWS Identity and Access Management (IAM), puoi controllare quali utenti del tuo AWS account sono autorizzati a creare, modificare o eliminare i tag. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

Puoi inoltre utilizzare i tag delle risorse per implementare il controllo basato sugli attributi (ABAC). Puoi creare le policy IAM che consentono operazioni basate sui tag per la risorsa. Per ulteriori informazioni, consulta Controllo dell'accesso alle risorse EC2 mediante i tag delle risorse.

Tagging delle risorse per la fatturazione

Puoi utilizzare i tag per organizzare la AWS fattura in modo che rifletta la tua struttura dei costi. A tale scopo, registrati per ricevere una fattura sul tuo AWS account con i valori chiave dell'etichetta inclusi. Per ulteriori informazioni sulla configurazione di un report di allocazione dei costi mediante i tag, consulta Report di allocazione dei costi mensili nella Guida per l'utente di AWS Billing . Per visualizzare il costo delle risorse combinate, puoi organizzare le informazioni di fatturazione in base alle risorse con gli stessi valori di chiave di tag. Puoi ad esempio applicare tag a numerose risorse con un nome di applicazione specifico, quindi organizzare le informazioni di fatturazione per visualizzare il costo totale dell'applicazione in più servizi. Per ulteriori informazioni, consulta Utilizzo dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

> **Note**
>
> Se hai appena abilitato la reportistica, i dati relativi al mese corrente saranno disponibili per la visualizzazione dopo 24 ore.

I tag di allocazione dei costi possono indicare quali risorse contribuiscono ai costi, ma eliminare o disattivare le risorse non sempre riduce i costi. Ad esempio, i dati di snapshot a cui fa riferimento un altro snapshot vengono conservati anche se viene eliminato lo snapshot contenente i dati originali. Per ulteriori informazioni, consulta Volumi e snapshot di Amazon Elastic Block Store nella Guida per l'utente di AWS Billing .

> **Note**
>
> Gli indirizzi IP elastici con tag non appaiono nel report di allocazione dei costi.

Utilizzo di tag tramite la console

Puoi utilizzare la console di Amazon EC2 per visualizzare i tag di una singola risorsa e per applicare o rimuovere i tag da una risorsa alla volta.

Puoi utilizzare il Tag Editor nella AWS Resource Groups console per visualizzare i tag di tutte le tue risorse Amazon EC2 in tutte le regioni. Puoi visualizzare i tag per risorsa e per tipo di risorsa e vedere quali tipi di risorsa sono associati a un tag specifico. Puoi applicare o rimuovere i tag da più risorse e più tipi contemporaneamente. Il Tag Editor offre un sistema centrale e unificato per creare e gestire i tuoi tag. Per ulteriori informazioni, consulta la Tagging AWS Resources User Guide.

Attività

- Visualizzazione dei tag
- Aggiunta ed eliminazione di tag in una singola risorsa
- Aggiunta ed eliminazione di tag per più risorse
- Aggiunta di un tag all'avvio di un'istanza
- Filtrare un elenco di risorse per tag

Visualizzazione dei tag

Nella console Amazon EC2 puoi visualizzare i tag di una singola risorsa. Per visualizzare i tag di tutte le tue risorse, usa il Tag Editor nella console AWS Resource Groups .

Visualizza i tag di una singola risorsa

Quando selezioni una pagina relativa alle risorse nella console Amazon EC2, viene visualizzato l'elenco delle risorse corrispondenti. Ad esempio, se nel riquadro di navigazione selezioni Instances (Istanze), nella console vengono visualizzate le istanze Amazon EC2. Quando selezioni una risorsa in uno di questi elenchi, ad esempio un'istanza, se la risorsa supporta i tag, potrai visualizzare e gestire i relativi tag. Nella maggior parte delle pagine delle risorse, è possibile visualizzare i tag scegliendo la scheda Tags (Tag).

All'elenco di risorse puoi aggiungere una colonna in cui visualizzare tutti i valori dei tag con la stessa chiave. Questa colonna ti permette di ordinare e filtrare l'elenco delle risorse in base al tag.

New console

Per aggiungere una nuova colonna all'elenco di risorse per visualizzare i tag

1. Nella console EC2, scegli l'icona Preferenze a forma di ingranaggio nell'angolo in alto a destra della schermata.
2. Nella finestra di dialogo Preferenze, in Tagga colonne (in basso a sinistra) seleziona almeno una delle chiavi di tag, quindi scegli Conferma.

Old console

Esistono due modi per aggiungere una nuova colonna all'elenco di risorse per visualizzare i tag.

- Nella scheda Tags (Tag) selezionare Show Column (Mostra colonna). Alla console viene aggiunta una nuova colonna.
- Scegliere l'icona a forma di ingranaggio Show/Hide Columns (Mostra/nascondi colonne) e nella finestra di dialogo Show/Hide Columns (Mostra/nascondi colonne) selezionare la chiave di tag in Your Tag Keys (Le tue chiavi dei tag).

Visualizzazione dei tag per più risorse

Puoi visualizzare i tag su più risorse utilizzando il Tag Editor nella console AWS Resource Groups. Per ulteriori informazioni, consulta la Tagging AWS Resources User Guide.

Aggiunta ed eliminazione di tag in una singola risorsa

Puoi gestire i tag per una singola risorsa direttamente dalla pagina della risorsa interessata.

Per aggiungere un tag a una singola risorsa

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, seleziona la Regione in cui si trova la risorsa alla quale applicare il tag. Per ulteriori informazioni, consulta Posizioni delle risorse.
3. Nel riquadro di navigazione selezionare un tipo di risorsa, ad esempio Instances (Istanze).
4. Selezionare la risorsa nell'elenco di risorse e scegliere la scheda Tags (Tag).
5. Scegli Gestisci i tag e poi sceglie Aggiungi un nuovo tag. Immettere una chiave e un valore per il tag. Scegli Aggiungi tag per ogni tag aggiuntivo. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

Per eliminare un tag da una singola risorsa

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, seleziona la Regione in cui si trova la risorsa dalla quale rimuovere il tag. Per ulteriori informazioni, consulta Posizioni delle risorse.
3. Nel riquadro di navigazione scegliere un tipo di istanza, ad esempio Instances (Istanze).
4. Selezionare la risorsa nell'elenco di risorse e scegliere la scheda Tags (Tag).
5. Scegliere Manage tags (Gestisci tag). Per rimuovere un tag, scegli Rimuovi. Al termine della rimozione dei tag, scegliere Save (Salva).

Aggiunta ed eliminazione di tag per più risorse

Per aggiungere un tag a più risorse

1. Apri il Tag Editor nella console AWS Resource Groups all'indirizzo https://console.aws.amazon.com/resource-groups/tag-editor.
2. Per le Regioni, seleziona una o più regioni in cui si trovano le risorse alle quali applicare i tag.
3. Per i tipi di risorse, seleziona il tipo di risorse da etichettare (ad esempio, AWS::EC2::Instance).

4. Scegli Cerca risorse.
5. In Risultati della ricerca delle risorse selezionare la casella di controllo accanto a ogni risorsa alla quale applicare i tag.
6. Scegli Gestisci i tag delle risorse selezionate.
7. In Modifica i tag di tutte le risorse selezionate, scegli Aggiungi tag, quindi inserisci la nuova chiave e il nuovo valore del tag. Scegliere Add tag (Aggiungi tag) per ogni tag aggiuntivo.

   > **Note**
   >
   > Se si aggiunge un tag la cui chiave è la stessa di un tag esistente, il nuovo tag sovrascrive il tag esistente.

8. Scegli Rivedi e applica modifiche.
9. Scegliere Apply changes to all selected (Applica le modifiche a tutte le risorse selezionate).

Per rimuovere un tag da più risorse

1. Apri il Tag Editor nella console AWS Resource Groups all'indirizzo https://console.aws.amazon.com/resource-groups/tag-editor.
2. Per le Regioni, seleziona le regioni in cui si trovano le risorse alle quali rimuovere i tag.
3. Per i tipi di risorse, seleziona il tipo di risorse da rimuovere dai tag (ad esempio, AWS::EC2::Instance).
4. Scegli Cerca risorse.
5. In Risultati della ricerca delle risorse seleziona la casella di controllo accanto a ogni risorsa da cui rimuovere i tag.
6. Scegli Gestisci i tag delle risorse selezionate.
7. In Modifica i tag di tutte le risorse selezionate, accanto al tag da rimuovere, scegli Rimuovi tag.
8. Scegli Rivedi e applica modifiche.
9. Scegliere Apply changes to all selected (Applica le modifiche a tutte le risorse selezionate).

Aggiunta di un tag all'avvio di un'istanza

New console

Aggiunta di un tag tramite la procedura guidata di avvio dell'istanza

1. Nella barra di navigazione selezionare la regione dell'istanza. Questa scelta è importante perché, a differenza di altre, alcune risorse Amazon EC2 possono essere condivise tra più regioni. Selezionare la regione che soddisfa le proprie esigenze. Per ulteriori informazioni, consulta Posizioni delle risorse.
2. Scegliere Launch Instance (Avvia istanza).
3. In Name and tags (Nome e tag), è possibile inserire un nome descrittivo per l'istanza e specificare i tag.

   Il nome dell'istanza è un tag, dove la chiave è Name (Nome) e il valore è il nome specificato. Puoi tag all'istanza, ai volumi, alla grafica elastica e alle interfacce di rete. Per le istanze spot, è possibile aggiungere un tag solo alla richiesta di istanza spot.

   La specifica di un nome di istanza e dei tag aggiuntivi è facoltativa.

   - Per Name (Nome), inserire un nome descrittivo per l'istanza. Se non si specifica un nome, l'istanza può essere identificata dal relativo ID, che viene generato automaticamente all'avvio dell'istanza.
   - Per aggiungere altri tag, scegliere Add additional tags (Aggiungi altri tag). Scegliere Add tag (Aggiungi tag), quindi immettere una chiave e un valore e selezionare il tipo di risorsa da taggare. Scegliere Add tag (Aggiungi tag) per ogni tag aggiuntivo.
4. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), scegli il sistema operativo (SO) per l'istanza e un'AMI. Per ulteriori informazioni, consulta Immagini di applicazioni e sistema operativo (Amazon Machine Image).
5. In Key pair (login) (Coppia di chiavi (login), per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o creane una nuova.
6. Mantieni tutti gli altri campi sui valori predefiniti o scegli valori specifici per la configurazione dell'istanza desiderata. Per informazioni sui campi, consulta Avvio di un'istanza utilizzando parametri definiti.
7. Nel pannello Summary (Riepilogo), verifica le impostazioni, quindi scegli Launch instance (Avvia istanza).

Old console

Aggiunta di un tag tramite la procedura guidata di avvio dell'istanza

1. Nella barra di navigazione selezionare la regione dell'istanza. Questa scelta è importante perché, a differenza di altre, alcune risorse Amazon EC2 possono essere condivise tra più regioni. Selezionare la regione che soddisfa le proprie esigenze. Per ulteriori informazioni, consulta Posizioni delle risorse.
2. Scegliere Launch Instance (Avvia istanza).
3. Nella pagina Choose an Amazon Machine Image (AMI) (Scegli Amazon Machine Image (AMI)) è visualizzato un elenco delle configurazioni di base denominato Amazon Machine Images (AMIs) (Amazon Machine Image (AMI)). Selezionare l'AMI da utilizzare e scegliere Select (Seleziona). Per ulteriori informazioni, consulta Trovare una AMI.
4. Nella pagina Configure Instance Details (Configura dettagli istanza) configurare le impostazioni dell'istanza in base alle specifiche esigenze, quindi scegliere Next: Add archiviazione (Successivo: Aggiungi archiviazione).
5. Nella pagina Add archiviazione (Aggiungi archiviazione) è possibile specificare i volumi di archiviazione aggiuntivi per l'istanza. Al termine, scegliere Next: Add Tags (Successivo: Aggiungi tag).
6. Nella pagina Add Tags (Aggiungi tag) specificare i tag per l'istanza, per i volumi o per entrambi. Scegliere Add another tag (Aggiungi un altro tag) per aggiungere più di un tag all'istanza. Scegliere Next: Configure Security Group (Successivo: Configura il gruppo di sicurezza).
7. Nella pagina Configure Security Group (Configurare gruppo di sicurezza) è possibile scegliere un gruppo di sicurezza esistente di cui l'utente è proprietario oppure consentire alla procedura guidata di creare automaticamente un nuovo gruppo di sicurezza. Al termine, scegliere Review and Launch (Analizza e avvia).
8. Verificare le impostazioni. Dopo aver verificato le selezioni, scegliere Launch (Avvia). Seleziona una coppia di chiavi esistente o creare una nuova, seleziona la casella di controllo per la conferma, quindi scegli Launch Instances (Avvia istanze).

Filtrare un elenco di risorse per tag

Puoi filtrare l'elenco di risorse in base a uno o più chiavi e valori di tag.

Per filtrare un elenco di risorse per tag nella console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare un tipo di risorsa, ad esempio Instances (Istanze).
3. Selezionare il campo di ricerca.
4. Nell'elenco, in Tag, scegli la chiave del tag.
5. Scegliere il valore del tag corrispondente dall'elenco.
6. Al termine, rimuovere il filtro.

Per ulteriori informazioni sull'uso dei filtri nella console di Amazon EC2, consulta Elencare e filtrare le risorse.

Per filtrare più risorse in più regioni per tag utilizzando il Tag Editor.

Puoi utilizzare l'editor di tag nella console AWS Resource Groups per filtrare più risorse in più regioni per tag. Per ulteriori informazioni, consulta Trovare risorse cui applicare un tag nella Guida all'uso delle risorse AWS dei Tag.

Utilizzo dei tag tramite la riga di comando

È possibile aggiungere tag a molte risorse EC2 al momento della creazione, utilizzando il parametro specifiche tag per il comando create. È possibile visualizzare i tag di una risorsa utilizzando il comando describe per la risorsa. È inoltre possibile aggiungere, aggiornare o eliminare tag per le risorse esistenti utilizzando i comandi seguenti.

Attività	AWS CLI	AWS Tools for Windows PowerShell
Aggiungere o sovrascrivere uno o più tag	create-tags	New-EC2Tag
Eliminare uno o più tag.	delete-tags	Remove-EC2Tag
Descrivere uno o più tag.	describe-tags	Get-EC2Tag

Attività

- Aggiunta di tag alla creazione di risorse

- Aggiunta di tag a una risorsa esistente
- Descrizione delle risorse con tag

Aggiunta di tag alla creazione di risorse

I seguenti esempi mostrano come applicare i tag quando crei le risorse.

> **Note**
>
> Il modo in cui si immettono parametri in formato JSON alla riga di comando varia a seconda del sistema operativo.
>
> - Linux, macOS o Unix e Windows PowerShell : usa le virgolette singole (') per racchiudere la struttura dei dati JSON.
> - Windows: ometti le virgolette singole quando usi i comandi con la riga di comando di Windows.
>
> Per ulteriori informazioni, vedere Specificare i valori dei parametri per AWS CLI.

Example Esempio: Avvio di un'istanza e applicazione di tag all'istanza e al volume

Il comando run-instances seguente avvia un'istanza e applica un tag con la chiave **`webserver`** e il valore **`production`** all'istanza. Il comando applica inoltre un tag con una chiave **`cost-center`** e un valore **`cc123`** a qualsiasi volume EBS creato, in questo caso il volume root.

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications
 'ResourceType=instance,Tags=[{Key=webserver,Value=production}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Puoi applicare le stesse chiavi di tag e gli stessi valori di tag sia alle istanze che ai volumi durante l'avvio. Il comando seguente avvia un'istanza e applica un tag con una chiave **`cost-center`** e un valore **`cc123`** sia all'istanza che a qualsiasi volume EBS creato.

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=cost-center,Value=cc123}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Example Esempio: Creazione di un volume e applicazione di un tag

Il comando seguente create-volume crea un volume e applica due tag: **`purpose=production`** e **`cost-center=cc123`**.

```
aws ec2 create-volume \
    --availability-zone us-east-1a \
    --volume-type gp2 \
    --size 80 \
    --tag-specifications 'ResourceType=volume,Tags=[{Key=purpose,Value=production},
{Key=cost-center,Value=cc123}]'
```

Aggiunta di tag a una risorsa esistente

Negli esempi seguenti viene illustrato come aggiungere tag a una risorsa esistente utilizzando il comando create-tags.

Example Esempio: aggiunta di un tag a una risorsa

Questo esempio aggiunge il tag **`Stack=production`** all'immagine specificata o sovrascrive un tag esistente per l'AMI in cui la chiave tag è **`Stack`**. Se il comando va a buon fine, non viene restituito alcun output.

```
aws ec2 create-tags \
    --resources ami-78a54011 \
    --tags Key=Stack,Value=production
```

Example Esempio: aggiunta di tag a più risorse.

Questo esempio aggiunge (o sovrascrive) due tag per un'AMI e un'istanza. Uno dei tag contiene solo una chiave (**`webserver`**), senza alcun valore (il valore viene impostato su una stringa vuota). L'altro

tag comprende una chiave (**stack**) e un valore (**Production**). Se il comando va a buon fine, non viene restituito alcun output.

```
aws ec2 create-tags \
    --resources ami-1a2b3c4d i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example Esempio: aggiunta di tag con caratteri speciali

Questo esempio aggiunge il tag **[Group]=test** a un'istanza. Le parentesi quadre (**[** e **]**) sono caratteri speciali, per i quali occorre eseguire l'escape.

Se si utilizza Linux o OS X, per eseguire l'escape dei caratteri speciali, racchiudere l'elemento con il carattere speciale tra virgolette doppie (**"**), quindi racchiudere l'intera struttura chiave e valore tra virgolette singole (**'**).

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Se si utilizza Windows, per eseguire l'escape dei caratteri speciali, racchiudere l'elemento con caratteri speciali tra virgolette doppie ("), quindi anteporre ad ogni carattere virgolette doppie una barra rovesciata (****) come segue:

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
    --tags Key=\"[Group]\",Value=test
```

Se utilizzate Windows PowerShell, per evitare i caratteri speciali, racchiudete il valore contenente caratteri speciali tra virgolette doppie (**"**), fate precedere ogni virgoletta doppia da una barra rovesciata (****), quindi racchiudete l'intera struttura di chiavi e valori tra virgolette singole () come segue: **'**

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Descrizione delle risorse con tag

Negli esempi seguenti viene illustrato come usare i filtri con describe-instances per visualizzare le istanze con tag specifici. Tutti i comandi EC2 describe utilizzano questa sintassi per filtrare per tag in un singolo tipo di risorsa. In alternativa, è possibile utilizzare il comando describe-tags per filtrare per tag tra i tipi di risorse EC2.

Example Esempio: descrizione delle istanze con la chiave di tag specificata

Il comando seguente descrive le istanze con un tag **`Stack`**, indipendentemente dal valore del tag stesso.

```
aws ec2 describe-instances \
    --filters Name=tag-key,Values=Stack
```

Example Esempio: descrizione delle istanze con il tag specificato

Il comando seguente descrive le istanze con il tag **`Stack=production`**.

```
aws ec2 describe-instances \
    --filters Name=tag:Stack,Values=production
```

Example Esempio: descrizione delle istanze con il valore di tag specificato

Il comando seguente descrive le istanze con un tag con il valore **`production`**, indipendentemente dalla chiave di tag.

```
aws ec2 describe-instances \
    --filters Name=tag-value,Values=production
```

Example Esempio: descrivere tutte le risorse EC2 con il tag specificato

Il comando seguente descrive tutte le risorse EC2 con il tag **`Stack=Test`**.

```
aws ec2 describe-tags \
    --filters Name=key,Values=Stack Name=value,Values=Test
```

Utilizzo dei tag dell'istanza nei metadati dell'istanza

È possibile accedere ai tag di un'istanza dai metadati dell'istanza. Accedendo ai tag dai metadati dell'istanza non è più necessario utilizzare Chiamate API `DescribeInstances` o `DescribeTags`

per recuperare le informazioni sui tag, ciò riduce le transazioni API al secondo e consente al recupero dei tag di scalare il numero di istanze che si controllano. Inoltre, i processi locali in esecuzione su un'istanza possono visualizzare le informazioni sui tag dell'istanza direttamente dai metadati dell'istanza.

Per impostazione predefinita, i tag non sono disponibili dai metadati dell'istanza; è necessario consentire esplicitamente l'accesso. È possibile consentire l'accesso all'avvio dell'istanza o dopo l'avvio su un'istanza in esecuzione o interrotta. È inoltre possibile consentire l'accesso ai tag specificandolo in un modello di avvio. Le istanze avviate utilizzando il modello consentono l'accesso ai tag nei metadati dell'istanza.

Se aggiungi o rimuovi un tag di istanza, i metadati dell'istanza vengono aggiornati mentre l'istanza è in esecuzione, senza doverla arrestare e poi avviare.

Argomenti

Per consentire l'accesso ai tag nei metadati delle istanze

Per impostazione predefinita, non è possibile accedere ai tag dell'istanza nei metadati dell'istanza. Per ogni istanza, è necessario consentire l'accesso esplicitamente utilizzando uno dei metodi descritti di seguito.

Per consentire l'accesso ai tag nei metadati dell'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare un'istanza e scegliere Actions (Operazioni),Instance settings (Impostazioni istanza),Allow tags in instance metadata (Consenti tag nei metadati dell'istanza).
4. Per consentire l'accesso ai tag nei metadati dell'istanza, selezionare la casella di controlloAllow (Abilita).
5. Selezionare Salva.

Per consentire l'accesso ai tag nei metadati dell'istanza all'avvio utilizzando AWS CLI

Utilizzare il comando run-instances e impostare `InstanceMetadataTags` a `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c3.large \
    ...
    --metadata-options "InstanceMetadataTags=enabled"
```

Per consentire l'accesso ai tag nei metadati dell'istanza su un'istanza in esecuzione o interrotta utilizzando AWS CLI

Utilizzate il comando e impostate modify-instance-metadata-optionssu. `--instance-metadata-tags enabled`

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags enabled
```

Disattivazione dell'accesso ai metadati dell'istanza

Per disattivare l'accesso ai tag dell'istanza nei metadati dell'istanza, utilizzare uno dei metodi descritti di seguito. Non è necessario disattivare l'accesso ai tag di istanza sui metadati delle istanze all'avvio perché è disattivato per impostazione predefinita.

Per disattivare l'accesso ai tag nei metadati dell'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare un'istanza e scegliere Actions (Operazioni),Instance settings (Impostazioni istanza),Allow tags in instance metadata (Consenti tag nei metadati dell'istanza).
4. Per disattivare l'accesso ai tag nei metadati dell'istanza, deselezionare la casella di controlloAllow (Abilita).
5. Selezionare Salva.

Per disattivare l'accesso ai tag nei metadati dell'istanza utilizzando il AWS CLI

Usa il modify-instance-metadata-optionscomando e imposta su`--instance-metadata-tags`. `disabled`

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags disabled
```

Verifica del consenso dell'accesso ai tag nei metadati dell'istanza

Per ogni istanza, puoi utilizzare la console Amazon EC2 o AWS CLI verificare se è consentito l'accesso ai tag dell'istanza dai metadati dell'istanza.

Verifica del consenso dell'accesso ai tag nei metadati dell'istanza tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione scegli Instances (Istanze) e quindi selezionarne una.
3. Nella scheda Details (Dettagli), seleziona il campo Allow tags in instance metadata (Consenti i tag nei metadati dell'istanza). Se il valore è Enabled (Abilitato), i tag nei metadati dell'istanza sono consentiti. Se il valore è Disabled (Disabilitato), i tag nei metadati dell'istanza non sono consentiti.

Per verificare se l'accesso ai tag nei metadati dell'istanza è consentito, utilizza il AWS CLI

Utilizza il comando describe-instances e specifica l'ID istanza.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0
```

L'output di esempio seguente è stato troncato per motivi di spazio. Il parametro `"InstanceMetadataTags"` indica se i tag nei metadati delle istanze sono consentiti. Se il valore è `enabled`, i tag nei metadati dell'istanza sono consentiti. Se il valore è `disabled`, i tag nei metadati dell'istanza non sono consentiti.

```
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
```

```
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0abcdef1234567890",
                    "InstanceId": "i-1234567890abcdef0",
    ...

    "MetadataOptions": {
    "State": "applied",
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "disabled",
    "InstanceMetadataTags": "enabled"
    },
    ...
```

Recupero dei tag dai metadati dell'istanza

Se i tag dell'istanza sono consentiti nei metadati dell'istanza, la categoria `tags/instance` è accessibile dai metadati dell'istanza. Per esempi su come recuperare i tag dai metadati dell'istanza, consultare Ottenere i tag dell'istanza per un'istanza.

Aggiungere tag a una risorsa utilizzando CloudFormation

Con i tipi di risorse Amazon EC2, è possibile specificare i tag utilizzando una proprietà `Tags` o `TagSpecifications`.

I seguenti esempi aggiungono il tag **`Stack=Production`** all'AWS::EC2::Instanceutilizzo della sua `Tags` proprietà.

Example Esempio: Tag in YAML

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example Esempio: Tag in JSON

```
"Tags": [
    {
        "Key": "Stack",
        "Value": "Production"
    }
```

```
]
```

Gli esempi seguenti aggiungono il tag **`Stack=Production`** all'AWS::EC2::LaunchTemplate LaunchTemplateDatautilizzo della relativa `TagSpecifications` proprietà.

Example Esempio: TagSpecifications in YAML

```
TagSpecifications:
  - ResourceType: "instance"
    Tags:
    - Key: "Stack"
      Value: "Production"
```

Example Esempio: TagSpecifications in JSON

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
]
```

Service Quotas di Amazon EC2

In Amazon EC2 sono disponibili varie risorse che è possibile utilizzare. Queste risorse includono immagini, istanze, volumi e snapshot. Quando crei le tue Account AWS, impostiamo quote predefinite (note anche come limiti) su queste risorse in base alla regione. Ad esempio, esiste un numero massimo di istanze che puoi avviare in una regione. Pertanto, se devi avviare un'istanza nella regione Stati Uniti occidentali (Oregon), ad esempio, la richiesta non deve comportare il superamento del numero massimo di istanze in tale regione.

La console Service Quotas è una posizione centrale in cui è possibile visualizzare e gestire le quote per AWS i servizi e richiedere un aumento della quota per molte delle risorse utilizzate. Utilizza le informazioni sulle quote che forniamo per gestire la tua AWS infrastruttura. Pianifica le richieste di incremento delle quote con un certo anticipo rispetto a quando ne avrai effettivamente bisogno.

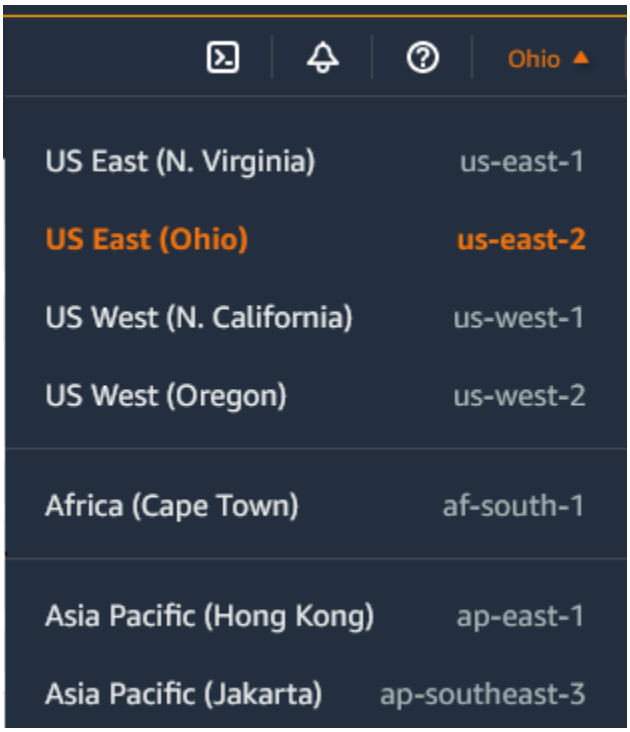
Per ulteriori informazioni, consulta Endpoint e quote Amazon EC2 e Endpoint e quote Amazon EBS nel. Riferimenti generali di Amazon Web Services

Visualizzazione delle quote correnti

È possibile visualizzare le quote per ciascuna regione utilizzando la console Service Quotas.

Visualizzazione delle quote correnti utilizzando la console Service Quotas

1. Aprire la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Nella barra di navigazione, nella parte superiore della schermata, seleziona una regione.



3. Utilizza il campo di filtro per filtrare l'elenco in base al nome della risorsa. Ad esempio, inserisci **`On-Demand`** per individuare le quote per le istanze on demand.
4. Per visualizzare ulteriori informazioni, scegli il nome della quota per aprire la pagina dei dettagli della quota.

Richiesta di un aumento

È possibile richiedere un aumento della quota per ciascuna regione.

Per richiedere un aumento utilizzando la console Service Quotas

1. Aprire la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Nella barra di navigazione, nella parte superiore della schermata, seleziona una regione.
3. Utilizza il campo di filtro per filtrare l'elenco in base al nome della risorsa. Ad esempio, inserisci **`On-Demand`** per individuare le quote per le istanze on demand.
4. Se la quota è modificabile, seleziona la quota e quindi scegli Richiedi aumento della quota.
5. In Modifica valore quota, inserisci il nuovo valore della quota.
6. Scegli Richiedi.
7. Per visualizzare eventuali richieste in sospeso o risolte di recente nella console, scegli Pannello di controllo dal riquadro di navigazione. Per le richieste in sospeso, scegliere lo stato della richiesta per aprire la ricevuta della richiesta. Lo stato iniziale di una richiesta è Pending (In attesa). Dopo la modifica dello stato in Quota richiesta, vedrai il numero del caso con AWS Support. Scegli il numero del caso per aprire il ticket della tua richiesta.

Per ulteriori informazioni, incluso come utilizzare AWS CLI o gli SDK per richiedere un aumento della quota, consulta Richiedere un aumento della quota nella Service Quotas User Guide.

Restrizione sull'e-mail inviata tramite la porta 25

Su tutte le istanze, Amazon EC2 limita il traffico in uscita agli indirizzi IP pubblici sulla porta 25 per impostazione predefinita. È possibile richiedere la rimozione di questa restrizione. Per ulteriori informazioni, consulta Come faccio a rimuovere la restrizione sulla porta 25 dalla mia istanza Amazon EC2 o dalla funzione Lambda?

> **Note**
>
> Questa restrizione non si applica al traffico in uscita inviato sulla porta 25 a:
>
> - Indirizzi IP nel blocco CIDR primario del VPC in cui esiste l'interfaccia di rete di origine.
> - Indirizzi IP nei CIDR definiti in RFC 1918, RFC 6598, e RFC 4193.

Risoluzione dei problemi relativi alle istanze EC2

Le procedure e i suggerimenti seguenti possono aiutarti a risolvere i problemi con le tue istanze Amazon EC2.

Indice

Problemi comuni con le istanze di Windows

I suggerimenti riportati di seguito possono aiutarti a risolvere problemi comuni associati alle istanze Windows Server EC2.

Problemi

- L'istanza perde la connettività di rete oppure le attività programmate non vengono eseguite quando previsto
- Impossibile ottenere l'output della console
- Windows Server 2012 R2 non disponibile sulla rete
- Collisione della firma del disco

I volumi EBS non vengono inizializzati su Windows Server 2016 e 2019

Le istanze create da Amazon Machine Image (AMI) di Windows Server 2016 e 2019 utilizzano l'agente EC2Launch v1 per una serie di attività di avvio, inclusa l'inizializzazione dei volumi EBS. Per impostazione predefinita, EC2Launch v1 non inizializza i volumi secondari. Tuttavia, puoi configurare EC2Launch v1 in modo che inizializzi questi dischi automaticamente, come indicato di seguito.

Mappatura delle lettere di unità nei volumi

1. Connettersi all'istanza da configurare e aprire il file `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` in un editor di testo.
2. Specifica le impostazioni del volume, come indicato di seguito:

```
{
"driveLetterMapping": [
 {
   "volumeName": "sample volume",
   "driveLetter": "H"
 }]
}
```

3. Salvare le modifiche e chiudere il file.
4. Apri Windows PowerShell e usa il seguente comando per eseguire lo script EC2Launch v1 che inizializza i dischi:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

   Per inizializzare i dischi ogni volta che l'istanza si avvia, aggiungere il contrassegno `-Schedule` come segue:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

L'agente EC2Launch v1 può eseguire script di inizializzazione delle istanze, come `initializeDisks.ps1` in parallelo con lo script `InitializeInstance.ps1`. Se lo script `InitializeInstance.ps1` riavvia l'istanza, potrebbe interrompere altre attività pianificate eseguite all'avvio dell'istanza. Per evitare potenziali conflitti, consigliamo di aggiungere logica allo script `initializeDisks.ps1`per garantire che l'inizializzazione dell'istanza venga terminata per prima.

> **Note**
>
> Se lo script EC2Launch non inizializza i volumi, assicurati che i volumi siano online. In caso contrario, esegui il comando seguente per portarli online.
>
> ```
> PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
>  $False
> ```

Avvio di un'istanza EC2 Windows in Directory Services Restore Mode (DSRM)

Se un'istanza che esegue Microsoft Active Directory sperimenta un errore di sistema o altri problemi critici, puoi risolvere tali anomalie avviando l'istanza in una versione speciale della modalità provvisoria denominata Directory Services Restore Mode (DSRM). Questa modalità ti permette di riparare o recuperare Active Directory.

Supporto driver per DSRM

Il modo di abilitare DSRM e avviare nell'istanza dipende dai driver che eseguono l'istanza. Nella console EC2 puoi visualizzare i dettagli della versione del driver per un'istanza dal log di sistema. La tabella seguente mostra quali driver sono supportati per DSRM.

Versioni driver	DSRM supportata?	Fasi successive
Citrix PV 5.9	No	Ripristina l'istanza da un backup. Non puoi abilitare DSRM.
AWS PV 7.2.0	No	Anche se la modalità DSRM non è supportata dal driver, puoi comunque distaccare il volume root dall'istanza, acquisire uno snapshot del volume o creare un'AMI da esso, quindi collegarlo a un'altra istanza nella stessa zona di disponibilità come volume secondario. Puoi quindi abilitare DSRM (come descritto in questa sezione).
AWS PV 7.2.2 e versioni successive	Sì	Distacca il volume root, collegalo a un'altra istanza e abilita DSRM (come descritto in questa sezione).
Reti avanzate	Sì	Distacca il volume root, collegalo a un'altra istanza e abilita DSRM (come descritto in questa sezione).

Per informazioni su come abilitare una rete avanzata, vedere. the section called “Elastic Network Adapter (ENA)” Per informazioni sull'aggiornamento dei driver AWS PV, consulta Aggiornamento dei driver PV su istanze Windows.

Configurazione di un'istanza da avviare in DSRM

Le istanze EC2 Windows non dispongono di una connessione di rete finché che il sistema operativo non è in esecuzione. Per questa ragione, non puoi premere il pulsante F8 sulla tastiera per selezionare un'opzione di avvio. È necessario utilizzare una delle procedure seguenti per avviare un'istanza Windows Server EC2 in modalità DSRM.

Se sospetti che Active Directory sia stato danneggiato e che l'istanza sia ancora in esecuzione, puoi configurare l'istanza per l'avvio in modalità DSRM utilizzando sia la finestra di dialogo di configurazione del sistema o il prompt dei comandi.

Per avviare un'istanza online in modalità DSRM tramite la finestra di dialogo di configurazione del sistema

1. Nella finestra di dialogo Run (Esegui) digitare `msconfig` e premere Invio.
2. Scegliere la scheda Boot (Avvio).
3. In Boot options (Opzioni di avvio) scegliere Safe boot (Avvio sicuro).
4. Scegliere Active Directory repair (Riparazione di Active Directory), quindi OK. Il sistema ti invita a riavviare il server.

Per avviare un'istanza online in modalità DSRM utilizzando la riga di comando

Da una finestra del prompt dei comandi, esegui il comando seguente:

```
bcdedit /set safeboot dsrepair
```

Se un'istanza è offline e irraggiungibile, distacca il volume root e collegalo a un'altra istanza per abilitare la modalità DSRM.

Per avviare un'istanza offline in modalità DSRM

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Individua e seleziona l'istanza interessata. Scegli Instance state (Stato istanza), Stop instance (Arresta istanza).
4. Scegli Launch instances (Avvia le istanze) e crea un'istanza temporanea nella stessa Zona di disponibilità dell'istanza interessata. Scegliere un tipo di istanza che utilizzi una versione diversa di Windows. Ad esempio, se la tua istanza è Windows Server 2016, scegli un'istanza di Windows Server 2019.

   > **Important**
   >
   > Se non crei l'istanza nella stessa Zona di disponibilità dell'istanza interessata, non potrai collegare il volume root dell'istanza interessata sulla nuova istanza.

5. Nel riquadro di navigazione, selezionare Volumes (Volumi).
6. Individua il volume root dell'istanza interessata. Distaccare il volume e collegarlo all'istanza temporanea creata in precedenza. Collegala con il nome del dispositivo predefinito (xvdf).

7. Utilizzare Desktop remoto per collegarsi all'istanza temporanea, quindi usare l'utilità Disk Management (Gestione disco) per rendere il volume disponibile per l'uso.
8. Aprire un prompt dei comandi ed eseguire il comando seguente. Sostituire D con la lettera di unità effettiva del volume secondario appena collegato:

```
bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
```

9. Nell'utilità Disk Management (Gestione disco), scegliere l'unità collegata in precedenza, aprire il menu contestuale (pulsante destro del mouse) e scegliere Offline.
10. Nella console EC2, distaccare il volume interessato dall'istanza temporanea e ricollegarlo all'istanza originale con il nome dispositivo `/dev/sda1`. Devi specificare questo nome del dispositivo per indicare il volume come volume root.
11. Avviare l'istanza.
12. Dopo che l'istanza ha superato i controlli dello stato nella console EC2, connettersi all'istanza tramite Desktop remoto e verificare che si avvii in modalità DSRM.
13. (Facoltativo) Eliminare o arrestare l'istanza temporanea creata in questa procedura.

L'istanza perde la connettività di rete oppure le attività programmate non vengono eseguite quando previsto

Se si riavvia l'istanza e si perde la connettività di rete, è possibile che l'ora dell'istanza sia errata.

Per impostazione predefinita, le istanze Windows utilizzano il formato UTC. Se si imposta l'ora dell'istanza su un fuso orario differente e successivamente la si riavvia, si produce una differenza oraria e l'istanza perde temporaneamente il suo indirizzo IP. L'istanza ristabilisce la connettività di rete alla fine, ma ciò può richiedere alcune ore. La quantità di tempo richiesta per tale recupero dipende dalla differenza tra UTC e l'altro fuso orario.

Lo stesso problema temporale può causare anche la mancata esecuzione di attività pianificate nel momento previsto. In questo caso, tali attività non vengono eseguite quando previsto perché l'ora dell'istanza è errata.

Per utilizzare un fuso orario diverso da UTC in modo persistente, devi impostare la chiave di RealTimeIsUniversalregistro. Senza questa chiave, un'istanza utilizza UTC dopo il riavvio.

Per risolvere problemi temporali che causano la perdita della connettività di rete

1. Assicurarsi di eseguire i driver PV raccomandati. Per ulteriori informazioni, consulta the section called “Aggiornamento dei driver PV”.
2. Verificate che la seguente chiave di registro esista e sia impostata su1: HKEY_LOCAL_MACHINE\ SYSTEM\ Set\ Control\ Information\ CurrentControl TimeZone RealTime IsUniversal

Impossibile ottenere l'output della console

Per le istanze Windows, la console dell'istanza mostra l'output delle attività eseguite durante il processo di avvio di Windows. Se Windows si avvia correttamente, l'ultimo messaggio registrato è `Windows is Ready to use`. È inoltre possibile visualizzare i messaggi del registro degli eventi nella console, ma questa funzionalità potrebbe non essere abilitata per impostazione predefinita a seconda della versione di Windows in uso. Per ulteriori informazioni, consulta the section called “Configura gli agenti di avvio di Windows”.

Per ottenere l'output della console per l'istanza utilizzando la console Amazon EC2, selezionare l'istanza, scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get system log (Ottieni il log di sistema). Per ottenere l'output della console utilizzando la riga di comando, utilizzate uno dei seguenti comandi: get-console-output (AWS CLI) o (). Get-EC2ConsoleOutputAWS Tools for Windows PowerShell

Per le istanze che eseguono Windows Server 2012 R2 e versioni precedenti, l'output della console vuoto potrebbe indicare un problema con il servizio EC2Config, come un file di configurazione configurato in modo errato o un errore di avvio di Windows. Per correggere il problema, scarica e installa la versione più recente del servizio EC2Config. Per ulteriori informazioni, consulta the section called “Installazione di EC2Config”.

Windows Server 2012 R2 non disponibile sulla rete

Per informazioni sulla risoluzione dei problemi di un'istanza di Windows Server 2012 R2 che non è disponibile sulla rete, vedi Windows Server 2012 R2 perde la connettività di rete e di archiviazione dopo il riavvio di un'istanza.

Collisione della firma del disco

Puoi controllare e risolvere le collisioni della firma del disco utilizzando EC2Rescue per Windows Server. In alternativa, puoi risolvere manualmente i problemi di firma del disco completando la seguente procedura.

> **Warning**
>
> Nella procedura seguente viene descritto come modificare il Registro di sistema di Windows utilizzando l'editor del Registro di sistema. Se non hai familiarità con il Registro di sistema di Windows o non sai come apportare modifiche in modo sicuro utilizzando l'editor del Registro di sistema, consulta Configura il Registro di sistema.

1. Apri un prompt dei comandi, digita regedit.exe e premi Invio.
2. In Registry Editor (Editor del Registro di sistema), scegli HKEY_LOCAL_MACHINE dal menu contestuale (tasto destro del mouse), quindi seleziona Find (Cerca).
3. Digita Windows Boot Manager e quindi seleziona Find Next (Trova successivo).
4. Scegli la chiave denominata `11000001`. Questa chiave è un pari livello della chiave trovata nella fase precedente.
5. Nel riquadro a destra, seleziona `Element` e quindi Modify (Modifica) dal menu contestuale (tasto destro del mouse).
6. Individua la firma del disco a quattro byte con offset 0x38 nei dati. Questa è la firma BCD (Boot Configuration Database). Inverti i byte per creare la firma del disco e annotala. Ad esempio, la firma del disco rappresentata dai seguenti dati è `E9EB3AA5`:

   ```
   ...
   0030  00 00 00 00 01 00 00 00
   0038  A5 3A EB E9 00 00 00 00
   0040  00 00 00 00 00 00 00 00
   ...
   ```

7. In una finestra del prompt dei comandi, esegui il comando seguente per avviare Microsoft DiskPart.

   ```
   diskpart
   ```

8. Esegui il `select disk` DiskPart comando e specifica il numero del disco per il volume con la collisione della firma del disco.

   > **Tip**
   >
   > Per verificare il numero del disco relativo al volume con la collisione della firma del disco, utilizza l'utilità Gestione disco. Apri un prompt dei comandi, digita `compmgmt.msc` e premi Invio. Nel pannello di navigazione a sinistra, fai doppio clic su Gestione disco. Nell'utilità Gestione disco, verifica il numero del disco per il volume offline con la collisione della firma del disco.

   ```
   DISKPART> select disk 1
   Disk 1 is now the selected disk.
   ```

9. Esegui il DiskPart comando seguente per ottenere la firma del disco.

   ```
   DISKPART>  uniqueid disk
   Disk ID: 0C764FA8
   ```

10. Se la firma del disco mostrata nel passaggio precedente non corrisponde alla firma del disco che hai annotato in precedenza, usa il DiskPart comando seguente per modificare la firma del disco in modo che corrisponda:

    ```
    DISKPART> uniqueid disk id=E9EB3AA5
    ```

Messaggi comuni con istanze di Windows

Questa sezione include suggerimenti per risolvere i problemi sulla base di messaggi comuni.

Messaggi

- "La password non è disponibile"
- "Password non ancora disponibile"
- "Impossibile recuperare la password di Windows"
- "In attesa del servizio di metadati"
- "Impossibile attivare Windows"

- "Windows non è originale (0x80070005)"
- "Nessun server Terminal Server License disponibile per fornire una licenza"
- "Alcune impostazioni sono gestite dalla tua organizzazione"

"La password non è disponibile"

Per connetterti a un'istanza Windows tramite Remote Desktop, è necessario specificare un account e una password. Gli account e le password forniti si basano sull'AMI utilizzata per avviare l'istanza. Puoi recuperare la password generata automaticamente per l'account Amministratore oppure utilizzare l'account e la password in uso nell'istanza originale da cui è stata creata l'AMI.

Puoi generare una password per l'account amministratore per le istanze avviate utilizzando un'AMI Windows personalizzata. Per generare la password, devi configurare alcune impostazioni nel sistema operativo prima della creazione dell'AMI. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.

Se l'istanza Windows non è configurata per generare una password casuale, riceverai il messaggio seguente al momento del recupero della password generata automaticamente tramite la console:

```
Password is not available.
The instance was launched from a custom AMI, or the default password has changed. A
password cannot be retrieved for this instance. If you have forgotten your password,
 you can
reset it using the Amazon EC2 configuration service. For more information, see
 Passwords for a
Windows Server instance.
```

Verifica l'output della console per l'istanza per vedere se l'AMI utilizzata per avviarla era stata creata con la generazione di password disattivata. Se la generazione di password è disattivata, l'output della console contiene quanto segue:

```
Ec2SetPassword: Disabled
```

Se la generazione di password è disattivata e non ricordi la password dell'istanza originale, puoi reimpostarla per tale istanza. Per ulteriori informazioni, consulta Reimpostazione di una password amministratore Windows persa o scaduta.

"Password non ancora disponibile"

Per connetterti a un'istanza Windows tramite Remote Desktop, è necessario specificare un account e una password. Gli account e le password forniti si basano sull'AMI utilizzata per avviare l'istanza. Puoi recuperare la password generata automaticamente per l'account Amministratore oppure utilizzare l'account e la password in uso nell'istanza originale da cui è stata creata l'AMI.

La password dovrebbe essere disponibile in pochi minuti. Se la password non è disponibile, riceverai il messaggio seguente al momento del recupero della password generata automaticamente tramite la console:

```
Password not available yet.
Please wait at least 4 minutes after launching an instance before trying to retrieve
 the
auto-generated password.
```

Se sono trascorsi più di quattro minuti senza ricevere la password, è possibile che l'agente di avvio per la tua istanza non sia configurato per generare una password. Verifica controllando se l'output della console è vuoto. Per ulteriori informazioni, consulta Impossibile ottenere l'output della console.

Verifica inoltre che l'`ec2:GetPasswordData`azione sia consentita sull'account AWS Identity and Access Management (IAM) utilizzato per accedere al portale di gestione. Per ulteriori informazioni sulle autorizzazioni IAM, consulta l'articolo relativo alla descrizione di IAM.

"Impossibile recuperare la password di Windows"

Per recuperare la password generata automaticamente per l'account Amministratore, è necessario utilizzare la chiave privata per la coppia di chiavi specificata all'avvio dell'istanza. Se non specifichi una coppia di chiavi quando viene avviata l'istanza, riceverai il messaggio seguente.

```
Cannot retrieve Windows password
```

Puoi terminare l'istanza e avviarne una nuova utilizzando la stessa AMI, assicurandoti di specificare una coppia di chiavi.

"In attesa del servizio di metadati"

Un'istanza Windows deve ottenere informazioni dai suoi metadati prima di attivarsi. Per impostazione predefinita, il valore `WaitForMetaDataAvailable` assicura che il servizio EC2Config attenda

che i metadati dell'istanza siano accessibili prima di proseguire con il processo di avvio. Per ulteriori informazioni, consulta Utilizzo dei metadati delle istanze.

Se l'istanza non supera la prova di raggiungibilità, prova a eseguire queste operazioni per risolvere il problema.

- Controllare il blocco CIDR per il VPC. Un'istanza Windows non può avviarsi correttamente se avviata in un VPC con un intervallo di indirizzi IP che varia da `224.0.0.0` a `255.255.255.255` (intervalli di indirizzi IP di classe D e classe E). Tali intervalli sono riservati e non devono essere assegnati ai dispositivi host. Si consiglia di creare un VPC con un blocco CIDR dagli intervalli di indirizzi IP privati (non instradabili pubblicamente), come specificato in RFC 1918.
- È possibile che il sistema sia stato configurato con un indirizzo IP statico. Provare a creare un'interfaccia di rete e a collegarla all'istanza.
- Per abilitare DHCP su un'istanza Windows con la quale non è possibile connettersi

  1. Arrestare l'istanza interessata e distaccarne il volume root.
  2. Avviare un'istanza temporanea nella stessa zona di disponibilità dell'istanza interessata.

     > **Warning**
     >
     > Se la tua istanza temporanea si basa sulla stessa AMI su cui si basa l'istanza originale, devi completare ulteriori operazioni o non sarai in grado di avviare l'istanza originale dopo aver ripristinato il volume radice a causa di una collisione di firme del disco. In alternativa, seleziona un'AMI diversa per l'istanza temporanea. Ad esempio, se l'istanza originale utilizza l'AMI AWS Windows per Windows Server 2016, avvia l'istanza temporanea utilizzando l'AMI AWS Windows per Windows Server 2019.

  3. Collegare il volume radice dall'istanza interessata all'istanza temporanea. Connettersi all'istanza temporanea, aprire l'utilità Disk Management (Gestione disco) e portare l'unità online.
  4. Dall'istanza temporanea aprire Regedit e selezionare HKEY_LOCAL_MACHINE. Dal menu File scegliere Load Hive (Carica Hive). Selezionare l'unità, aprire il file `Windows\System32\config\SYSTEM` e specificare un nome della chiave quando richiesto (è possibile utilizzare qualsiasi nome).
  5. Selezionare la chiave appena caricata e passare a `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Ciascuna interfaccia di rete è elencata da una GUID. Selezionare l'interfaccia di rete corretta. Se DHCP è disattivato e un indirizzo IP statico è

assegnato, `EnableDHCP` è impostato su 0. Per abilitare DHCP, impostare `EnableDHCP` su 1, quindi eliminare le chiavi seguenti, se presenti: `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Selezionare nuovamente la chiave e, dal menu File, scegliere Unload Hive (Scarica Hive).

> **Note**
>
> In presenza di più interfacce di rete, sarà necessario identificare l'interfaccia corretta per attivare DHCP. Per identificare l'interfaccia di rete corretta, esaminare i seguenti valori della chiave `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Questi valori mostrano la configurazione statica della precedente istanza.

6. (Facoltativo) Se DHCP è già attivato, è possibile che non sia disponibile alcun percorso al servizio di metadati. È possibile risolvere questo problema aggiornando il servizio EC2Config.

   a. Scaricare e installare la versione più recente del servizio EC2Config. Per ulteriori informazioni sull'installazione di questo servizio, consulta the section called “Installazione di EC2Config”.

   b. Estrarre i file dal file `.zip` nella directory `Temp` sull'unità collegata.

   c. Aprire Regedit e selezionare HKEY_LOCAL_MACHINE. Dal menu File scegliere Load Hive (Carica Hive). Selezionare l'unità, aprire il file `Windows\System32\config\SOFTWARE` e specificare un nome della chiave quando richiesto (è possibile utilizzare qualsiasi nome).

   d. Selezionare la chiave appena caricata e passare a `Microsoft\Windows\CurrentVersion`. Selezionare la chiave `RunOnce`. (Se questa chiave non esiste, fare clic con il pulsante destro del mouse su `CurrentVersion`, puntare su New (Nuovo), selezionare Key (Chiave) e nominare la chiave `RunOnce`). Fare clic con il pulsante destro del mouse, puntare su New (Nuovo), quindi selezionare String Value (Valore stringa). Immettere il nome `Ec2Install` e i dati `C:\Temp\Ec2Install.exe -q`.

   e. Selezionare nuovamente la chiave e, dal menu File, scegliere Unload Hive (Scarica Hive).

7. (Facoltativo) Se la tua istanza temporanea si basa sulla stessa AMI su cui si basa quella originale, devi completare ulteriori operazioni o non sarai in grado di avviare l'istanza originale dopo aver ripristinato il volume di root a causa di un conflitto di firme del disco.

> **Warning**
>
> Nella procedura seguente viene descritto come modificare il Registro di sistema di Windows utilizzando l'editor del Registro di sistema. Se non hai familiarità con il Registro di sistema di Windows o non sai come apportare modifiche in modo sicuro utilizzando l'editor del Registro di sistema, consulta Configura il Registro di sistema.

a. Apri un prompt dei comandi, digita regedit.exe e premi Invio.

b. In Registry Editor (Editor del Registro di sistema), scegli HKEY_LOCAL_MACHINE dal menu contestuale (tasto destro del mouse), quindi seleziona Find (Cerca).

c. Digita Windows Boot Manager e quindi seleziona Find Next (Trova successivo).

d. Scegli la chiave denominata `11000001`. Questa chiave è un pari livello della chiave trovata nella fase precedente.

e. Nel riquadro a destra, seleziona `Element` e quindi Modify (Modifica) dal menu contestuale (tasto destro del mouse).

f. Individua la firma del disco a quattro byte con offset 0x38 nei dati. Inverti i byte per creare la firma del disco e annotala. Ad esempio, la firma del disco rappresentata dai seguenti dati è `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. In una finestra del prompt dei comandi, esegui il comando seguente per avviare Microsoft DiskPart.

```
diskpart
```

h. Esegui il DiskPart comando seguente per selezionare il volume. (È possibile verificare che il numero del disco sia 1 utilizzando l'utilità Gestione del disco.)

```
DISKPART> select disk 1
```

```
Disk 1 is now the selected disk.
```

i. Esegui il DiskPart comando seguente per ottenere la firma del disco.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Se la firma del disco mostrata nel passaggio precedente non corrisponde alla firma del disco BCD che hai annotato in precedenza, usa il DiskPart comando seguente per modificare la firma del disco in modo che corrisponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. Tramite l'utilità Disk Management (Gestione disco), portare l'unità offline.

> **Note**
>
> L'unità è automaticamente non in linea se l'istanza temporanea esegue lo stesso sistema operativo dell'istanza interessata, quindi non sarà necessario disconnetterla manualmente.

9. Distaccare il volume dall'istanza temporanea. Se non si utilizza più l'istanza temporanea, è possibile terminarla.
10. Ripristinare il volume root dell'istanza interessata collegandolo come `/dev/sda1`.
11. Avviare l'istanza interessata.

Se sei connesso all'istanza, apri un browser Internet dall'istanza e immetti l'URL seguente per il server di metadati:

```
http://169.254.169.254/latest/meta-data/
```

Se non riesci a contattare il server di metadati, prova a eseguire queste operazioni per risolvere il problema:

- Scaricare e installare la versione più recente del servizio EC2Config. Per ulteriori informazioni sull'installazione di questo servizio, consulta the section called “Installazione di EC2Config”.

- Verificate se nell'istanza di Windows sono in esecuzione driver RedHat PV. In tal caso, aggiornare i driver PV di Citrix. Per ulteriori informazioni, consulta the section called “Aggiornamento dei driver PV”.
- Verificare che le impostazioni di firewall, IPSec e proxy non blocchino il traffico in uscita verso il servizio di metadati (`169.254.169.254`) o i server AWS KMS (gli indirizzi sono specificati negli elementi `TargetKMSServer` in `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml`).
- Verificare che sia disponibile un percorso al servizio di metadati (`169.254.169.254`) utilizzando il comando seguente.

```
route print
```

- Verificare eventuali problemi di rete che potrebbero interessare la zona di disponibilità dell'istanza. Vai a http://status.aws.amazon.com/.

"Impossibile attivare Windows"

Le istanze Windows utilizzano l'attivazione di Windows AWS KMS . Puoi ricevere questo messaggio:`A problem occurred when Windows tried to activate. Error Code 0xC004F074`, se l'istanza non riesce a raggiungere il AWS KMS server. Windows deve essere attivato ogni 180 giorni. EC2Config tenta di contattare il AWS KMS server prima della scadenza del periodo di attivazione per garantire che Windows rimanga attivo.

Se riscontri un problema di attivazione di Windows, utilizza la procedura seguente per risolvere il problema.

Per EC2Config (AMI di Windows Server 2012 R2 e precedenti)

1. Scaricare e installare la versione più recente del servizio EC2Config. Per ulteriori informazioni sull'installazione di questo servizio, consulta the section called “Installazione di EC2Config”.
2. Connettersi all'istanza e aprire il file seguente: `C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml`.
3. Individua il plugin Ec2 WindowsActivate nel file. `config.xml` Modificare lo stato in Enabled (Abilitato) e salvare le modifiche.
4. Nell'applicazione Servizi di Windows, riavviare il servizio EC2Config o l'istanza.

Se la procedura non risolve il problema di attivazione, esegui queste operazioni aggiuntive.

1. Imposta l' AWS KMS obiettivo: C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Attivare Windows: C:\> slmgr.vbs /ato

Per EC2Launch (AMI di Windows Server 2016 e successive)

1. Da un PowerShell prompt con diritti amministrativi, importa il modulo EC2Launch:

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1"
```

2. Richiama la funzione Add-Routes per visualizzare l'elenco dei nuovi percorsi:

```
PS C:\> Add-Routes
```

3. Chiama la funzione Set-: ActivationSettings

```
PS C:\> Set-Activationsettings
```

4. Quindi, esegui lo script seguenti per attivare Windows:

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Se continui a ricevere un errore di attivazione sia per EC2Config che per EC2Launch, verifica le informazioni seguenti.

- Verificate di disporre di percorsi verso i AWS KMS server. Apri `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` e individua gli elementi `TargetKMSServer`. Esegui il comando seguente e controlla se gli indirizzi di questi AWS KMS server sono elencati.

```
route print
```

- Verifica che la chiave AWS KMS client sia impostata. Esegui il comando seguente e controllare l'output.

```
C:\Windows\System32\slmgr.vbs /dlv
```

Se l'output contiene Error: product key not found, la chiave AWS KMS client non è impostata. Se la chiave AWS KMS client non è impostata, cerca la chiave client come descritto in questo articolo di Microsoft: AWS KMS Client Setup Keys, quindi esegui il comando seguente per impostare la chiave AWS KMS client.

```
C:\Windows\System32\slmgr.vbs /ipk client_key
```

- Verifica l'ora e il fuso orario del sistema siano corretti. Se utilizzi un fuso orario diverso da UTC, aggiungi la seguente chiave di registro e impostala 1 per assicurarti che l'ora sia corretta:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal`.
- Se Windows Firewall è abilitato, disattivalo temporaneamente utilizzando il comando seguente.

```
netsh advfirewall set allprofiles state off
```

"Windows non è originale (0x80070005)"

Le istanze di Windows utilizzano l'attivazione di Windows AWS KMS . Se un'istanza non è in grado di completare il processo di attivazione, segnala che la copia di Windows non è originale.

Segui i suggerimenti della sezione "Impossibile attivare Windows".

"Nessun server Terminal Server License disponibile per fornire una licenza"

Per impostazione predefinita, Windows Server prevede una licenza per due utenti simultanei tramite Desktop remoto. Se è necessario garantire a più di due utenti l'accesso simultaneo all'istanza Windows tramite Desktop remoto, puoi acquistare una licenza CAL per Servizi Desktop remoto e installare l'host della sessione di Desktop remoto e i ruoli del Server licenze di Desktop remoto.

Verifica i problemi seguenti:

- Hai superato il numero massimo di sessioni RDP simultanee.
- Hai installato il ruolo di Servizi Desktop remoto di Windows.
- La licenza è scaduta. Se la licenza è scaduta, non puoi connetterti con l'istanza Windows come utente. Puoi eseguire le operazioni indicate di seguito:
  - Connettiti all'istanza da una riga di comando utilizzando un parametro `/admin`, ad esempio:

```
mstsc /v:instance /admin
```

Per ulteriori informazioni, consulta il seguente articolo di Microsoft sull'Accesso al desktop remoto tramite riga di comando.

- Arresta l'istanza, distaccane i volumi Amazon EBS e collegali a un'altra istanza nella stessa zona di disponibilità per recuperare i dati.

"Alcune impostazioni sono gestite dalla tua organizzazione"

Le istanze lanciate dalle ultime AMI di Windows Server potrebbero mostrare il seguente messaggio di Windows Update: "Alcune impostazioni sono gestite dalla tua organizzazione". Questo messaggio viene visualizzato a seguito di modifiche apportate a Windows Server e non influisce sul comportamento di Windows Update o sulla possibilità di gestire le impostazioni di aggiornamento.

Per rimuovere l'avviso

1. Aprire `gpedit.msc` e navigare su Computer Configuration (Configurazione computer), Administrative Templates (Modelli amministrativi), Windows Components (Computer Windows), Windows updates (Aggiornamenti Windows). Modifica Configure Automatic Update (Configura aggiornamento automatico) e impostalo su enabled (abilitato).
2. In un prompt dei comandi, aggiornare la policy di gruppo utilizzando gpupdate /force.
3. Chiudere e riaprire le impostazioni di Windows Update. Sarà visualizzato il messaggio riportato sopra riguardante la gestione delle impostazioni da parte dell'organizzazione, seguito da "Scaricheremo automaticamente gli aggiornamenti, tranne che nelle connessioni a consumo (dove potrebbero applicarsi costi). In quel caso, scaricheremo automaticamente gli aggiornamenti richiesti per il buon funzionamento di Windows".
4. Tornare a `gpedit.msc` e impostare nuovamente le policy di gruppo su not configured (non configurati). Eseguire nuovamente gpupdate /force.
5. Chiudere il prompt dei comandi e attendere alcuni minuti.
6. Riaprire le impostazioni di Windows Update. Non dovrebbe essere visualizzato il messaggio "Alcune impostazioni sono gestite dall'organizzazione".

Risoluzione dei problemi di avvio delle istanze

I seguenti problemi impediscono l'avvio di un'istanza.

Problemi di avvio

- Nome del dispositivo non valido
- Superamento del limite di istanze
- Capacità insufficiente dell'istanza
- La configurazione richiesta attualmente non è supportata. Controlla la documentazione per verificare le configurazioni supportate.
- Terminazione immediata dell'istanza
- Autorizzazioni insufficienti
- Utilizzo elevato della CPU poco dopo l'avvio di Windows (solo istanze Windows)

Nome del dispositivo non valido

Descrizione

Viene restituito l'errore `Invalid device name` *`device_name`* quando si tenta di avviare una nuova istanza.

Causa

La visualizzazione di questo errore durante l'avvio di un'istanza indica che il nome del dispositivo specificato per uno o più volumi nella richiesta ha un nome del dispositivo non valido. Tra le cause possibili sono incluse:

- Il nome del dispositivo potrebbe essere utilizzato dall'AMI selezionata.
- Il nome del dispositivo potrebbe essere riservato ai volumi root.
- Il nome del dispositivo potrebbe essere utilizzato per un altro volume nella richiesta.
- Il nome del dispositivo potrebbe non essere valido per il sistema operativo.

Soluzione

Per risolvere il problema:

- Verifica che il nome del dispositivo non sia utilizzato nell'AMI selezionata. Esegui il comando seguente per visualizzare i nomi dei dispositivi utilizzati dall'AMI.

```
aws ec2 describe-images --image-id ami_id --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- Evita di utilizzare un nome di dispositivo riservato ai volumi root. Per ulteriori informazioni, consulta Nomi dei dispositivi disponibili.
- Verifica che ogni volume specificato nella richiesta disponga di un nome di dispositivo univoco.
- Verifica che i nomi dei dispositivi specificati siano nel formato corretto. Per ulteriori informazioni, consulta Nomi dei dispositivi disponibili.

Superamento del limite di istanze

Descrizione

Viene restituito l'errore `InstanceLimitExceeded` quando si tenta di avviare una nuova istanza o di riavviare un'istanza interrotta.

Causa

Se viene restituito un errore `InstanceLimitExceeded` mentre si tenta di avviare una nuova istanza o di riavviare un'istanza interrotta, significa che è stato raggiunto il numero massimo di istanze che si possono avviare in una regione. Quando crei il tuo AWS account, impostiamo limiti predefiniti sul numero di istanze che puoi eseguire in base alla regione.

Soluzione

È possibile richiedere un aumento del limite di istanze in base alle singole regioni. Per ulteriori informazioni, consulta Service Quotas di Amazon EC2.

Capacità insufficiente dell'istanza

Descrizione

Viene restituito l'errore `InsufficientInstanceCapacity` quando si tenta di avviare una nuova istanza o di riavviare un'istanza interrotta.

Causa

Se viene restituito un errore quando si tenta di avviare un'istanza o di riavviare un'istanza interrotta, significa che AWS al momento non dispone di sufficiente capacità on demand per evadere la richiesta.

Soluzione

Per risolvere il problema, prova a eseguire queste operazioni:

- Attendere alcuni minuti, quindi inviare di nuovo la richiesta; la capacità può cambiare di frequente.
- Inviare una nuova richiesta con un numero ridotto di istanze. Ad esempio, se si effettua un'unica richiesta di avvio di 15 istanze, tentare creando 3 richieste per 5 istanze oppure 15 richieste per 1 istanza.
- Se si sta avviando un'istanza, inviare una nuova richiesta senza specificare alcuna zona di disponibilità.
- Se si sta avviando un'istanza, inviare una nuova richiesta utilizzando un tipo di istanza diverso (che è possibile ridimensionare in un secondo momento). Per ulteriori informazioni, consulta Cambiare il tipo di istanza.
- Se si stanno avviando delle istanze in un gruppo di collocazione cluster, si potrebbe ricevere un errore di capacità insufficiente. Per ulteriori informazioni, consulta Lavorare con gruppi di collocamento.

La configurazione richiesta attualmente non è supportata. Controlla la documentazione per verificare le configurazioni supportate.

Descrizione

Viene visualizzato l'errore `Unsupported` quando si tenta di avviare una nuova istanza perché la configurazione dell'istanza non è supportata.

Causa

Il messaggio di errore fornisce ulteriori dettagli. Ad esempio, un tipo di istanza o un'opzione di acquisto di istanza potrebbe non essere supportata nell'area o nella zona di disponibilità specificata.

Soluzione

Prova con una configurazione di istanza diversa. Per cercare un tipo di istanza che soddisfi i requisiti, consulta Individuazione di un tipo di istanza Amazon EC2.

Terminazione immediata dell'istanza

Descrizione

La tua istanza passa dallo stato `pending` allo stato `terminated`.

Causa

Di seguito sono riportati alcuni motivi per cui un'istanza potrebbe terminare immediatamente:

- Hai superato i limiti di volume EBS. Per ulteriori informazioni, consulta Limiti dei volumi delle istanze.
- Una snapshot EBS è danneggiata.
- Il volume EBS root è crittografato e non disponi delle autorizzazioni per accedere alla Chiave KMS per la decrittografia.
- Uno snapshot specificato nel mapping del dispositivo a blocchi per l'AMI è crittografato e non si dispone delle autorizzazioni per accedere alla Chiave KMS per la decrittografia o non si dispone dell'accesso alla Chiave KMS per crittografare i volumi ripristinati.
- Nell'AMI supportata da instance store utilizzata per avviare l'istanza manca una parte obbligatoria (un file image.part.xx).

Per ulteriori informazioni, ottenere il motivo della cessazione utilizzando uno dei seguenti metodi.

Per recuperare il motivo della terminazione tramite console Amazon EC2

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza.
3. Nella prima scheda, individuare il motivo accanto a State transition reason (Motivo transizione stato).

Per conoscere il motivo della cessazione, utilizza il AWS Command Line Interface

1. Utilizzare il comando describe-instances e specificare l'ID istanza.

```
aws ec2 describe-instances --instance-id instance_id
```

2. Analizzare la risposta JSON restituita dal comando e annotare i valori nell'elemento della risposta `StateReason`.

   Il seguente blocco di codice mostra un esempio di un elemento di risposta `StateReason`.

```
"StateReason": {
  "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
  "Code": "Server.InternalError"
},
```

Per ottenere il motivo della cessazione utilizzando AWS CloudTrail

Per ulteriori informazioni, consulta Visualizzazione degli eventi con cronologia degli CloudTrail eventi nella Guida per l'AWS CloudTrail utente.

Soluzione

Eseguire una delle seguenti operazioni, a seconda del motivo della terminazione:

- **`Client.VolumeLimitExceeded: Volume limit exceeded`** — Eliminare i volumi inutilizzati. È possibile inviare una richiesta per aumentare il limite di volume.
- **`Client.InternalError: Client error on launch`**— Assicurati di disporre delle autorizzazioni necessarie per accedere ai dati AWS KMS keys utilizzati per decrittografare e crittografare i volumi. Per ulteriori informazioni, consulta Utilizzo delle policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

Autorizzazioni insufficienti

Descrizione

Viene restituito l'errore `"errorMessage": "You are not authorized to perform this operation."` quando provi ad avviare una nuova istanza e l'avvio fallisce.

Causa

Se ricevi questo errore quando provi ad avviare un'istanza, non disponi delle autorizzazioni IAM necessarie per farlo.

Alcune delle possibili autorizzazioni mancanti sono le seguenti:

- `ec2:RunInstances`
- `iam:PassRole`

Potrebbero inoltre essere richieste altre autorizzazioni. Per l'elenco delle autorizzazioni necessarie per avviare un'istanza, consulta le policy IAM di esempio nelle pagine Esempio: utilizzo della procedura guidata per l'avvio dell'istanza EC2 e Avvia istanze () RunInstances.

Soluzione

Per risolvere il problema:

- Se stai effettuando richieste come utente IAM, verifica di disporre delle autorizzazioni seguenti:
  - `ec2:RunInstances` con una risorsa jolly ("*")
  - `iam:PassRole` con la risorsa corrispondente all'ARN del ruolo (ad esempio, `arn:aws:iam::999999999999:role/ExampleRoleName`)
- Se non disponi delle autorizzazioni precedenti, modifica la policy IAM associata al ruolo o all'utente IAM per aggiungere le autorizzazioni richieste mancanti.

Se il problema persiste e continui a ricevere un errore di avvio non riuscito, puoi decodificare il messaggio di errore di autorizzazione incluso nell'errore. Il messaggio decodificato include le autorizzazioni che mancano nella policy IAM. Per ulteriori informazioni, consulta Come faccio a decodificare un messaggio di errore di autorizzazione dopo aver ricevuto un errore "UnauthorizedOperation" durante l'avvio di un'istanza EC2?

Utilizzo elevato della CPU poco dopo l'avvio di Windows (solo istanze Windows)

> **Note**
>
> Questo suggerimento per la risoluzione dei problemi riguarda solo le istanze di Windows.

Se Windows Update viene impostato su Check for updates but let me choose whether to download and install them (Ricerca aggiornamenti ma permettimi di scegliere se scaricarli e installarli) (impostazione predefinita dell'istanza), questo controllo può richiedere l'utilizzo di una percentuale compresa tra il 50 e il 99% della CPU nell'istanza. Se questo utilizzo della CPU implica problemi per le applicazioni, puoi modificare manualmente le impostazioni di Windows Update in Control Panel (Pannello di controllo) o utilizzare lo script seguente nel campo dei dati dell'utente di Amazon EC2:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v
 AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Quando esegui questo script, specifica un valore per /d. Il valore predefinito è 3. I valori possibili sono:

1. Non ricercare mai aggiornamenti
2. Ricerca aggiornamenti ma permettimi di scegliere se scaricarli e installarli
3. Scarica aggiornamenti ma permettimi di scegliere se installarli
4. Installa gli aggiornamenti automaticamente

Dopo avere modificato i dati utente, puoi eseguire l'istanza. Per ulteriori informazioni, consulta Eseguire i comandi sull'istanza di Windows all'avvio.

Risolvi i problemi di connessione alla tua istanza Linux

Le informazioni e gli errori comuni seguenti possono essere utili per risolvere i problemi di connessione all'istanza Linux.

Problemi di connessione

- Cause comuni dei problemi di connessione
- Errore di connessione all'istanza: Connection timed out
- Errore: impossibile caricare la chiave... Valore previsto: QUALSIASI CHIAVE PRIVATA
- Errore: User key not recognized by server
- Errore: autorizzazione negata o connessione chiusa dalla porta 22 [istanza]
- Errore: Unprotected Private Key File (File della chiave privata non protetto)
- Errore: la chiave privata deve iniziare con "-----BEGIN RSA PRIVATE KEY-----" e finire con "-----END RSA PRIVATE KEY-----"

- Errore: Server refused our key o No supported authentication methods available
- Cannot Ping Instance (Impossibile eseguire il ping dell'istanza)
- Errore: il server ha chiuso inaspettatamente la connessione di rete
- Errore: convalida della chiave host non riuscita per EC2 Instance Connect
- Impossibile connettersi all'istanza Ubuntu tramite EC2 Instance Connect
- Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Linux?

Cause comuni dei problemi di connessione

Ti consigliamo di iniziare a risolvere i problemi di connessione delle istanze verificando di aver eseguito con precisione le seguenti attività.

Verifica il nome utente per l'istanza

È possibile connettersi all'istanza utilizzando il nome utente dell'account utente o il nome utente predefinito per l'AMI utilizzato per avviare l'istanza.

- Ottenere il nome utente per il proprio account utente.

  Per ulteriori informazioni su come creare un account utente, consulta Gestisci gli utenti di sistema sulla tua istanza Linux.
- Ottieni il nome utente predefinito per l'AMI che hai utilizzato per avviare l'istanza:

AMI utilizzata per avviare l'istanza	Nome utente predefinito
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
RHEL	`ec2-user` o `root`

AMI utilizzata per avviare l'istanza	Nome utente predefinito
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Altro	Verifica con il provider dell'AMI

Verificare che le regole del gruppo di sicurezza consentano il traffico

Verificare che il gruppo di sicurezza associato alla tua istanza consenta il traffico SSH in entrata dal tuo indirizzo IP. Per impostazione predefinita, il gruppo di sicurezza predefinito per il VPC non consente il traffico SSH in entrata. Per impostazione predefinita, il gruppo di sicurezza creato dalla procedura guidata di avvio abilita il traffico SSH. Per i passaggi per aggiungere una regola per il traffico SSH in entrata alla tua istanza Linux, consulta Regole per la connessione alle istanze dal computer in uso. Per le fasi di verifica, consulta Errore di connessione all'istanza: Connection timed out.

Verificare che l'istanza sia pronta

Dopo aver avviato un'istanza, possono essere necessari alcuni minuti affinché sia pronta e sia possibile connettervisi. Controllare l'istanza per assicurarsi che sia in esecuzione e che abbia superato i controlli di stato.

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza desiderata.
3. Verificare quanto segue:
   a. Nella colonna Instance state (Stato istanza), verificare che l'istanza sia nello stato `running`.
   b. Nella colonna Status check (Controllo stato), verificare che l'istanza abbia superato i due controlli di stato.

Verifica che siano soddisfatto tutti i prerequisiti per connetterti

Assicurati di avere tutte le informazioni necessarie per connetterti. Per ulteriori informazioni, consulta Connessione all'istanza di Linux.

Per i prerequisiti specifici per i tipi di connessione, come SSH, EC2 Instance Connect, OpenSSH, PuTTY e altri, consulta le seguenti opzioni.

Linux o MacOS X

Se il sistema operativo del computer locale è Linux o macOS X, consulta i prerequisiti specifici per le seguenti opzioni di connessione:

- Client SSH
- EC2 Instance Connect
- AWS Systems Manager Gestore delle sessioni

Windows

Se il sistema operativo del computer locale è Microsoft, consulta i prerequisiti specifici per le seguenti opzioni di connessione:

- OpenSSH
- PuTTY
- AWS Systems Manager Gestore di sessione
- Sottosistema Windows per Linux

Errore di connessione all'istanza: Connection timed out

Se si tenta di connettersi all'istanza e si riceve il messaggio di errore `Network error: Connection timed out` o `Error connecting to [instance], reason: -> Connection timed out: connect`, provare a procedere come segue:

Verificare le regole del gruppo di sicurezza.

È necessaria una regola del gruppo di sicurezza che consenta il traffico in entrata dall'indirizzo IPv4 pubblico del computer locale sulla porta corretta.

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza desiderata.

3. Nella scheda Security (Sicurezza) nella parte inferiore della pagina della console, in Inbound rules (Regole in entrata) controllare l'elenco delle regole in vigore per l'istanza selezionata.

   - Per le istanze Linux: verifica che sia presente una regola che consente il traffico dal computer locale alla porta 22 (SSH).
   - Per le istanze Windows: verifica che sia presente una regola che consente il traffico dal computer locale alla porta 3389 (RDP).

   Se il gruppo di sicurezza non dispone di una regola che consente il traffico in entrata dal computer locale, aggiungi una regola al gruppo di sicurezza. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.
4. Per la regola che consente il traffico in entrata, controlla il campo Source (Origine). Se il valore è un singolo indirizzo IP e se l'indirizzo IP non è statico, verrà assegnato un nuovo indirizzo IP ogni volta che si riavvia il computer. Ciò farà sì che la regola non includa il traffico di indirizzi IP del tuo computer. L'indirizzo IP potrebbe non essere statico se il computer si trova su una rete aziendale o se si sta effettuando la connessione tramite un fornitore di servizi Internet (ISP) o l'indirizzo IP del computer è dinamico e cambia ogni volta che si riavvia il computer. Per essere certi che la regola del gruppo di sicurezza consenta il traffico in entrata dal computer locale, anziché specificare un singolo indirizzo IP per il campo Source (Origine) specifica l'intervallo di indirizzi IP utilizzati dai computer client.

   Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta Regole sui gruppi di sicurezza nella Guida per l'utente di Amazon VPC.

Verificare la tabella di routing per la sottorete.

È necessario adottare un instradamento che invii tutto il traffico destinato al di fuori del VPC all'Internet gateway per il VPC.

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza desiderata.
3. Nella scheda Networking (Rete), prendere nota dei valori per VPC ID e subnet (sottorete).
4. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
5. Nel riquadro di navigazione, scegliere Internet Gateways. Verificare che al VPC sia associato un Internet gateway. In caso contrario, scegliere Create internet gateway (Crea gateway Internet), immettere un nome per il gateway Internet e scegliere Create internet gateway (Crea gateway

Internet). Quindi, per il gateway Internet creato, scegliere Actions (Operazioni), Attach to VPC (Collega a VPC), selezionare il VPC e quindi scegliere Attach internet gateway (Collega gateway Internet) per collegarlo al VPC.

6. Nel riquadro di navigazione scegliere Subnets (Sottoreti) e selezionare la sottorete desiderata.
7. Nella scheda Route table (Tabella di routing), verificare che sia presente un instradamento con `0.0.0.0/0` come destinazione e il gateway Internet del VPC come target. Se si sta effettuando la connessione all'istanza utilizzando il relativo indirizzo IPv6, verificare che sia disponibile un instradamento per tutto il traffico IPv6 (`::/0`) che punti all'Internet gateway. In caso contrario, eseguire le seguenti operazioni:

   a. Selezionare l'ID per la tabella di routing (rtb-xxxxxxxx) per navigare alla tabella di routing.
   b. Nella scheda Routes (Route), scegliere Edit routes (Modifica route). Selezionare Add route (Aggiungi route), utilizzare `0.0.0.0/0` come destinazione e il gateway internet come target. Per IPv6, selezionare Add route (Aggiungi route), utilizzare `::/0` come destinazione e il gateway internet come target.
   c. Selezionare Save routes (Salva route).

Verificare la lista di controllo accessi (ACL) di rete della sottorete.

Le ACL di rete devono consentire il traffico in entrata dall'indirizzo IP locale sulla porta 22 (per le istanze Linux) o sulla porta 3389 (per le istanze Windows). Deve inoltre consentire il traffico in uscita alle porte effimere (1024-65535).

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Seleziona la sottorete.
4. Nella scheda Lista di controllo accessi di rete, per Regole in entrata verifica che le regole permettano il traffico in entrata dal computer in uso sulla porta richiesta. Altrimenti, elimina o modifica la regola che blocca il traffico.
5. Per Regole in uscita, verifica che le regole permettano il traffico verso computer in uso sulle porte effimere. Altrimenti, elimina o modifica la regola che blocca il traffico.

Se il computer si trova su una rete aziendale

Chiedere all'amministratore di rete se il firewall interno permette il traffico in entrata e in uscita dal computer in uso sulla porta 22 (per le istanze Linux) o sulla porta 3389 (per le istanze Windows).

Se sul computer è presente un firewall, verificare che consenta il traffico in entrata e in uscita dal computer in uso sulla porta 22 (per le istanze Linux) o sulla porta 3389 (per le istanze Windows).

Controllare che l'istanza abbia un indirizzo IPv4 pubblico.

Se non lo ha, è possibile associare un indirizzo IP Elastic all'istanza. Per ulteriori informazioni, consulta Indirizzi IP elastici.

Verificare il carico della CPU sull'istanza; è possibile che il server sia in sovraccarico.

AWS fornisce automaticamente dati come i CloudWatch parametri di Amazon e lo stato dell'istanza, che puoi utilizzare per vedere il carico della CPU sull'istanza e, se necessario, modificare il modo in cui vengono gestiti i carichi. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.

- Se il carico è variabile, è possibile aumentare o diminuire automaticamente le istanze utilizzando Auto Scaling ed Elastic Load Balancing.
- Se il carico è in crescita stabile, è possibile passare a un tipo di istanza più grande. Per ulteriori informazioni, consulta Cambiare il tipo di istanza.

Per connettersi all'istanza utilizzando un indirizzo IPv6, verificare quanto riportato di seguito:

- La sottorete deve essere associata a una tabella di routing che prevede un instradamento per il traffico IPv6 (`::/0`) a un Internet gateway.
- Le regole del gruppo di sicurezza devono permettere il traffico in entrata dall'indirizzo IPv6 locale sulla porta corretta (22 per Linux e 3389 per Windows).
- Le regole dell'ACL di rete devono permettere il traffico IPv6 in entrata e in uscita.
- Se l'istanza è stata avviata da un'AMI meno recente, potrebbe non essere configurata per DHCPv6 (gli indirizzi IPv6 non vengono riconosciuti automaticamente sull'interfaccia di rete). Per ulteriori informazioni, consulta Configurazione di IPv6 sulle istanze nella Guida per l'utente di Amazon VPC.
- Il tuo computer locale deve avere un indirizzo IPv6 ed essere configurato per utilizzare IPv6.

Errore: impossibile caricare la chiave... Valore previsto: QUALSIASI CHIAVE PRIVATA

Se tenti di connetterti all'istanza e ricevi il messaggio di errore, `unable to load key ... Expecting: ANY PRIVATE KEY`, il file in cui è archiviata la chiave privata non è configurato

correttamente. Se il file della chiave privata termina con `.pem`, potrebbe comunque essere configurato in modo errato. Una possibile causa di una configurazione errata di un file della chiave privata è la mancanza di un certificato.

Se il file della chiave privata non è configurato correttamente, segui questi passaggi per risolvere l'errore

1. Creazione di una nuova coppia di chiavi. Per ulteriori informazioni, consulta Creazione di una coppia di chiavi utilizzando Amazon EC2.

   > **Note**
   >
   > In alternativa, è possibile creare una nuova coppia di chiavi tramite uno strumento di terze parti. Per ulteriori informazioni, consulta Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2.

2. Aggiungi la nuova coppia di chiavi all'istanza. Per ulteriori informazioni, consulta Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Linux?.
3. Connettiti all'istanza utilizzando la nuova coppia di chiavi.

Errore: User key not recognized by server

Se per connettersi all'istanza si utilizza SSH

- Utilizzare `ssh -vvv` per recuperare le informazioni sul debug triple verbose durante la connessione:

  ```
  ssh -vvv -i path/key-pair-name.pem instance-user-
  name@ec2-203-0-113-25.compute-1.amazonaws.com
  ```

  Il seguente output di esempio mostra quanto visualizzato se si è tentato di connettersi all'istanza con una chiave che non è stata riconosciuta dal server:

  ```
  open/ANT/myusername/.ssh/known_hosts).
  debug2: bits set: 504/1024
  debug1: ssh_rsa_verify: signature correct
  debug2: kex_derive_keys
  debug2: set_newkeys: mode 1
  debug1: SSH2_MSG_NEWKEYS sent
  ```

```
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Se per connettersi all'istanza si utilizza PuTTY

- Verificare che il file della chiave privata (.pem) sia stato convertito nel formato riconosciuto da PuTTY (.ppk). Per ulteriori informazioni sulla conversione della chiave privata, consultare Connessione all'istanza Linux da Windows tramite PuTTY.

  > **Note**
  >
  > In PuTTYgen caricare il file della chiave privata e selezionare Save Private Key (Salva chiave privata) anziché Generate (Genera).

- Accertarsi di connettersi con il nome utente corretto dell'AMI in uso. Immettere il nome utente nella casella Nome host nella finestra Configurazione PuTTY.

AMI utilizzata per avviare l'istanza	Nome utente predefinito
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Altro	Verifica con il provider dell'AMI

- Accertarsi di disporre di una regola del gruppo di sicurezza che permetta il traffico in entrata verso la porta corretta. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.

Errore: autorizzazione negata o connessione chiusa dalla porta 22 [istanza]

Se esegui la connessione all'istanza usando SSH e ricevi uno degli errori seguenti, `Host key not found in [directory]`, `Permission denied (publickey)`, `Authentication failed, permission denied` o `Connection closed by [instance] port 22`, assicurati di connetterti con il nome utente corretto dell'AMI e di avere specificato il file della chiave privata corretto (`.pem`) per l'istanza in uso.

I nomi utente appropriati sono i seguenti:

AMI utilizzata per avviare l'istanza	Nome utente predefinito
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Altro	Verifica con il provider dell'AMI

Ad esempio, per utilizzare un client SSH per connettersi a un'istanza Amazon Linux, utilizzare il seguente comando:

```
ssh -i /path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Controllare di utilizzare il file della chiave privata corrispondente alla coppia di chiavi selezionata all'avvio dell'istanza.

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, scegliere Instances (Istanze) e selezionare l'istanza desiderata.
3. Nella scheda Details (Dettagli), in Instance details (Dettagli istanza), verificare il valore Key pair name (Nome della coppia di chiavi).
4. Se all'avvio dell'istanza non è stata specificata una coppia di chiavi, è possibile terminare l'istanza e avviarne una nuova, accertandosi di specificare una coppia di chiavi. Se si tratta di un'istanza già utilizzata ma non si dispone più del file `.pem`, è possibile sostituire la coppia di chiavi con una nuova. Per ulteriori informazioni, consulta Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Linux?.

Se è stata generata una coppia di chiavi, accertarsi che il relativo generatore sia configurato per la creazione delle chiavi RSA. Le chiavi DSA non sono accettate.

Se si riceve un errore `Permission denied (publickey)` e nessuna delle condizioni sopra indicate è applicabile (ad esempio, è stato possibile connettersi in precedenza), è possibile che siano state modificate le autorizzazioni della home directory. Le autorizzazioni per `/home/`*`instance-user-name`*`/.ssh/authorized_keys` devono essere limitate esclusivamente al proprietario.

Per verificare le autorizzazioni dell'istanza

1. Arrestare l'istanza e distaccare il volume radice. Per ulteriori informazioni, consulta Arresta e avvia le istanze Amazon EC2.
2. Avviare un'istanza temporanea nella stessa zona di disponibilità dell'istanza corrente (utilizzare la medesima AMI utilizzata per l'istanza corrente o una simile), quindi collegare il volume radice all'istanza temporanea.
3. Connettersi all'istanza temporanea, creare un punto di montaggio e montare il volume che è stato collegato.
4. Dall'istanza temporanea, controllare le autorizzazioni della directory /home/*instance-user-name*/ del volume collegato. Se necessario, adeguare le autorizzazioni nel modo seguente:

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. Smontare il volume, distaccarlo dall'istanza temporanea e ricollegarlo all'istanza originale. Accertarsi di specificare il nome di dispositivo corretto per il volume radice, ad esempi, `/dev/xvda`.
6. Avviare l'istanza. Se l'istanza temporanea non è più necessaria, è possibile terminarla.

Errore: Unprotected Private Key File (File della chiave privata non protetto)

Il file della chiave privata deve essere protetto dalle operazioni di lettura e scrittura eseguite dagli altri utenti. Se la chiave privata può essere letta o scritta da altri utenti, SSH ignora la chiave in uso e viene visualizzato il seguente messaggio di avviso.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Se viene visualizzato un messaggio simile quando si tenta di accedere all'istanza, esaminare la prima riga del messaggio di errore per verificare se si sta utilizzando la chiave pubblica corretta per l'istanza. L'esempio sopra utilizza la chiave privata `.ssh/my_private_key.pem` con le autorizzazioni di file `0777`, che consentono a chiunque di leggere o scrivere in questo file. Trattandosi di un livello di autorizzazione estremamente non sicuro, SSH ignora questa chiave.

Se ti connetti da MacOS o Linux, per risolvere l'errore esegui il seguente comando, sostituendo il percorso del file con quello della chiave privata.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Se ci si connette da Windows, attenersi alla seguente procedura sul computer locale.

1. Individuare il file .pem.
2. Fare clic con il pulsante destro del mouse sul file .pem e selezionare Properties (Proprietà).
3. Scegliere la scheda Sicurezza.
4. Selezionare Advanced (Avanzate).

5. Verificare di essere il proprietario del file. In caso contrario, cambiare il proprietario con il proprio nome utente.
6. Selezionare Disable inheritance (Disabilita l'ereditarietà) e Remove all inherited permissions from this object (Rimuovi tutte le autorizzazioni ereditate da questo oggetto).
7. Selezionare Add (Aggiungi), Select a principal (Seleziona un'entità principale), inserire il proprio nome utente e selezionare OK.
8. Dalla finestra Permission Entry (Voce di autorizzazione), concedere le autorizzazioni Read (Lettura) e selezionare OK.
9. Fai clic su Apply (Applica) per assicurarti che tutte le impostazioni vengano salvate.
10. Selezionare OK per chiudere la finestra Advanced Security Settings (Impostazioni di sicurezza avanzate).
11. Selezionare OK per chiudere la finestra Properties (Proprietà).
12. Dovrebbe essere possibile stabilire una connessione a un'istanza Linux da Windows tramite SSH.

Da una finestra del prompt dei comandi Windows, esegui il comando seguente:

1. Dal prompt dei comandi, passare al percorso del file .pem.
2. Eseguire il seguente comando per reimpostare e rimuovere le autorizzazioni esplicite:

```
icacls.exe $path /reset
```

3. Eseguire il seguente comando per concedere le autorizzazioni di lettura all'utente attuale:

```
icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
```

4. Eseguire il seguente comando per disabilitare l'ereditarietà e rimuovere le autorizzazioni ereditate.

```
icacls.exe $path /inheritance:r
```

5. Dovrebbe essere possibile stabilire una connessione a un'istanza Linux da Windows tramite SSH.

Errore: la chiave privata deve iniziare con "-----BEGIN RSA PRIVATE KEY-----" e finire con "-----END RSA PRIVATE KEY-----"

Se utilizzi uno strumento di terze parti, ad esempio ssh-keygen, per creare una coppia di chiavi RSA, genera la chiave privata nel formato chiave OpenSSH. Quando esegui la connessione all'istanza, se utilizzi la chiave privata nel formato OpenSSH per decrittografare la password, riceverai l'errore `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`.

Per risolvere l'errore, la chiave privata deve essere nel formato PEM. Utilizza il seguente comando per creare la chiave privata nel formato PEM:

```
ssh-keygen -m PEM
```

Errore: Server refused our key o No supported authentication methods available

Se si effettua la connessione all'istanza utilizzando PuTTY e si ricevono gli errori, Error: Server refused our key (Errore: Il server ha rifiutato la chiave) o Error: No supported authentication methods available (Errore: Nessun metodo di autenticazione supportato disponibile), accertarsi di connettersi con il nome utente corretto dell'AMI. Digitare il nome utente in User name (Nome utente) nella finestra PuTTY Configuration (Configurazione PuTTY).

I nomi utente appropriati sono i seguenti:

AMI utilizzata per avviare l'istanza	Nome utente predefinito
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`

AMI utilizzata per avviare l'istanza	Nome utente predefinito
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Altro	Verifica con il provider dell'AMI

Devi anche verificare che:

- Stai usando la versione più recente di PuTTY. Per ulteriori informazioni, consulta la pagina Web di PuTTY.
- Il file della chiave privata (.pem) deve essere stato convertito nel formato riconosciuto da PuTTY (.ppk). Per ulteriori informazioni sulla conversione della chiave privata, consultare Connessione all'istanza Linux da Windows tramite PuTTY.

Cannot Ping Instance (Impossibile eseguire il ping dell'istanza)

Il comando `ping` è un tipo di traffico ICMP; se non è possibile effettuare il ping dell'istanza, accertarsi che le regole del gruppo di sicurezza relative al traffico in entrata permettano il traffico ICMP per il messaggio `Echo Request` da tutte le origini oppure dal computer o dall'istanza da cui si sta eseguendo il comando.

Se non è possibile eseguire un comando `ping` dall'istanza, accertarsi che le regole del gruppo di sicurezza relative al traffico in uscita permettano il traffico ICMP per il messaggio `Echo Request` verso tutte le destinazioni oppure verso l'host per il quale si sta tentando di effettuare il ping.

I comandi `Ping` possono anche essere bloccati da un firewall o timeout a causa di latenza di rete o problemi hardware. Per ulteriori informazioni sulla risoluzione dei problemi, consultare l'amministratore di rete locale o di sistema.

Errore: il server ha chiuso inaspettatamente la connessione di rete

Se ci si connette all'istanza con PuTTY e si riceve l'errore "Connessione di rete in attesa del server", verificare di aver abilitato i segnali keepalive nella pagina Connessione della configurazione PuTTY per evitare di essere disconnessi. Alcuni server disconnettono i client quando non ricevono dati entro un periodo di tempo specificato. Impostare i Secondi tra i segnali keepalive a 59 secondi.

Se i problemi persistono dopo l'abilitazione dei segnali keepalive, provare a disabilitare l'algoritmo di Nagle nella pagina Connessione della configurazione PuTTY.

Errore: convalida della chiave host non riuscita per EC2 Instance Connect

Se ruoti le chiavi host dell'istanza, le nuove chiavi host non vengono caricate automaticamente nel database delle chiavi host AWS affidabili. Ciò fa sì che la convalida della chiave host fallisca quando si tenta di connettersi all'istanza utilizzando il client EC2 Instance Connect basato su browser e non si è in grado di connettersi all'istanza.

Per risolvere l'errore, è necessario eseguire lo script `eic_harvest_hostkeys` sull'istanza, che carica la nuova chiave host in EC2 Instance Connect. Lo script si trova in `/opt/aws/bin/` nelle istanze Amazon Linux 2 e in `/usr/share/ec2-instance-connect/` nelle istanze Ubuntu.

Amazon Linux 2

Per risolvere l'errore di convalida della chiave host non riuscita su un'istanza Amazon Linux 2

1. Connettersi all'istanza tramite SSH.

   È possibile connettersi utilizzando la CLI EC2 Instance Connect oppure tramite la coppia di chiavi SSH assegnata all'istanza al momento dell'avvio e il nome utente predefinito dell'AMI utilizzata per avviare l'istanza. Per Amazon Linux 2, il nome utente predefinito è `ec2-user`.

   Ad esempio, se l'istanza è stata avviata tramite Amazon Linux 2, il suo nome DNS pubblico è `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e la coppia di chiavi è `my_ec2_private_key.pem`, utilizzare il comando seguente per accedere all'istanza tramite SSH:

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH..

2. Accedere alla cartella:

```
[ec2-user ~]$ cd /opt/aws/bin/
```

3. Eseguire il seguente comando sull'istanza.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Si noti che una chiamata riuscita non produce alcun risultato.

È ora possibile utilizzare il client EC2 Instance Connect basato su browser per connettersi all'istanza.

Ubuntu

Per risolvere l'errore di convalida della chiave host non riuscito su un'istanza Ubuntu

1. Connettersi all'istanza tramite SSH.

   È possibile connettersi utilizzando la CLI EC2 Instance Connect oppure tramite la coppia di chiavi SSH assegnata all'istanza al momento dell'avvio e il nome utente predefinito dell'AMI utilizzata per avviare l'istanza. Per Ubuntu, il nome utente predefinito è `ubuntu`.

   Ad esempio, se l'istanza è stata avviata tramite Ubuntu, il suo nome DNS pubblico è `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e la coppia di chiavi è `my_ec2_private_key.pem`, utilizzare il comando seguente per accedere all'istanza tramite SSH:

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti alla tua istanza Linux da Linux o macOS utilizzando SSH..

2. Accedere alla cartella:

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Eseguire il seguente comando sull'istanza.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Si noti che una chiamata riuscita non produce alcun risultato.

È ora possibile utilizzare il client EC2 Instance Connect basato su browser per connettersi all'istanza.

Impossibile connettersi all'istanza Ubuntu tramite EC2 Instance Connect

Se utilizzi EC2 Instance Connect per connetterti all'istanza Ubuntu e visualizzi un errore durante il tentativo di connessione, puoi utilizzare le seguenti informazioni per provare a risolvere il problema.

Possibile causa

Il pacchetto `ec2-instance-connect` sull'istanza non è la versione più recente.

Soluzione

Aggiorna il pacchetto `ec2-instance-connect` sull'istanza alla versione più recente, come segue:

1. Collegati all'istanza utilizzando un metodo diverso da EC2 Instance Connect.
2. Esegui il comando seguente sull'istanza per aggiornare alla versione più recente il pacchetto `ec2-instance-connect`.

```
apt update && apt upgrade
```

Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Linux?

Se si perde la chiave privata per un'istanza supportata da EBS, è possibile riottenere l'accesso all'istanza. Arrestare l'istanza, distaccarne il volume root e collegarlo a un'altra istanza come volume dati, modificare il file `authorized_keys` con una nuova chiave pubblica, riportare il volume

all'istanza originale e riavviare l'istanza. Per ulteriori informazioni sull'avvio, la connessione e l'arresto delle istanze, consulta Ciclo di vita dell'istanza.

Questa procedura è supportata solo per le istanze con volumi root EBS. Se il dispositivo principale è un volume dell'instance store, non è possibile utilizzare questa procedura per riconquistare l'accesso all'istanza; è necessario disporre della chiave privata per connettersi all'istanza. Per determinare il tipo di dispositivo root dell'istanza, apri la console Amazon EC2, scegli Istanze, seleziona l'istanza, scegli la scheda Archiviazione e nella sezione Dettagli del dispositivo root controlla il valore Tipo di dispositivo root.

Il valore è `EBS` o `INSTANCE-STORE`.

In aggiunta ai passaggi seguenti, esistono altri modi per connettersi all'istanza Linux in caso di perdita della chiave privata. Per ulteriori informazioni, consulta Come posso connettermi alla mia istanza Amazon EC2 se ho perso la mia coppia di chiavi SSH dopo il suo avvio iniziale?

Per connettersi a un'istanza supportata da EBS con una coppia di chiavi diversa

- Fase 1: creazione di una nuova coppia di chiavi
- Fase 2: Ottenere informazioni sull'istanza originale e il relativo volume radice
- Fase 3: Arrestare l'istanza originale
- Fase 4: Avviare un'istanza temporanea
- Fase 5: scollegare il volume radice dall'istanza originale e collegarlo all'istanza temporanea
- Fase 6: aggiungere la nuova chiave pubblica a authorized_keys sul volume originale montato sull'istanza temporanea
- Fase 7: smontare e scollegare il volume originale dall'istanza temporanea e ricollegarlo all'istanza originale
- Fase 8: connettersi all'istanza originale utilizzando la nuova coppia di chiavi
- Fase 9: pulizia

Fase 1: creazione di una nuova coppia di chiavi

Creare una nuova coppia di chiavi tramite la console Amazon EC2 o uno strumento di terza parte. Se si vuole assegnare alla nuova coppia di chiavi lo stesso nome della chiave privata persa, bisogna prima eliminare la coppia di chiavi esistente. Per informazioni su come creare una coppia di chiavi, consulta Creazione di una coppia di chiavi utilizzando Amazon EC2 o Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2.

Fase 2: Ottenere informazioni sull'istanza originale e il relativo volume radice

Prendere nota delle seguenti informazioni perché sono necessarie per completare questa procedura.

Per ottenere informazioni sull'istanza originale

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza a cui ci si vuole connettere. (Ci si riferirà a questa come istanza originale).
3. Nella scheda Details (Dettagli), prendere nota dell'ID istanza e dell'ID AMI.
4. Nella scheda Networking (Reti), prendere nota della zona di disponibilità.
5. Nella scheda Storage (Archiviazione), sotto Root device name (Nome dispositivo root) annotare il nome del dispositivo per il volume root (ad esempio `/dev/xvda`). Quindi, trova il nome di questo dispositivo in Block devices (Dispositivi a blocchi) e annota l'ID volume (ad esempio, vol-0a1234b5678c910de).

Fase 3: Arrestare l'istanza originale

Scegli Instance state (Stato istanza), Stop instance (Arresta istanza). Se questa opzione è disabilitata, l'istanza è già arrestata o il suo dispositivo root è un volume di instance store.

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

Fase 4: Avviare un'istanza temporanea

New console

Per avviare un'istanza temporanea

1. Nel riquadro di navigazione, selezionare Instances (Istanze), quindi selezionare Launch Instance (Avvia istanza).
2. Nella sezione Name and tags (Nome e tag), per Name (Nome) inserisci Temporary.

3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona la stessa AMI utilizzata per avviare l'istanza originale. Se questa AMI non è disponibile, è possibile creare un'AMI che può essere utilizzata dall'istanza arrestata. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.
4. Nella sezione Instance type (Tipo di istanza), mantieni il tipo di istanza di default.
5. Nella sezione Key pair (Coppia di chiavi), per Key pair name (Nome della coppia di chiavi) seleziona una coppia di chiavi esistente o creane una nuova.
6. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica), quindi per Subnet (Sottorete) seleziona una sottorete nella stessa zona di disponibilità dell'istanza originale.
7. Nel pannello Summary (Riepilogo), scegli Launch (Avvia).

Old console

Scegliere Launch instances (Avvia istanze), quindi utilizzare la procedura guidata di avvio per avviare un'istanza temporanea con le seguenti opzioni:

- Nella pagina Choose an AMI (Scegli un'AMI), selezionare la stessa AMI utilizzata per avviare l'istanza originale. Se questa AMI non è disponibile, è possibile creare un'AMI che può essere utilizzata dall'istanza arrestata. Per ulteriori informazioni, consulta Crea un'AMI supportata da Amazon EBS.
- Nella pagina Choose an Instance Type (Scegli un tipo di istanza), lasciare il tipo di istanza predefinita selezionata dalla procedura guidata.
- Nella pagina Configure Instance Details (Configura dettagli istanza) specificare la stessa zona di disponibilità dell'istanza originale. Se si sta avviando un'istanza in un VPC, selezionare una sottorete in questa zona di disponibilità.
- Nella pagina Add Tags (Aggiungi tag), aggiungere il tag `Name=Temporary` all'istanza per indicare che si tratta di un'istanza temporanea.
- Nella pagina Revisione, selezionare Launch (Avvia). Seleziona la coppia di chiavi che hai creato nella Fase 1, quindi seleziona Launch Instances (Avvia istanze).

Fase 5: scollegare il volume radice dall'istanza originale e collegarlo all'istanza temporanea

1. Nel riquadro di navigazione, selezionare Volumes (Volumi), quindi selezionare il volume dispositivo root per l'istanza originale (l'ID del volume è stato annotato in una fase precedente).

Scegli Actions (Operazioni), Detach volume (Scollega volume), quindi scegli Detach (Scollega). Attendere che lo stato del volume diventi `available`. (Potrebbe essere necessario scegliere l'icona Refresh (Aggiorna)).

2. Con il volume ancora selezionato, scegli Actions (Operazioni), quindi scegli Attach volume (Collega volume). Seleziona l'ID istanza dell'istanza temporanea, prendi nota del nome del dispositivo specificato sotto Device name (Nome del dispositivo), ad esempio `/dev/sdf`, quindi scegli Attach volume (Collega volume).

> **Note**
>
> Se hai avviato l'istanza originale da un' Marketplace AWS AMI e il volume contiene Marketplace AWS codici, devi prima interrompere l'istanza temporanea prima di poter collegare il volume.

Fase 6: aggiungere la nuova chiave pubblica a **`authorized_keys`** sul volume originale montato sull'istanza temporanea

1. Connettersi all'istanza temporanea.
2. Dall'istanza temporanea, montare il volume collegato all'istanza in modo da poter accedere al file system. Ad esempio, se il nome del dispositivo è `/dev/sdf`, utilizzare i seguenti comandi per montare il volume come `/mnt/tempvol`.

> **Note**
>
> Il nome del dispositivo potrebbe apparire in modo diverso nell'istanza. Ad esempio, i dispositivi montati come `/dev/sdf` potrebbero essere visualizzati come `/dev/xvdf` nell'istanza. Alcune versioni di Red Hat (o le relative varianti, come CentOS), potrebbero anche aggiungere alla lettera finale 4 caratteri, in modo che `/dev/sdf` diventi `/dev/xvdk`.

   a. Utilizzare il comando lsblk per determinare se il volume è partizionato.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
```

```
##xvda1 202:1    0    8G  0 part /
xvdf    202:80   0  101G  0 disk
##xvdf1 202:81   0  101G  0 part
xvdg    202:96   0   30G  0 disk
```

Nell'esempio precedente, `/dev/xvda` e `/dev/xvdf` sono volumi partizionati, mentre `/dev/xvdg` non lo è. Se il volume è partizionato, montare la partizione (`/dev/xvdf1`) invece del dispositivo raw (`/dev/xvdf`) nelle fasi successive.

b. Creare una directory temporanea per montare il volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Montare il volume (o la partizione) nel punto di montaggio temporaneo, utilizzando il nome del volume o del dispositivo identificato in precedenza. Il comando necessario dipende dal file system del sistema operativo. Nota: il nome del dispositivo potrebbe apparire in modo diverso nell'istanza. Per ulteriori informazioni, consulta la sezione note nel passaggio 6.

- Amazon Linux, Ubuntu e Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 e RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Se si riceve un errore che indica che il file system è corrotto, eseguire il seguente comando per utilizzare l'utilità fsck per controllare il file system e risolvere qualsiasi guasto:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Dall'istanza temporanea, utilizzare il seguente comando per aggiornare `authorized_keys` nel volume montato con la nuova chiave pubblica da `authorized_keys` per l'istanza temporanea.

> **Important**
>
> Gli esempi seguenti utilizzano il nome utente di Amazon Linux `ec2-user`. Potrebbe essere necessario sostituire un nome utente diverso, ad esempio `ubuntu` per le istanze di Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Se la copia ha avuto successo, è possibile passare alla fase successiva.

(Facoltativo) Altrimenti, se non si ha il permesso di modificare i file in `/mnt/tempvol`, sarà necessario aggiornare il file utilizzando sudo, quindi occorrerà controllare le autorizzazioni sul file per verificare di poter accedere all'istanza originale. Utilizzare il comando seguente per verificare le autorizzazioni per il file:

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

In questo esempio di output, *222* è l'ID utente e *500* è l'ID di gruppo. Quindi, utilizzare sudo per eseguire nuovamente il comando di copia non riuscito.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Eseguire nuovamente il comando seguente per stabilire se le autorizzazioni sono state modificate.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Se l'ID utente e l'ID gruppo sono stati modificati, utilizzare il seguente comando per ripristinarli.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Fase 7: smontare e scollegare il volume originale dall'istanza temporanea e ricollegarlo all'istanza originale

1. Dall'istanza temporanea, smontare il volume collegato all'istanza in modo da ricollegarlo all'istanza originale. Ad esempio, utilizzare il seguente comando per smontare il volume in `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Scollega il volume dall'istanza temporanea (è stato smontato nel passaggio precedente): dalla console Amazon EC2, scegli Volumes (Volumi) nel riquadro di navigazione, seleziona il volume del dispositivo root per l'istanza originale (l'ID del volume è stato annotato in un passaggio precedente), scegli Actions (Operazioni), Detach volume (Scollega volume), quindi scegli Detach (Scollega). Attendere che lo stato del volume diventi `available`. (Potrebbe essere necessario scegliere l'icona Refresh (Aggiorna)).
3. Ricollega il volume all'istanza originale: con il volume ancora selezionato, scegli Actions (Operazioni), Attach volume (Collega volume). Seleziona l'ID dell'istanza originale, specifica il nome del dispositivo annotato in precedenza nel Passaggio 2 per il collegamento del dispositivo root originale (`/dev/sda1` o `/dev/xvda`), quindi scegli Attach volume (Collega volume).

   > **Important**
   >
   > Se non si specifica lo stesso nome del dispositivo dell'allegato originale, non è possibile avviare l'istanza originale. Amazon EC2 prevede il volume del dispositivo di root su `sda1` o `/dev/xvda`.

Fase 8: connettersi all'istanza originale utilizzando la nuova coppia di chiavi

Seleziona l'istanza originale, scegli Instance state (Stato istanza), Start instance (Avvia istanza). Dopo che l'istanza acquisisce lo stato `running`, è possibile connettersi a essa tramite il file della chiave privata per la nuova coppia di chiavi.

> **Note**
>
> Se il nome della nuova coppia di chiavi e del corrispondente file di chiave privata è diverso dal nome della coppia di chiavi originale, assicurarsi di specificare il nome del nuovo file della chiave privata quando ci si connette all'istanza.

Fase 9: pulizia

(Facoltativo) È possibile terminare l'istanza temporanea se non la si utilizza più. Selezionare l'istanza temporanea e scegliere Instance state (Stato istanza), Terminate instance (Termina istanza).

Risoluzione dei problemi di connessione all'istanza Windows

Le seguenti informazioni e gli errori comuni possono aiutarti a risolvere i problemi di connessione all'istanza di Windows.

Problemi di connessione

- Il desktop remoto non può connettersi al computer remoto
- Errore durante l'uso del client macOS RDP
- RDP mostra una schermata nera invece del desktop
- Impossibile accedere da remoto a un'istanza con un utente che non è un amministratore
- Risoluzione dei problemi relativi a Remote Desktop utilizzando AWS Systems Manager
- Abilitazione di Desktop remoto in un'istanza EC2 con il Registro di sistema remoto
- Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Windows?

Il desktop remoto non può connettersi al computer remoto

Prova a eseguire le operazioni seguenti per risolvere i problemi relativi alla connessione all'istanza:

- Verificare di utilizzare il nome host DNS pubblico corretto. (Nella console Amazon EC2 selezionare l'istanza, quindi scegliere Public DNS (IPv4) (DNS pubblico (IPv4)) nel riquadro dei dettagli). Se l'istanza si trova in un VPC e non si visualizza un nome DNS pubblico, è necessario abilitare i nomi host DNS. Per ulteriori informazioni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC.

- Verificare che l'istanza abbia un indirizzo IPv4 pubblico. Se non lo ha, è possibile associare un indirizzo IP Elastic all'istanza. Per ulteriori informazioni, consulta Indirizzi IP elastici.
- Per connettersi all'istanza utilizzando un indirizzo IPv6, controllare che il computer locale abbia un indirizzo IPv6 e che sia configurato per utilizzare IPv6. Per ulteriori informazioni, consulta Configurazione di IPv6 sulle istanze nella Guida per l'utente di Amazon VPC.
- Verificare che il gruppo di sicurezza abbia una regola che consente l'accesso RDP.
- Se si copia la password ma si verifica l'errore `Your credentials did not work`, provare a digitarla manualmente quando richiesto. È possibile che manchi un carattere o che sia stato inserito uno spazio vuoto aggiuntivo durante la copia della password.
- Verificare che l'istanza abbia superato i controlli dello stato. Per ulteriori informazioni, consulta Verifiche dello stato delle istanze e the section called “Controlli di stato non riusciti su Linux”.
- Verificare che la tabella di routing per la sottorete abbia un percorso che instrada tutto il traffico destinato al di fuori del VPC al gateway Internet per il VPC. Per ulteriori informazioni, consulta Creazione di una tabella di routing personalizzata (gateway Internet) nella Guida per l'utente di Amazon VPC.
- Verificare che Windows Firewall, o un altro firewall, non stia bloccando il traffico RDP alla istanza. Si consiglia di disabilitare Windows Firewall e di controllare l'accesso all'istanza utilizzando le regole del gruppo di sicurezza. Puoi utilizzare AWSSupport-TroubleshootRDP per disable the Windows Firewall profiles using SSM Agent. Per disattivare Windows Firewall su un'istanza di Windows non configurata per AWS Systems ManagerAWSSupport-ExecuteEC2Rescue, utilizza o utilizza i seguenti passaggi manuali:

Procedura manuale

1. Arrestare l'istanza interessata e distaccarne il volume root.
2. Avviare un'istanza temporanea nella stessa zona di disponibilità dell'istanza interessata.

> **Warning**
>
> Se la tua istanza temporanea si basa sulla stessa AMI su cui si basa l'istanza originale, devi completare ulteriori operazioni o non sarai in grado di avviare l'istanza originale dopo aver ripristinato il volume radice a causa di una collisione di firme del disco. In alternativa, seleziona un'AMI diversa per l'istanza temporanea. Ad esempio, se

l'istanza originale utilizza l'AMI AWS Windows per Windows Server 2016, avvia l'istanza temporanea utilizzando l'AMI AWS Windows per Windows Server 2019.

3. Collegare il volume radice dall'istanza interessata all'istanza temporanea. Connettersi all'istanza temporanea, aprire l'utilità Disk Management (Gestione disco) e portare l'unità online.
4. Aprire Regedit e selezionare HKEY_LOCAL_MACHINE. Dal menu File scegliere Load Hive (Carica Hive). Selezionare l'unità, aprire il file `Windows\System32\config\SYSTEM` e specificare un nome della chiave quando richiesto (è possibile utilizzare qualsiasi nome).
5. Selezionare la chiave appena caricata e passare a `ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy`. Per ciascuna chiave con un nome dal formato xxxxProfile, selezionare la chiave e modificare `EnableFirewall` da 1 a 0. Selezionare nuovamente la chiave e, dal menu File, scegliere Unload Hive (Scarica Hive).
6. (Facoltativo) Se la tua istanza temporanea si basa sulla stessa AMI su cui si basa quella originale, devi completare ulteriori operazioni o non sarai in grado di avviare l'istanza originale dopo aver ripristinato il volume di root a causa di un conflitto di firme del disco.

   Warning

   Nella procedura seguente viene descritto come modificare il Registro di sistema di Windows utilizzando l'editor del Registro di sistema. Se non hai familiarità con il Registro di sistema di Windows o non sai come apportare modifiche in modo sicuro utilizzando l'editor del Registro di sistema, consulta Configura il Registro di sistema.

   a. Apri un prompt dei comandi, digita regedit.exe e premi Invio.
   b. In Registry Editor (Editor del Registro di sistema), scegli HKEY_LOCAL_MACHINE dal menu contestuale (tasto destro del mouse), quindi seleziona Find (Cerca).
   c. Digita Windows Boot Manager e quindi seleziona Find Next (Trova successivo).
   d. Scegli la chiave denominata `11000001`. Questa chiave è un pari livello della chiave trovata nella fase precedente.
   e. Nel riquadro a destra, seleziona `Element` e quindi Modify (Modifica) dal menu contestuale (tasto destro del mouse).
   f. Individua la firma del disco a quattro byte con offset 0x38 nei dati. Inverti i byte per creare la firma del disco e annotala. Ad esempio, la firma del disco rappresentata dai seguenti dati è `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. In una finestra del prompt dei comandi, esegui il comando seguente per avviare Microsoft DiskPart.

```
diskpart
```

h. Esegui il DiskPart comando seguente per selezionare il volume. (È possibile verificare che il numero del disco sia 1 utilizzando l'utilità Gestione del disco.)

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Esegui il DiskPart comando seguente per ottenere la firma del disco.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Se la firma del disco mostrata nel passaggio precedente non corrisponde alla firma del disco BCD che hai annotato in precedenza, usa il DiskPart comando seguente per modificare la firma del disco in modo che corrisponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

7. Tramite l'utilità Disk Management (Gestione disco), portare l'unità offline.

> **Note**
>
> L'unità è automaticamente non in linea se l'istanza temporanea esegue lo stesso sistema operativo dell'istanza interessata, quindi non sarà necessario disconnetterla manualmente.

8. Distaccare il volume dall'istanza temporanea. Se non si utilizza più l'istanza temporanea, è possibile terminarla.

9. Ripristinare il volume root dell'istanza interessata collegandolo come `/dev/sda1`.
10. Avviare l'istanza.

- Verifica che Network Level Authentication sia disabilitato per le istanze che non sono parte di un dominio Active Directory (utilizza AWSSupport-TroubleshootRDP per disable NLA).
- Verificate che il tipo di avvio di Remote Desktop Service (TermService) sia Automatico e che il servizio sia avviato (utilizzare AWSSupport-TroubleshootRDPperenable and start the RDP service).
- Assicurati di connetterti alla porta Remote Desktop Protocol corretta, che, per impostazione predefinita, è 3389 (utilizza AWSSupport-TroubleshootRDP per read the current RDP port e change it back to 3389).
- Verifica che le connessioni Remote Desktop siano consentite sull'istanza (utilizza AWSSupport-TroubleshootRDP per enable Remote Desktop connections).
- Verificare che la password non sia scaduta. Se la password è scaduta, è possibile reimpostarla. Per ulteriori informazioni, consulta Reimpostazione di una password amministratore Windows persa o scaduta.
- Se tenti di connetterti utilizzando un utente creato nell'istanza e ricevi l'errore `The user cannot connect to the server due to insufficient access privileges`, assicurati di aver garantito all'utente il diritto di accesso locale. Per ulteriori informazioni, consulta l'articolo su come garantire a un membro il diritto di accesso locale.
- Se si tenta di aprire un numero di sessioni RDP contemporanee superiore alla soglia massima consentita, la sessione viene terminata con il messaggio `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.` Per impostazione predefinita, sono consentite due sessioni RDP contemporanee sull'istanza.

Errore durante l'uso del client macOS RDP

Se ti connetti a un'istanza di Windows Server utilizzando il client Remote Desktop Connection dal sito Web di Microsoft, potresti ricevere il seguente errore:

```
Remote Desktop Connection cannot verify the identity of the computer that you want to
 connect to.
```

Scaricare l'app Microsoft Remote Desktop dal Mac App Store e utilizzarla per connettersi all'istanza.

RDP mostra una schermata nera invece del desktop

Per risolvere il problema, prova a eseguire queste operazioni:

- Per ulteriori informazioni, controllare l'output della console. Per ottenere l'output della console per l'istanza utilizzando la console Amazon EC2, selezionare l'istanza, scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get system log (Ottieni il log di sistema).
- Verificare che sia in esecuzione la versione più recente del client RDP.
- Provare le impostazioni predefinite per il client RDP. Per ulteriori informazioni, consulta l'articolo sull'ambiente della sessione remota.
- Se si utilizza la connessione al desktop remoto, provare ad avviarla con l'opzione `/admin` come mostrato di seguito.

```
mstsc /v:instance /admin
```

- Se il server esegue un'applicazione a schermo intero, è possibile che abbia smesso di rispondere. Usare Ctrl+Maiusc+Esc per avviare Windows Task Manager, quindi chiudere l'applicazione.
- Se il server viene utilizzato in modo eccessivo, è possibile che abbia smesso di rispondere. Per monitorare l'istanza che utilizza la console Amazon EC2, selezionare l'istanza e quindi la scheda Monitoring (Monitoraggio). Se è necessario cambiare il tipo di istanza con uno di dimensioni maggiori, consulta Cambiare il tipo di istanza.

Impossibile accedere da remoto a un'istanza con un utente che non è un amministratore

Se non riesci ad accedere da remoto a un'istanza Windows con un utente che non è un account amministratore, verifica di aver concesso all'utente il diritto di accedere in locale. Consulta Garantire a un utente o a un gruppo il diritto di accesso locale ai controller di dominio.

Risoluzione dei problemi relativi a Remote Desktop utilizzando AWS Systems Manager

Puoi utilizzarlo AWS Systems Manager per risolvere i problemi di connessione all'istanza di Windows tramite RDP.

AWSSupport- Risolvi i problemi RDP

Il documento di automazione AWSSupport -TroubleshootRDP consente all'utente di controllare o modificare le impostazioni comuni sull'istanza di destinazione che possono influire sulle connessioni RDP (Remote Desktop Protocol), come la porta RDP, l'autenticazione a livello di rete (NLA) e i profili Windows Firewall. Per impostazione predefinita, il documento legge e produce i valori di queste impostazioni.

Il documento di automazione AWSSupport -TroubleshootRDP può essere utilizzato con istanze EC2, istanze locali e macchine virtuali (VM) abilitate all'uso con AWS Systems Manager (istanze gestite). Inoltre, può essere utilizzato anche con istanze EC2 per Windows Server che non sono abilitate per l'utilizzo con Systems Manager. Per informazioni sull'abilitazione delle istanze da utilizzare con, consulta Managed nodes nella Guida per l'utente. AWS Systems ManagerAWS Systems Manager

Per risolvere i problemi relativi all'utilizzo del documento -TroubleshootRDP AWSSupport

1. Accedere alla console Systems Manager.
2. Verificare di trovarsi nella stessa regione dell'istanza danneggiata.
3. Scegli Documents (Documenti) nel riquadro di navigazione sinistro.
4. Nella scheda Owned by Amazon (Di proprietà di Amazon), inserisci `AWSSupport-TroubleshootRDP` nel campo di ricerca. Quando appare il documento `AWSSupport-TroubleshootRDP`, selezionalo.
5. Scegliere Execute automation (Esegui automazione).
6. Per Execution Mode (Modalità esecuzione), scegliere Simple execution (Esecuzione semplice).
7. Per i parametri di input, abilitate Mostra il selettore interattivo di istanze. InstanceId
8. Scegliere l'istanza Amazon EC2.
9. Rivedere gli esempi, quindi scegliere Execute (Esegui).
10. Per monitorare l'avanzamento dell'esecuzione, per Execution status (Stato esecuzione), aspettare che lo stato cambi da Pending (In sospeso) a Success (Riuscito). Espandere Outputs (Output) per vedere i risultati. Per vedere l'output delle singole fasi, in Executed Steps (Fasi eseguite), scegliere Step ID (ID fase).

AWSSupport- Esempi di RDP di Troubleshoot

Gli esempi seguenti mostrano come eseguire le attività di risoluzione dei problemi più comuni utilizzando -TroubleshootRDP. AWSSupport È possibile utilizzare il AWS CLI start-automation-executioncomando di esempio o il collegamento fornito a. AWS Management Console

Example Esempio: verificare lo stato RDP attuale

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=instance_id, Action=Custom" --region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Esempio: disabilitare Windows Firewall

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, Firewall=Disable" --
region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Esempio: disabilitare Network Level Authentication

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, NLASettingAction=Disable" --
region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion
```

Example Esempio: impostare RDP Service Startup Type su Automatico e avviare il servizio RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPServiceStartupType=Auto,
 RDPServiceAction=Start" --region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Esempio: ripristinare la porta RDP predefinita (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPPortAction=Modify" --
region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example Esempio: consentire connessioni remote

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RemoteConnections=Enable" --
region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport- Esegui EC2 Rescue

Il documento di automazione AWSSupport -Exec2Rescue utilizza EC2Rescue for Windows Server per risolvere e ripristinare automaticamente i problemi di connettività delle istanze EC2 e RDP. Per ulteriori informazioni, consulta Esecuzione dello strumento EC2Rescue su istanze non raggiungibili.

Il documento di automazione -ExeceEC2Rescue richiede l'arresto e il AWSSupport riavvio dell'istanza. Systems Manager arresta l'istanza e crea un'Amazon Machine Image (AMI). I dati archiviati nei volumi dell'instance store vengono persi. L'indirizzo IP pubblico viene modificato se non si utilizza un IP elastico. Per ulteriori informazioni, consulta Esecuzione dello strumento EC2Rescue su istanze non raggiungibili nella Guida per l'utente di AWS Systems Manager .

Per risolvere i problemi relativi all'utilizzo del documento -Exec2Rescue AWSSupport

1. Aprire la console Systems Manager.
2. Verificare di trovarsi nella stessa regione dell'istanza Amazon EC2 danneggiata.
3. Nel riquadro di navigazione, scegli Documenti.
4. Cerca e seleziona il documento `AWSSupport-ExecuteEC2Rescue`, quindi scegli Esegui automazione.
5. In Execution Mode (Modalità esecuzione), scegliere Simple execution (Esecuzione semplice).
6. Nella sezione Parametri di input, per UnreachableInstanceId, inserisci l'ID dell'istanza Amazon EC2 dell'istanza irraggiungibile.
7. (Facoltativo) Per LogDestination, inserisci il nome del bucket Amazon Simple Storage Service (Amazon S3) se desideri raccogliere i log del sistema operativo per la risoluzione dei problemi della tua istanza Amazon EC2. I log vengono automaticamente caricati nel bucket specificato.
8. Selezionare Execute (Esegui).
9. Per monitorare l'avanzamento dell'esecuzione, nello stato Execution (Esecuzione), aspettare che lo stato cambi da Pending (In sospeso) a Success (Riuscito). Espandere Outputs (Output) per vedere i risultati. Per vedere l'output delle singole fasi, in Executed Steps (Fasi eseguite), scegliere Step ID (ID Fase).

Abilitazione di Desktop remoto in un'istanza EC2 con il Registro di sistema remoto

Se l'istanza irraggiungibile non è gestita da AWS Systems Manager Session Manager, è possibile utilizzare il registro remoto per abilitare Remote Desktop.

1. Dalla console EC2, arrestare l'istanza irraggiungibile.
2. Scollega il volume root dell'istanza non raggiungibile e collegalo a un'istanza raggiungibile nella stessa zona di disponibilità come volume di archiviazione. Se non disponi di un'istanza raggiungibile nella stessa zona di disponibilità, avviane una. Prendi nota del nome del dispositivo del volume root sull'istanza irraggiungibile.
3. Sull'istanza raggiungibile, apri Gestione disco. Ciò è possibile emettendo il comando seguente in una finestra di prompt dei comandi.

   ```
   diskmgmt.msc
   ```
4. Fai clic con il pulsante destro del mouse sul nuovo volume collegato proveniente dall'istanza irraggiungibile, quindi scegli Online.
5. Apri l'editor del Registro di Windows. Ciò è possibile emettendo il comando seguente in una finestra di prompt dei comandi.

   ```
   regedit
   ```
6. Nell'Editor del registro di sistema, scegliere HKEY_LOCAL_MACHINE, quindi selezionare File, Carica Hive.
7. Selezionare l'unità del volume allegato, passare a `\Windows\System32\config\`, selezionare `SYSTEM`, quindi scegliere Open (Apri).
8. Per Key Name (Nome chiave), immettere un nome univoco per l'hive e scegliere OK.
9. Eseguire il backup dell'hive del Registro di sistema prima di apportare modifiche al Registro di sistema.

   a. Nell'albero della console dell'Editor del registro di sistema seleziona l'hive caricato: HKEY_LOCAL_MACHINE*`nome_chiave`*.

   b. Scegli File, Esporta.

c. Nella finestra di dialogo Esporta file del Registro di sistema scegliere il percorso in cui si desidera salvare la copia di backup e quindi digitare un nome per il file di backup nel campo Nome file.

d. Seleziona Salva.

10. Nell'Editor del registro di sistema passare a `HKEY_LOCAL_MACHINE\`*`your key name`*`\ControlSet001\Control\Terminal Server`, quindi, nel riquadro dei dettagli, fare doppio clic su fDenyTSConnections.
11. Nella casella Modifica valore DWORD immettere `0` nel campo Dati valore.
12. Seleziona OK.

> **Note**
>
> Se il valore nel campo Dati valore è `1`, l'istanza negherà le connessioni desktop remoto. Un valore di `0` consente connessioni desktop remoto.

13. Nell'Editor del registro di sistema, scegli HKEY_LOCAL_MACHINE*`nome_chiave`*, quindi seleziona File, Carica Hive.
14. Chiudere l'Editor del registro di sistema e Gestione disco.
15. Dalla console EC2, scollegare il volume root dall'istanza raggiungibile e collegarlo di nuovo all'istanza non raggiungibile. Quando si collega il volume all'istanza irraggiungibile, immettere il nome del dispositivo salvato in precedenza nel campo Dispositivo.
16. Riavviare l'istanza irraggiungibile.

Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Windows?

Quando ci si connette a un'istanza di Windows appena avviata, decodificare la password per l'account amministratore utilizzando la chiave privata per la coppia di chiavi specificata all'avvio dell'istanza.

Se si perde la password dell'amministratore e non si dispone più della chiave privata, è necessario reimpostare la password o creare una nuova istanza. Per ulteriori informazioni, consulta Reimpostazione di una password amministratore Windows persa o scaduta. Per la procedura di reimpostazione della password utilizzando un documento Systems Manager, consulta

Reimpostazione di password e chiavi SSH sulle istanze EC2 nella Guida per l'utente di AWS Systems Manager .

Reimpostazione di una password amministratore Windows persa o scaduta

> **Note**
>
> Questa sezione si applica solo alle istanze di Windows.

Se non è più possibile accedere all'istanza Amazon EC2 di Windows perché la password dell'amministratore di Windows è persa o scaduta, è possibile reimpostare la password.

> **Note**
>
> Esiste un documento di AWS Systems Manager automazione che applica automaticamente i passaggi manuali necessari per reimpostare la password dell'amministratore locale. Per ulteriori informazioni, consulta Reimpostazione delle password e delle chiavi SSH sulle istanze EC2 nella Guida per l'utente.AWS Systems Manager

I metodi manuali di reimpostazione della password amministratore utilizzano EC2Launch v2, EC2Config o EC2Launch.

- Per tutte le AMI di Windows supportate che includono l'agente EC2Launch v2, utilizza EC2Launch v2.
- Per le AMI Windows precedenti a Windows Server 2016, utilizza il servizio EC2Config.
- Per le AMI Windows Server 2016 e successive, utilizza il servizio EC2Launch.

Tali procedure descrivono inoltre come connettersi a un'istanza se hai perso la coppia di chiavi utilizzata per creare l'istanza. Amazon EC2 utilizza una chiave pubblica per crittografare un singolo dato, come una password, e una chiave privata per decrittografare i dati. La chiave pubblica e quella privata sono note come coppia di chiavi. Con le istanze Windows, puoi utilizzare una coppia di chiavi per ottenere la password amministratore e accedere tramite RDP.

> **Note**
>
> Se nell'istanza è stato disattivato l'account amministratore locale e l'istanza è configurata per Systems Manager, è inoltre possibile riattivare e reimpostare la password dell'amministratore locale utilizzando EC2Rescue e Run Command. Per ulteriori informazioni, vedere Usare EC2Rescue per Windows Server with Systems Manager Run Command.

Indice

Reimpostazione della password amministratore Windows tramite EC2Launch v2

Se hai perso la password amministratore Windows e utilizzi un'AMI Windows supportata che include l'agente EC2Launch v2, puoi utilizzare EC2Launch v2 per generare una nuova password.

Se utilizzi un'AMI Windows Server 2016 o versione successiva che non include l'agente EC2Launch v2, consulta la sezione Reimpostazione della password amministratore Windows tramite EC2Launch.

Se utilizzi un'AMI Windows Server precedente a Windows Server 2016 che non include l'agente EC2Launch v2, consulta la sezione Reimpostazione della password amministratore Windows tramite EC2Config.

> **Note**
>
> Se nell'istanza è stato disattivato l'account amministratore locale e l'istanza è configurata per Systems Manager, è inoltre possibile riattivare e reimpostare la password dell'amministratore locale utilizzando EC2Rescue e Run Command. Per ulteriori informazioni, vedere Usare EC2Rescue per Windows Server with Systems Manager Run Command.

> **Note**
>
> Esiste un documento di AWS Systems Manager automazione che applica automaticamente i passaggi manuali necessari per reimpostare la password dell'amministratore locale. Per ulteriori informazioni, consulta Reimpostazione delle password e delle chiavi SSH sulle istanze EC2 nella Guida per l'utente.AWS Systems Manager

Per reimpostare la password dell'amministratore di Windows usando EC2Launch v2, è necessario eseguire la seguente azione:

- Fase 1: Verifica che l'agente EC2Launch v2 sia in esecuzione
- Fase 2: Distaccare il volume radice dall'istanza
- Fase 3: Collegare il volume a un'istanza temporanea.
- Fase 4: Eliminare il file .run-once
- Fase 5: Riavviare l'istanza originale.

Fase 1: Verifica che l'agente EC2Launch v2 sia in esecuzione

Prima di tentare di reimpostare la password amministratore, verifica che l'agente EC2Launch v2 sia installato e in esecuzione. Puoi utilizzare l'agente EC2Launch v2 per reimpostare la password amministratore più avanti in questa sezione.

Per verificare che l'agente EC2Launch v2 sia in esecuzione

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Instances (Istanze), quindi selezionare l'istanza per la quale si desidera reimpostare la password. In questa procedura questa istanza viene chiamata istanza originale.
3. Scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get system log (Ottieni il log di sistema).
4. Individua la voce di avvio di EC2, ad esempio Launch: EC2Launch v2 service v2.0.124. Se viene visualizzata questa voce, il servizio EC2Launch v2 è in esecuzione.

   Se l'output del log di sistema è vuoto, o se l'agente EC2Launch v2 non è in esecuzione, risolvi il problema dell'istanza con il servizio di acquisizione di screenshot della console dell'istanza. Per ulteriori informazioni, consulta Acquisizione di uno screenshot di un'istanza irraggiungibile.

Fase 2: Distaccare il volume radice dall'istanza

Non è possibile usare EC2Launch v2 per reimpostare una password amministratore se il volume in cui la password è archiviata è collegato a un'istanza come il volume root. È necessario distaccare il volume dall'istanza originale prima che sia possibile collegarlo a un'istanza temporanea come volume secondario.

Per distaccare il volume root dall'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza che richiede la reimpostazione della password e scegli Instance state, Stop instance. Dopo aver modificato lo stato dell'istanza in Stopped (Arrestato), passa alla fase successiva.
4. (Facoltativo) Se disponi della chiave privata specificata al momento dell'avvio dell'istanza, passa alla fase successiva. In caso contrario, attieniti alla seguente procedura per sostituire l'istanza con una nuova istanza avviata con una nuova coppia di chiavi.

    a. Creare una nuova coppia di chiavi tramite la console Amazon EC2. Per assegnare alla nuova coppia di chiavi lo stesso nome della chiave privata persa, bisogna prima eliminare la coppia di chiavi esistente.
    b. Selezionare l'istanza da sostituire. Prendere nota del tipo di istanza, del VPC, della sottorete, del gruppo di sicurezza e del ruolo IAM dell'istanza.
    c. Con l'istanza selezionata, scegli Azioni, Immagine e modelli, Crea immagine. Digitare un nome e una descrizione dell'immagine, quindi selezionare Create image (Crea immagine).
    d. Nel riquadro di navigazione scegliere AMIs (AMI). Attendi che lo stato dell'immagine diventi disponibile. Quindi, seleziona l'immagine e scegli Launch instance from AMI.
    e. Completa i campi per avviare un'istanza, assicurandoti di selezionare lo stesso tipo di istanza, VPC, sottorete, gruppo di sicurezza e ruolo IAM dell'istanza da sostituire, quindi scegli Launch instance.
    f. Quando richiesto, scegli la key pair che hai creato per la nuova istanza, quindi scegli Launch instance.
    g. (Facoltativo) Se l'istanza originale dispone di un indirizzo IP elastico associato, trasferirlo alla nuova istanza. Se l'istanza originale ha volumi EBS oltre al volume root, trasferirli nella nuova istanza.
5. Distaccare il volume root dall'istanza originale come indicato di seguito:

a. Seleziona l'istanza originale e scegli la scheda Archiviazione. Annota il nome del dispositivo root in Nome dispositivo root. Trova il volume con questo nome di dispositivo in Blocca dispositivi e annota l'ID del volume.

b. Nel riquadro di navigazione, selezionare Volumes (Volumi).

c. Nell'elenco dei volumi, seleziona il volume che hai indicato come dispositivo principale e scegli Azioni, Scollega volume. Una volta modificato lo stato del volume su available (disponibile), passare alla fase successiva.

6. Se hai creato una nuova istanza per sostituire l'istanza originale, ora puoi terminare l'istanza originale. Non è più necessaria. Per il resto di questa procedura, tutti i riferimenti all'istanza originale si applicano alla nuova istanza creata.

Fase 3: Collegare il volume a un'istanza temporanea.

Successivamente, avviare un'istanza temporanea e collegare il volume come volume secondario. Questa è l'istanza che viene usata per modificare il file di configurazione.

Per avviare un'istanza temporanea e collegare il volume

1. Avviare l'istanza temporanea come indicato di seguito:

   a. Nel pannello di navigazione, selezionare Instances (Istanze), selezionare Launch instances (Avvia istanze) e poi selezionare una AMI.

   > **Important**
   >
   > Per evitare collisioni di firme del disco è necessario selezionare un'AMI per una versione diversa di Windows. Ad esempio, se l'istanza originale esegue Windows Server 2019, avviare l'istanza temporanea utilizzando l'AMI di base per Windows Server 2016.

   b. Lasciare il tipo di istanza predefinito, quindi scegliere Next: Configure Instance Details (Successivo: configura dettagli dell'istanza).

   c. Alla pagina Configure Instance Details (Configura i dettagli dell'istanza), per Subnet (Sottorete) selezionare la stessa zona di disponibilità dell'istanza originale e scegliere Review and Launch (Rivedi e avvia).

> **Important**
>
> L'istanza temporanea deve trovarsi nella stessa zona di disponibilità dell'istanza originale. Se l'istanza temporanea si trova in una zona di disponibilità diversa, non è possibile collegare il volume root dell'istanza originale.

d. Nella pagina Review Instance Launch (Verifica avvio istanza), scegliere Launch (Avvia).

e. Quando richiesto, creare una nuova coppia di chiavi, scaricarla su un percorso sicuro nel computer, quindi scegliere Launch Instances (Avvia istanze).

2. Collegare il volume all'istanza temporanea come volume secondario seguendo questi passaggi:

   a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza originale e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

   b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza temporanea, quindi selezionare l'istanza dall'elenco.

   c. Per Device (Dispositivo), digitare **`xvdf`** (se non è già inserito) e scegliere Attach (Collega).

Fase 4: Eliminare il file .run-once

È ora necessario eliminare il file `.run-once` dal volume offline allegato all'istanza. Questo indica a EC2Launch v2 di eseguire tutte le attività con una frequenza di `once`, che include l'impostazione della password amministratore. Il percorso del file nel volume secondario collegato sarà simile a `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

Per eliminare il file .run-once

1. Apri l'utilità Gestione disco e porta l'unità online seguendo queste istruzioni: Rendi disponibile un volume Amazon EBS per l'uso.
2. Individua il file `.run-once` nel disco che hai portato online.
3. Elimina il file .run-once.

> **Important**
>
> Qualsiasi script impostato per un'esecuzione sarà attivato da questa azione.

Fase 5: Riavviare l'istanza originale.

Dopo aver eliminato il file `.run-once`, ricollegare il volume all'istanza originale come volume root e collegarlo all'istanza usando la sua coppia di chiavi per recuperare la password dell'amministratore.

1. Collegare nuovamente il volume all'istanza originale come segue:

   a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

   b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza originale, quindi selezionare l'istanza.

   c. Per Device (Dispositivo), digitare **`/dev/sda1`**.

   d. Scegliere Attach (Collega). Dopo che lo stato del volume cambia in `in-use`, passa alla fase successiva.

2. Nel riquadro di navigazione, seleziona Instances (Istanze). Selezionare l'istanza originale e scegliere Instance state (Stato istanza), Start instance (Avvia istanza). Dopo che lo stato dell'istanza cambia in `Running`, passa alla fase successiva.

3. Recuperare la nuova password di amministratore di Windows utilizzando la chiave privata per la nuova coppia di chiavi e connettersi all'istanza. Per ulteriori informazioni, consulta Connettiti all'istanza Windows .

   > **Important**
   >
   > Quando viene arrestata e riavviata, l'istanza riceve un nuovo indirizzo IP pubblico. Assicurarsi di collegarsi all'istanza utilizzando il relativo nome DNS pubblico. Per ulteriori informazioni, consulta Ciclo di vita dell'istanza.

4. (Facoltativo) È possibile terminare l'istanza temporanea se non la si utilizza più. Selezionare l'istanza temporanea e scegliere Instance state (Stato istanza), Terminate instance (Termina istanza).

Reimpostazione della password amministratore Windows tramite EC2Config

Se hai perso la password amministratore Windows e utilizzi un'AMI Windows precedente a Windows Server 2016, puoi utilizzare l'agente EC2Config per generare una nuova password.

Se hai perso la password amministratore Windows e utilizzi un'AMI Windows Server 2016 o successiva, consulta la sezione Reimpostazione della password amministratore Windows tramite EC2Launch oppure utilizza lo strumento EC2Rescue, che utilizza il servizio EC2Launch per generare una nuova password.

> **Note**
>
> Se nell'istanza è stato disattivato l'account amministratore locale e l'istanza è configurata per Systems Manager, è inoltre possibile riattivare e reimpostare la password dell'amministratore locale utilizzando EC2Rescue e Run Command. Per ulteriori informazioni, vedere Usare EC2Rescue per Windows Server with Systems Manager Run Command.

> **Note**
>
> Esiste un documento di AWS Systems Manager automazione che applica automaticamente i passaggi manuali necessari per reimpostare la password dell'amministratore locale. Per ulteriori informazioni, consulta Reimpostazione delle password e delle chiavi SSH sulle istanze EC2 nella Guida per l'utente.AWS Systems Manager

Per reimpostare la password dell'amministratore di Windows usando EC2Config, è necessario eseguire la seguente azione:

- Fase 1: Verifica che il servizio EC2Config sia in esecuzione
- Fase 2: Distaccare il volume radice dall'istanza
- Fase 3: Collegare il volume a un'istanza temporanea.
- Fase 4: modificare il file di configurazione
- Fase 5: Riavviare l'istanza originale.

Fase 1: Verifica che il servizio EC2Config sia in esecuzione

Prima di tentare di reimpostare la password amministratore, verificare che il servizio EC2Config sia installato e in esecuzione. Puoi utilizzare il servizio EC2Config per reimpostare la password amministratore più avanti in questa sezione.

Per verificare che il servizio EC2Config sia in esecuzione

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Instances (Istanze), quindi selezionare l'istanza per la quale si desidera reimpostare la password. In questa procedura questa istanza viene chiamata istanza originale.
3. Scegli Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get system log (Ottieni il log di sistema).

   (Vecchia console) Scegli Actions (Operazioni), System Settings (Impostazioni di sistema), Get System Log (Ottieni log di sistema).
4. Individuare la voce dell'agente EC2, ad esempio EC2 Agent: Ec2Config service v3.18.1118 (Agente EC2: servizio Ec2Config v3.18.1118). Se questa voce viene visualizzata, il servizio EC2Config è in esecuzione.

   Se l'output del log di sistema è vuoto, o se il servizio EC2Config non è in esecuzione, risolvere il problema dell'istanza con il servizio di acquisizione di screenshot della console dell'istanza. Per ulteriori informazioni, consulta Acquisizione di uno screenshot di un'istanza irraggiungibile.

Fase 2: Distaccare il volume radice dall'istanza

Non è possibile usare EC2Config per reimpostare una password amministratore se il volume in cui la password è archiviata è collegato a un'istanza come il volume della radice. È necessario distaccare il volume dall'istanza originale prima che sia possibile collegarlo a un'istanza temporanea come volume secondario.

Per distaccare il volume root dall'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.

3. Seleziona l'istanza che richiede la reimpostazione della password e scegli Instance state, Stop instance. Dopo aver modificato lo stato dell'istanza in Stopped (Arrestato), passa alla fase successiva.
4. (Facoltativo) Se disponi della chiave privata specificata al momento dell'avvio dell'istanza, passa alla fase successiva. In caso contrario, attieniti alla seguente procedura per sostituire l'istanza con una nuova istanza avviata con una nuova coppia di chiavi.

   a. Creare una nuova coppia di chiavi tramite la console Amazon EC2. Per assegnare alla nuova coppia di chiavi lo stesso nome della chiave privata persa, bisogna prima eliminare la coppia di chiavi esistente.
   b. Selezionare l'istanza da sostituire. Prendere nota del tipo di istanza, del VPC, della sottorete, del gruppo di sicurezza e del ruolo IAM dell'istanza.
   c. Con l'istanza selezionata, scegli Azioni, Immagine e modelli, Crea immagine. Digitare un nome e una descrizione dell'immagine, quindi selezionare Create image (Crea immagine).
   d. Nel riquadro di navigazione scegliere AMIs (AMI). Attendi che lo stato dell'immagine diventi disponibile. Quindi, seleziona l'immagine e scegli Launch instance from AMI.
   e. Completa i campi per avviare un'istanza, assicurandoti di selezionare lo stesso tipo di istanza, VPC, sottorete, gruppo di sicurezza e ruolo IAM dell'istanza da sostituire, quindi scegli Launch instance.
   f. Quando richiesto, scegli la key pair che hai creato per la nuova istanza, quindi scegli Launch instance.
   g. (Facoltativo) Se l'istanza originale dispone di un indirizzo IP elastico associato, trasferirlo alla nuova istanza. Se l'istanza originale ha volumi EBS oltre al volume root, trasferirli nella nuova istanza.
5. Distaccare il volume root dall'istanza originale come indicato di seguito:

   a. Seleziona l'istanza originale e scegli la scheda Archiviazione. Annota il nome del dispositivo root in Nome dispositivo root. Trova il volume con questo nome di dispositivo in Blocca dispositivi e annota l'ID del volume.
   b. Nel riquadro di navigazione, selezionare Volumes (Volumi).
   c. Nell'elenco dei volumi, seleziona il volume che hai indicato come dispositivo principale e scegli Azioni, Scollega volume. Una volta modificato lo stato del volume su available (disponibile), passare alla fase successiva.

6. Se hai creato una nuova istanza per sostituire l'istanza originale, ora puoi terminare l'istanza originale. Non è più necessaria. Per il resto di questa procedura, tutti i riferimenti all'istanza originale si applicano alla nuova istanza creata.

Fase 3: Collegare il volume a un'istanza temporanea.

Successivamente, avviare un'istanza temporanea e collegare il volume come volume secondario. Questa è l'istanza che viene usata per modificare il file di configurazione.

Per avviare un'istanza temporanea e collegare il volume

1. Avviare l'istanza temporanea come indicato di seguito:

   a. Nel pannello di navigazione, selezionare Instances (Istanze), selezionare Launch instances (Avvia istanze) e poi selezionare una AMI.

   > **Important**
   >
   > Per evitare collisioni di firme del disco è necessario selezionare un'AMI per una versione diversa di Windows. Ad esempio, se l'istanza originale esegue Windows Server 2019, avviare l'istanza temporanea utilizzando l'AMI di base per Windows Server 2016.

   b. Lasciare il tipo di istanza predefinito, quindi scegliere Next: Configure Instance Details (Successivo: configura dettagli dell'istanza).

   c. Alla pagina Configure Instance Details (Configura i dettagli dell'istanza), per Subnet (Sottorete) selezionare la stessa zona di disponibilità dell'istanza originale e scegliere Review and Launch (Rivedi e avvia).

   > **Important**
   >
   > L'istanza temporanea deve trovarsi nella stessa zona di disponibilità dell'istanza originale. Se l'istanza temporanea si trova in una zona di disponibilità diversa, non è possibile collegare il volume root dell'istanza originale.

   d. Nella pagina Review Instance Launch (Verifica avvio istanza), scegliere Launch (Avvia).

   e. Quando richiesto, creare una nuova coppia di chiavi, scaricarla su un percorso sicuro nel computer, quindi scegliere Launch Instances (Avvia istanze).

2. Collegare il volume all'istanza temporanea come volume secondario seguendo questi passaggi:

   a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza originale e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

   b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza temporanea, quindi selezionare l'istanza dall'elenco.

   c. Per Device (Dispositivo), digitare **`xvdf`** (se non è già inserito) e scegliere Attach (Collega).

Fase 4: modificare il file di configurazione

Dopo aver collegato il volume all'istanza temporanea come volume secondario, modificare il plugin `Ec2SetPassword` nel file di configurazione.

Per modificare il file di configurazione

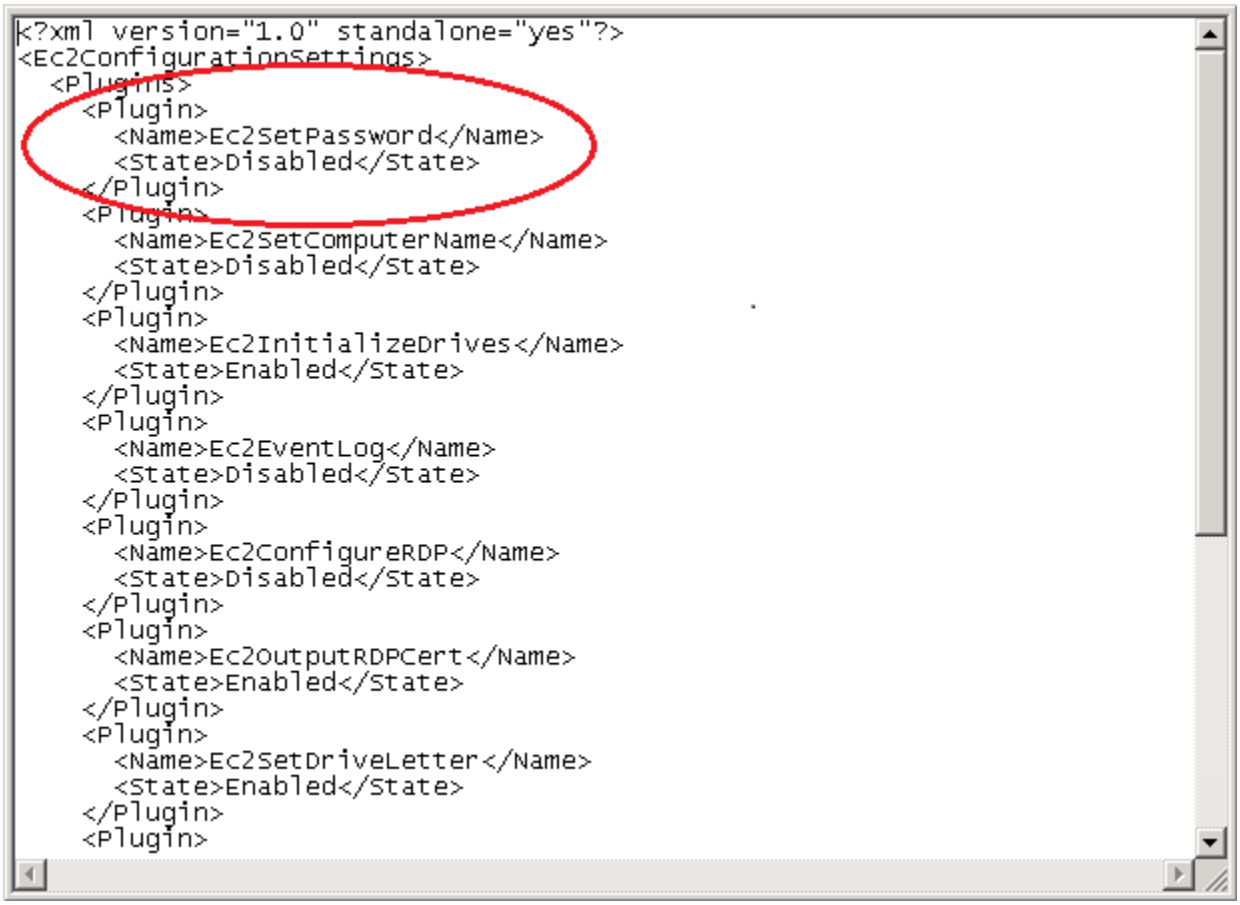
1. Dall'istanza temporanea, modificare il file di configurazione sul volume secondario come segue:

   a. Avviare e collegare all'istanza temporanea.

   b. Utilizza le seguenti istruzioni per portare l'unità online: Rendi disponibile un volume Amazon EBS per l'uso.

   c. Andare al volume secondario e aprire `\Program Files\Amazon\Ec2ConfigService\Settings\config.xml` con un editor di testo come Notepad.

   d. Nella parte superiore del file, cercare il plug-in con il nome `Ec2SetPassword`, come nella schermata. Modificare lo stato da `Disabled` a `Enabled` e salvare il file.



2. Dopo aver modificato il file di configurazione, distaccare il volume secondario dall'istanza temporanea come segue:

   a. Tramite l'utilità Disk Management (Gestione disco), portare il volume offline.

   b. Disconnettersi dall'istanza temporanea e tornare alla console Amazon EC2.

   c. Nel riquadro di navigazione, selezionare Volumes (Volumi), selezionare il volume e quindi scegliere Actions (Operazioni), Detach Volume (Distacca volume). Una volta che lo stato del volume cambia in available (disponibile), continuare con la fase successiva.

Fase 5: Riavviare l'istanza originale.

Dopo aver modificato il file di configurazione, ricollegare il volume all'istanza originale come volume root e collegarlo all'istanza usando la sua coppia di chiavi per recuperare la password dell'amministratore.

1. Collegare nuovamente il volume all'istanza originale come segue:

a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza originale, quindi selezionare l'istanza.

c. Per Device (Dispositivo), digitare **`/dev/sda1`**.

d. Scegliere Attach (Collega). Dopo che lo stato del volume cambia in `in-use`, passa alla fase successiva.

2. Nel riquadro di navigazione, seleziona Instances (Istanze). Selezionare l'istanza originale e scegliere Instance state (Stato istanza), Start instance (Avvia istanza). Dopo che lo stato dell'istanza cambia in `Running`, passa alla fase successiva.

3. Recuperare la nuova password di amministratore di Windows utilizzando la chiave privata per la nuova coppia di chiavi e connettersi all'istanza. Per ulteriori informazioni, consulta Connettiti all'istanza Windows .

> **Important**
>
> Quando viene arrestata e riavviata, l'istanza riceve un nuovo indirizzo IP pubblico. Assicurarsi di collegarsi all'istanza utilizzando il relativo nome DNS pubblico. Per ulteriori informazioni, consulta Ciclo di vita dell'istanza.

4. (Facoltativo) È possibile terminare l'istanza temporanea se non la si utilizza più. Selezionare l'istanza temporanea e scegliere Instance state (Stato istanza), Terminate instance (Termina istanza).

Reimpostazione della password amministratore Windows tramite EC2Launch

Se hai perso la password amministratore Windows e utilizzi un'AMI Windows Server 2016 o successiva, puoi utilizzare lo strumento EC2Rescue, che utilizza il servizio EC2Launch per generare una nuova password.

Se utilizzi un'AMI Windows Server 2016 o versione successiva che non include l'agente EC2Launch v2, puoi utilizzare EC2Launch v2 per generare una nuova password.

Se utilizzi un'AMI Windows Server precedente a Windows Server 2016, consulta Reimpostazione della password amministratore Windows tramite EC2Config.

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per non perdere i dati dei volumi di archivio istanza, è opportuno creare una copia di backup nell'archiviazione persistente.

> **Note**
>
> Se nell'istanza è stato disattivato l'account amministratore locale e l'istanza è configurata per Systems Manager, è inoltre possibile riattivare e reimpostare la password dell'amministratore locale utilizzando EC2Rescue e Run Command. Per ulteriori informazioni, vedere Usare EC2Rescue per Windows Server with Systems Manager Run Command.

> **Note**
>
> Esiste un documento di AWS Systems Manager automazione che applica automaticamente i passaggi manuali necessari per reimpostare la password dell'amministratore locale. Per ulteriori informazioni, consulta Reimpostazione delle password e delle chiavi SSH sulle istanze EC2 nella Guida per l'utente.AWS Systems Manager

Per reimpostare la password dell'amministratore di Windows usando EC2Launch, è necessario eseguire la seguente azione:

- Fase 1: Distaccare il volume radice dall'istanza
- Fase 2: Collegare il volume a un'istanza temporanea.
- Fase 3: Reimpostare la password amministratore
- Fase 4: Riavviare l'istanza originale.

Fase 1: Distaccare il volume radice dall'istanza

Non è possibile usare EC2Launch per reimpostare una password amministratore se il volume in cui la password è archiviata è collegato a un'istanza come il volume root. È necessario distaccare il volume dall'istanza originale prima che sia possibile collegarlo a un'istanza temporanea come volume secondario.

Per distaccare il volume root dall'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza che richiede la reimpostazione della password e scegli Instance state, Stop instance. Dopo aver modificato lo stato dell'istanza in Stopped (Arrestato), passa alla fase successiva.
4. (Facoltativo) Se disponi della chiave privata specificata al momento dell'avvio dell'istanza, passa alla fase successiva. In caso contrario, attieniti alla seguente procedura per sostituire l'istanza con una nuova istanza avviata con una nuova coppia di chiavi.

    a. Creare una nuova coppia di chiavi tramite la console Amazon EC2. Per assegnare alla nuova coppia di chiavi lo stesso nome della chiave privata persa, bisogna prima eliminare la coppia di chiavi esistente.
    b. Selezionare l'istanza da sostituire. Prendere nota del tipo di istanza, del VPC, della sottorete, del gruppo di sicurezza e del ruolo IAM dell'istanza.
    c. Con l'istanza selezionata, scegli Azioni, Immagine e modelli, Crea immagine. Digitare un nome e una descrizione dell'immagine, quindi selezionare Create image (Crea immagine).
    d. Nel riquadro di navigazione scegliere AMIs (AMI). Attendi che lo stato dell'immagine diventi disponibile. Quindi, seleziona l'immagine e scegli Launch instance from AMI.
    e. Completa i campi per avviare un'istanza, assicurandoti di selezionare lo stesso tipo di istanza, VPC, sottorete, gruppo di sicurezza e ruolo IAM dell'istanza da sostituire, quindi scegli Launch instance.
    f. Quando richiesto, scegli la key pair che hai creato per la nuova istanza, quindi scegli Launch instance.
    g. (Facoltativo) Se l'istanza originale dispone di un indirizzo IP elastico associato, trasferirlo alla nuova istanza. Se l'istanza originale ha volumi EBS oltre al volume root, trasferirli nella nuova istanza.
5. Distaccare il volume root dall'istanza originale come indicato di seguito:

a. Seleziona l'istanza originale e scegli la scheda Archiviazione. Annota il nome del dispositivo root in Nome dispositivo root. Trova il volume con questo nome di dispositivo in Blocca dispositivi e annota l'ID del volume.

b. Nel riquadro di navigazione, selezionare Volumes (Volumi).

c. Nell'elenco dei volumi, seleziona il volume che hai indicato come dispositivo principale e scegli Azioni, Scollega volume. Una volta modificato lo stato del volume su available (disponibile), passare alla fase successiva.

6. Se hai creato una nuova istanza per sostituire l'istanza originale, ora puoi terminare l'istanza originale. Non è più necessaria. Per il resto di questa procedura, tutti i riferimenti all'istanza originale si applicano alla nuova istanza creata.

Fase 2: Collegare il volume a un'istanza temporanea.

Successivamente, avviare un'istanza temporanea e collegare il volume come volume secondario. Questa è l'istanza che viene usata per eseguire EC2Launch.

Per avviare un'istanza temporanea e collegare il volume

1. Avviare l'istanza temporanea come indicato di seguito:

   a. Nel pannello di navigazione, selezionare Instances (Istanze), selezionare Launch instances (Avvia istanze) e poi selezionare una AMI.

   > **Important**
   >
   > Per evitare collisioni di firme del disco è necessario selezionare un'AMI per una versione diversa di Windows. Ad esempio, se l'istanza originale esegue Windows Server 2019, avviare l'istanza temporanea utilizzando l'AMI di base per Windows Server 2016.

   b. Lasciare il tipo di istanza predefinito, quindi scegliere Next: Configure Instance Details (Successivo: configura dettagli dell'istanza).

   c. Alla pagina Configure Instance Details (Configura i dettagli dell'istanza), per Subnet (Sottorete) selezionare la stessa zona di disponibilità dell'istanza originale e scegliere Review and Launch (Rivedi e avvia).

> **Important**
>
> L'istanza temporanea deve trovarsi nella stessa zona di disponibilità dell'istanza originale. Se l'istanza temporanea si trova in una zona di disponibilità diversa, non è possibile collegare il volume root dell'istanza originale.

d. Nella pagina Review Instance Launch (Verifica avvio istanza), scegliere Launch (Avvia).

e. Quando richiesto, creare una nuova coppia di chiavi, scaricarla su un percorso sicuro nel computer, quindi scegliere Launch Instances (Avvia istanze).

2. Collegare il volume all'istanza temporanea come volume secondario seguendo questi passaggi:

   a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza originale e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

   b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza temporanea, quindi selezionare l'istanza dall'elenco.

   c. Per Device (Dispositivo), digitare **`xvdf`** (se non è già inserito) e scegliere Attach (Collega).

Fase 3: Reimpostare la password amministratore

Successivamente, connettersi all'istanza temporanea e utilizzare EC2Launch per reimpostare la password amministratore.

Per reimpostare la password amministratore

1. Connettersi all'istanza temporanea e utilizzare lo strumento EC2Rescue for Windows Server sull'istanza per reimpostare la password amministratore come segue:

   a. Scaricare il file .zip EC2Rescue for Windows Server, estrarne i contenuti ed eseguire EC2Rescue.exe.

   b. Nella schermata License Agreement (Contratto di licenza), leggere il contratto di licenza e, se si accettano i relativi termini, selezionare I Agree (Accetto).

   c. Nella schermata Welcome to EC2Rescue for Windows Server (Benvenuti in EC2Rescue), selezionare Next (Successivo).

   d. Nella schermata Select mode (Seleziona modalità), scegliere Offline instance (Istanza offline).

e. Nella schermata Select a disk (Seleziona un disco), scegliere il dispositivo xvdf e selezionare Next (Successivo).

f. Confermare la selezione del disco e scegliere Yes (Sì).

g. Dopo aver caricato il volume, selezionare OK.

h. Nella schermata Select Offline Instance (Seleziona istanza offline), scegliere Diagnose and Rescue (Diagnosi e recupero).

i. Nella schermata Summary (Riepilogo), controllare le informazioni e scegliere Next (Successivo).

j. Nella schermata Detected possible issues (Probabili problemi rilevati), selezionare Reset Administrator Password (Reimposta password amministratore) e scegliere Next (Successivo).

k. Nella schermata Confirm (Conferma), selezionare Rescue (Ripristina), OK.

l. Nella schermata Done (Fatto), selezionare Finish (Fine).

m. Chiudere lo strumento EC2Rescue for Windows Server, scollegarsi dall'istanza temporanea e quindi tornare alla console Amazon EC2.

2. Distaccare il volume (`xvdf`) secondario dall'istanza temporanea come indicato di seguito:

a. Nel riquadro di navigazione, selezionare Instances (Istanze) e selezionare l'istanza temporanea.

b. Nella scheda Storage per l'istanza temporanea, prendere nota dell'ID del volume EBS elencato come xvdf.

c. Nel riquadro di navigazione, selezionare Volumes (Volumi).

d. Nell'elenco dei volumi, selezionare il volume annotato nella fase precedente e scegliere Actions (Operazioni), Detach Volume (Distacca il volume). Una volta modificato lo stato del volume su available (disponibile), passare alla fase successiva.

Fase 4: Riavviare l'istanza originale.

Dopo aver reimpostato la password amministratore usando EC2Launch, ricollegare il volume all'istanza originale come volume root e collegarlo all'istanza usando la sua coppia di chiavi per recuperare la password dell'amministratore.

Per riavviare l'istanza originale

1. Collegare nuovamente il volume all'istanza originale come segue:

a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza originale, quindi selezionare l'istanza.

c. Per Device (Dispositivo), digitare **`/dev/sda1`**.

d. Scegliere Attach (Collega). Dopo che lo stato del volume cambia in `in-use`, passa alla fase successiva.

2. Nel riquadro di navigazione, seleziona Instances (Istanze). Selezionare l'istanza originale e scegliere Instance state (Stato istanza), Start instance (Avvia istanza). Dopo che lo stato dell'istanza cambia in `Running`, passa alla fase successiva.
3. Recuperare la nuova password di amministratore di Windows utilizzando la chiave privata per la nuova coppia di chiavi e connettersi all'istanza. Per ulteriori informazioni, consulta Connettiti all'istanza Windows .
4. (Facoltativo) È possibile terminare l'istanza temporanea se non la si utilizza più. Selezionare l'istanza temporanea e scegliere Instance state (Stato istanza), Terminate instance (Termina istanza).

Risoluzione di problemi relativi a un'istanza irraggiungibile

Puoi utilizzare i seguenti metodi per risolvere un'istanza Amazon EC2 non raggiungibile.

Indice

Riavvio dell'istanza

La possibilità di riavviare le istanze altrimenti non raggiungibili è importante sia per la risoluzione dei problemi che per la gestione generale delle istanze.

Così come puoi ripristinare un computer tramite l'apposito pulsante, puoi ripristinare le istanze EC2 utilizzando la console di Amazon EC2, la CLI o l'API. Per ulteriori informazioni, consulta Riavvio dell'istanza.

Output della console delle istanze

L'output della console rappresenta un prezioso strumento per diagnosticare i problemi. In particolare, è utile per risolvere i problemi del kernel e della configurazione dei servizi che potrebbero causare la terminazione o la mancata raggiungibilità di un'istanza prima che il relativo daemon SSH possa essere avviato.

- Istanze Linux: l'output della console dell'istanza mostra l'esatto output della console che normalmente verrebbe visualizzato su un monitor fisico collegato a un computer. L'output della console restituisce le informazioni di buffering pubblicate poco dopo lo stato transitorio di un'istanza (avvio, arresto, riavvio e terminazione). L'output pubblicato non viene aggiornato continuamente, ma solo quando viene ritenuto importante.
- Istanze Windows: l'output della console dell'istanza include gli ultimi tre errori del registro degli eventi di sistema.

Solo il proprietario dell'istanza può accedere all'output della console.

È possibile recuperare l'output più recente della console seriale durante il ciclo di vita dell'istanza. Questa opzione è supportata solo sulle istanze create sul sistema Nitro. AWS Non è supportato tramite la console Amazon EC2.

Console

Per ottenere l'output della console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegliere Instances (Istanze).
3. Selezionare l'istanza e poi scegliere Operazioni, Monitoraggio e risoluzione dei problemi, Ottieni il log di sistema.

Command line

Per ottenere l'output della console

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- get-console-output (AWS CLI)
- Get-EC2ConsoleOutput (AWS Tools for Windows PowerShell)

Acquisizione di uno screenshot di un'istanza irraggiungibile

Se non riesci a connetterti alla tua istanza, puoi catturare uno screenshot dell'istanza e visualizzarla come immagine. L'immagine può fornire visibilità dello stato dell'istanza e risolvere più rapidamente eventuali problemi.

Puoi generare screenshot mentre l'istanza è in esecuzione o dopo il suo arresto. L'immagine è generata in formato JPG e non supera i 100 KB. Per lo screenshot non sono previsti costi di trasferimento dei dati.

Limitazioni

Questa funzionalità non è supportata dalle seguenti istanze:

- Istanze bare metal (istanze del tipo `*.metal`)
- L'istanza utilizza un driver NVIDIA GRID
- Istanze alimentate da processori Graviton basati su ARM
- Istanze Windows attive AWS Outposts
- Istanze Windows su AWS Local Zones

Regioni supportate

Questa funzionalità è disponibile nelle seguenti regioni :

- US East (N. Virginia) Region
- Stati Uniti orientali (Ohio)
- Regione Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Regione Africa (Città del Capo)
- Regione Asia Pacifico (Hong Kong)
- Regione Asia Pacifico (Hyderabad)

- Regione Asia Pacifico (Giacarta)
- Regione Asia Pacifico (Melbourne)
- Regione Asia Pacifico (Mumbai)
- Regione Asia Pacifico (Osaka-Locale)
- Regione Asia Pacifico (Seoul)
- Regione Asia Pacifico (Singapore)
- Regione Asia Pacifico (Sydney)
- Regione Asia Pacifico (Tokyo)
- Regione Canada (Centrale)
- Regione Canada occidentale (Calgary)
- Regione Cina (Pechino)
- Regione Cina (Ningxia)
- Regione Europa (Francoforte)
- Regione Europa (Irlanda)
- Regione Europa (Londra)
- Regione Europa (Milano)
- Regione Europa (Parigi)
- Regione Europa (Spagna)
- Regione Europa (Stoccolma)
- Regione Europa (Zurigo)
- Regione di Israele (Tel Aviv)
- Regione Sud America (San Paolo)
- Regione Medio Oriente (Bahrein)
- Regione Medio Oriente (EAU)

Console

Per ottenere uno screenshot di un'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Instances (Istanze).
3. Selezionare l'istanza da acquisire.

4. Scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get instance screenshot (Ottieni screenshot istanza).
5. Scegliere Download (Scarica) o fare clic con il pulsante destro del mouse sull'immagine per scaricarla e salvarla.

Command line

Per acquisire uno screenshot di un'istanza

È possibile utilizzare uno dei seguenti comandi. Il contenuto restituito è con codifica base64. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Accesso a Amazon EC2.

- get-console-screenshot (AWS CLI)
- GetConsoleScreenshot(API di interrogazione Amazon EC2)

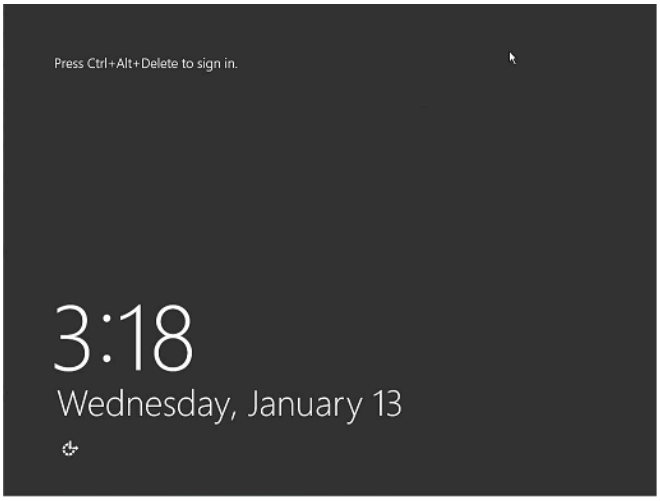
Schermate comuni per le istanze Windows

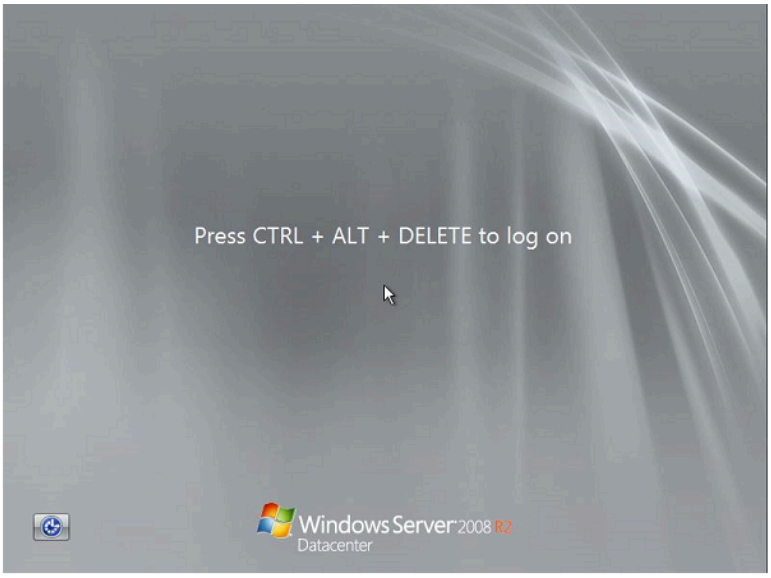
Puoi utilizzare le informazioni seguenti per facilitare la risoluzione dei problemi associati a un'istanza Windows irraggiungibile in base all'acquisizione di screenshot restituiti dal servizio.

- Schermata di accesso (Ctrl+Alt+Canc)
- Schermata della console di ripristino
- Schermata Windows Boot Manager
- Schermata Sysprep
- Schermata di preparazione
- Schermata Windows Update
- Chkdsk

Schermata di accesso (Ctrl+Alt+Canc)

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.





Se un'istanza diventa irraggiungibile durante l'accesso, potrebbe esserci un problema relativo alla configurazione di rete o ai Servizi Desktop remoto di Windows. Un'istanza può inoltre non rispondere se un processo utilizza una quantità significativa di CPU.

Configurazione della rete

Usa le seguenti informazioni per verificare che le tue configurazioni di rete AWS, Microsoft Windows e locale (o locale) non blocchino l'accesso all'istanza.

AWS configurazione di rete

Configurazione	Verifica
Configurazione del gruppo di sicurezza	Verifica che la porta 3389 sia aperta per il gruppo di sicurezza. Verifica che ti stai collegando all'indirizzo IP pubblico corretto. Se l'istanza non è stata associata a un IP elastico, l'IP pubblico cambia dopo l'arresto/avvio dell'istanza. Per ulteriori informazioni, consulta Il desktop remoto non può connettersi al computer remoto.
Configurazione VPC (liste di controllo degli accessi di rete)	Verifica che la lista di controllo accessi (ACL) del tuo Amazon VPC non stia bloccando l'accesso. Per informazioni, consulta Liste di

Configurazione	Verifica
	controllo degli accessi di rete nella Guida per l'utente di Amazon VPC.
Configurazione VPN	Se ti stai connettendo al VPC tramite una rete privata virtuale (VPN), verifica la connettività del tunnel della VPN. Per ulteriori informazioni, consulta l'articolo che illustra in che modo risolvere i problemi di connettività del tunnel della VPN a un Amazon VPC?.

Configurazione di rete Windows

Configurazione	Verifica
Windows Firewall	Verifica che Windows Firewall non stia bloccando le connessioni alla istanza. Disabilita Windows Firewall come descritto al punto 7 della sezione di risoluzione dei problemi del desktop remoto, Il desktop remoto non può connettersi al computer remoto.
Configurazione TCP/IP avanzata (utilizzo di un IP statico)	L'istanza potrebbe non rispondere perché hai configurato un indirizzo IP statico. Per un VPC, creare un'interfaccia di rete e collegarla all'istanza.

Configurazione di rete locale o on-premise

Verifica che una configurazione di rete locale non stia bloccando l'accesso. Prova a connetterti a un'altra istanza nello stesso VPC dell'istanza irraggiungibile. Se non riesci ad accedere a un'altra istanza, contatta il tuo amministratore di rete locale per stabilire se una policy locale limita l'accesso.

Problema correlato ai Servizi Desktop remoto

Se l'istanza diventa irraggiungibile durante l'accesso, potrebbe esserci un problema relativo ai Servizi Desktop remoto (RDS) nell'istanza.

> **Tip**
>
> Puoi utilizzare il runbook `AWSSupport-TroubleshootRDP` per verificare e modificare varie impostazioni che potrebbero influire sulle connessioni RDP (Remote Desktop Protocol). Per ulteriori informazioni, consulta `AWSSupport-TroubleshootRDP` in Documentazione di riferimento del runbook di AWS Systems Manager Automation.

Configurazione dei Servizi Desktop remoto

Configurazione	Verifica
RDS in esecuzione	Verificare che RDS sia in esecuzione sull'istanza. Connettiti all'istanza tramite l'applicazione Servizi di Microsoft Managemen t Console (MMC) (`services.msc`). Nell'elenco dei servizi verificare che Remote Desktop Services (Servizi Desktop remoto) sia Running (In esecuzione). In caso contrario, avviarli e impostare il tipo di avvio su Automatic (Automatico). Se non è possibile connettersi all'istanza utilizzando l'applicazione Servizi, distaccare il volume root dall'istanza, acquisire uno snapshot del volume o creare un'AMI da esso, collegare il volume originale a un'altra istanza nella stessa zona di disponibilità come volume secondario e modificare la chiave di registro Start. Una volta terminato, ricollega il volume radice all'istanza originale.
RDS abilitato	Anche se il servizio è avviato, potrebbe essere disabilitato. Distacca il volume root dall'istanza, acquisisci una snapshot del volume o crea un'AMI da esso, collega il volume originale a un'altra istanza nella stessa zona di disponibilità come volume secondario e abilita il servizio modificando la chiave di registro Terminal Server come descritto in Abilitazione di Desktop remoto in un'istanza EC2 con il Registro di sistema remoto: Una volta terminato, ricollega il volume radice all'istanza originale.

Elevato utilizzo della CPU

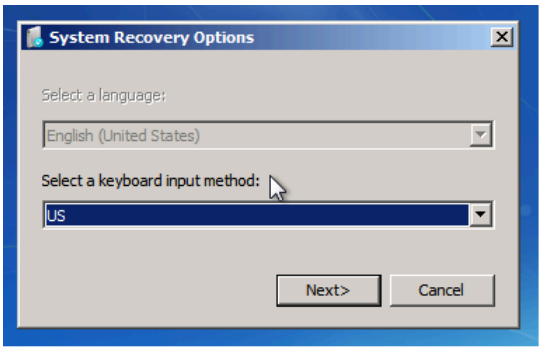
Controlla la metrica di utilizzo della CPU (massimo) sulla tua istanza utilizzando Amazon. CloudWatch Se il valore CPUUtilization (Maximum) è un numero elevato, attendere che si abbassi e riprovare. Un utilizzo elevato della CPU può essere causato da:

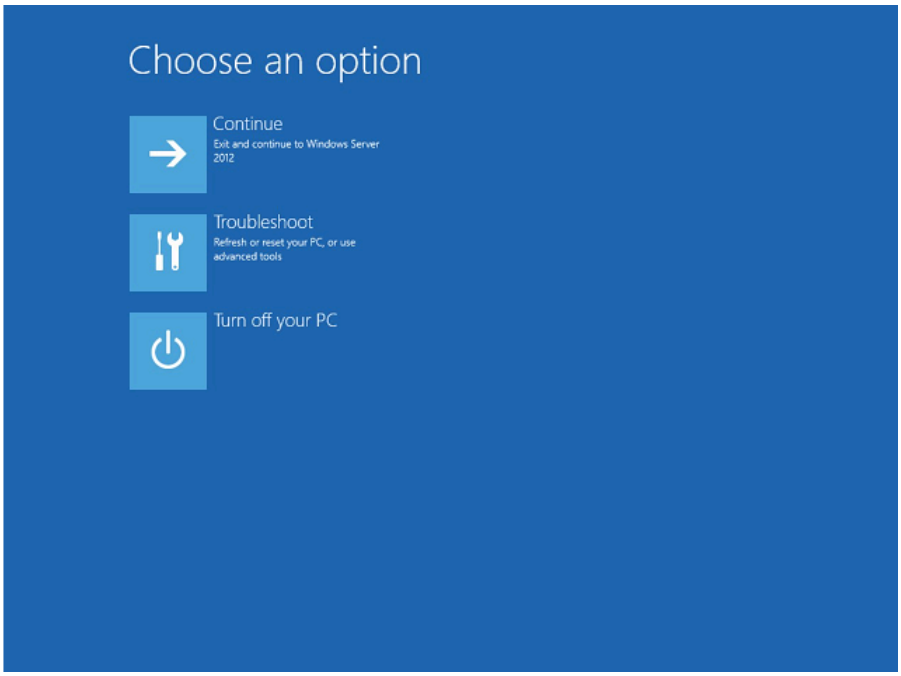
- Windows Update
- Scansione del software di sicurezza
- Script di avvio personalizzato
- Pianificatore di attività

Per ulteriori informazioni, consulta Ottieni statistiche per una risorsa specifica nella Amazon CloudWatch User Guide. Per ulteriori suggerimenti per la risoluzione di problemi, consulta Utilizzo elevato della CPU poco dopo l'avvio di Windows (solo istanze Windows).

Schermata della console di ripristino

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.





Se `bootstatuspolicy` non è impostato su `ignoreallfailures`, il sistema operativo potrebbe avviarsi nella console di ripristino e restare bloccato in questo stato. Utilizza la procedura seguente per cambiare la configurazione `bootstatuspolicy` in `ignoreallfailures`.

Per impostazione predefinita, la configurazione delle policy per le AMI Windows pubbliche fornita da AWS è impostata su. `ignoreallfailures`

1. Arrestare l'istanza irraggiungibile.
2. Creare una snapshot del volume root. Il volume root è collegato all'istanza come `/dev/sda1`.

   Distacca il volume root dall'istanza irraggiungibile, acquisisci una snapshot del volume o crea un'AMI da esso, quindi collegalo a un'altra istanza nella stessa zona di disponibilità come volume secondario.

   > **Warning**
   >
   > Se la tua istanza temporanea e l'istanza originale sono state avviate utilizzando la stessa AMI, dovrai completare altre operazioni o non sarai in grado di avviare l'istanza originale dopo aver ripristinato il volume root a causa di un conflitto di firme del disco. Se devi creare un'istanza temporanea utilizzando la stessa AMI, completa le operazioni in Collisione della firma del disco per evitare un conflitto di firma del disco.
   > In alternativa, seleziona un'AMI diversa per l'istanza temporanea. Ad esempio, se l'istanza originale utilizza un'AMI per Windows Server 2016, avvia l'istanza temporanea utilizzando un'AMI per Windows Server 2019.

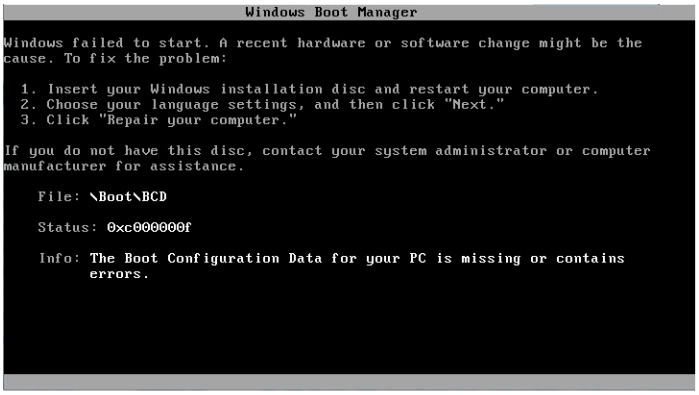
3. Accedi all'istanza ed emetti il comando seguente da un prompt di comandi per modificare la configurazione di `bootstatuspolicy` in `ignoreallfailures`.

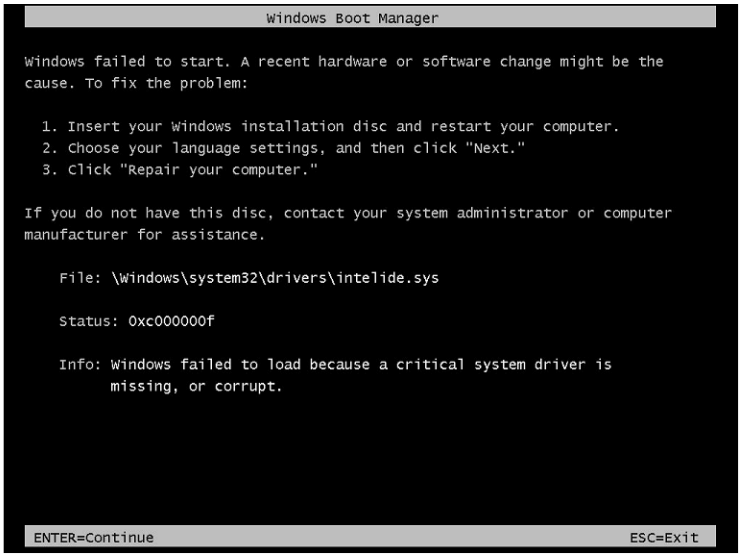
   ```
   bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy
    ignoreallfailures
   ```

4. Ricollegare il volume all'istanza irraggiungibile e avviare nuovamente l'istanza.

Schermata Windows Boot Manager

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.

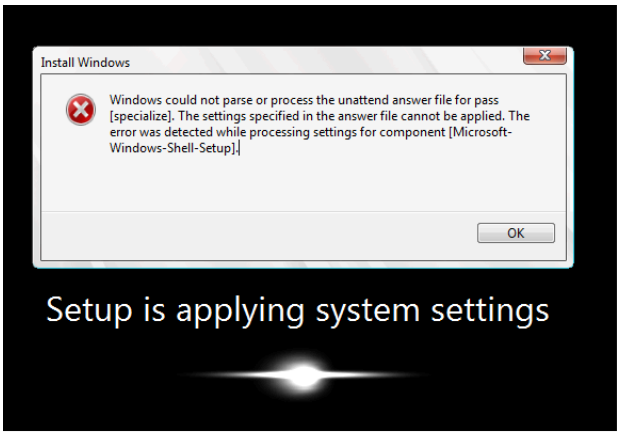


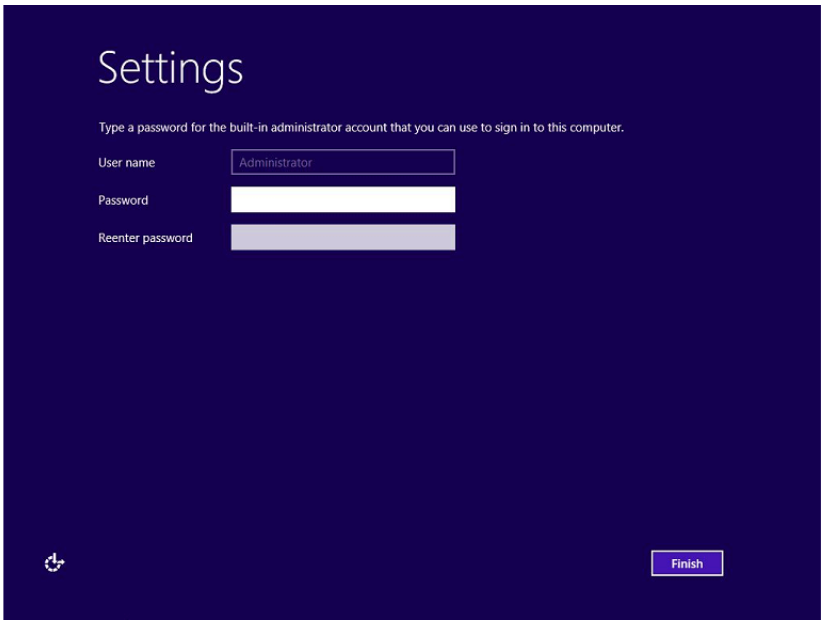


Il sistema operativo ha subito un danno irreversibile nel file di sistema e/o registro. Quando un'istanza è bloccata in questo stato, puoi recuperarla da un'AMI di backup recente o avviare un'istanza di sostituzione. Se è necessario accedere ai dati dell'istanza, distacca qualsiasi volume root dall'istanza irraggiungibile, acquisisci una snapshot di tali volumi o crea un'AMI da essi, quindi collegali a un'altra istanza nella stessa zona di disponibilità come volume secondario.

Schermata Sysprep

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.



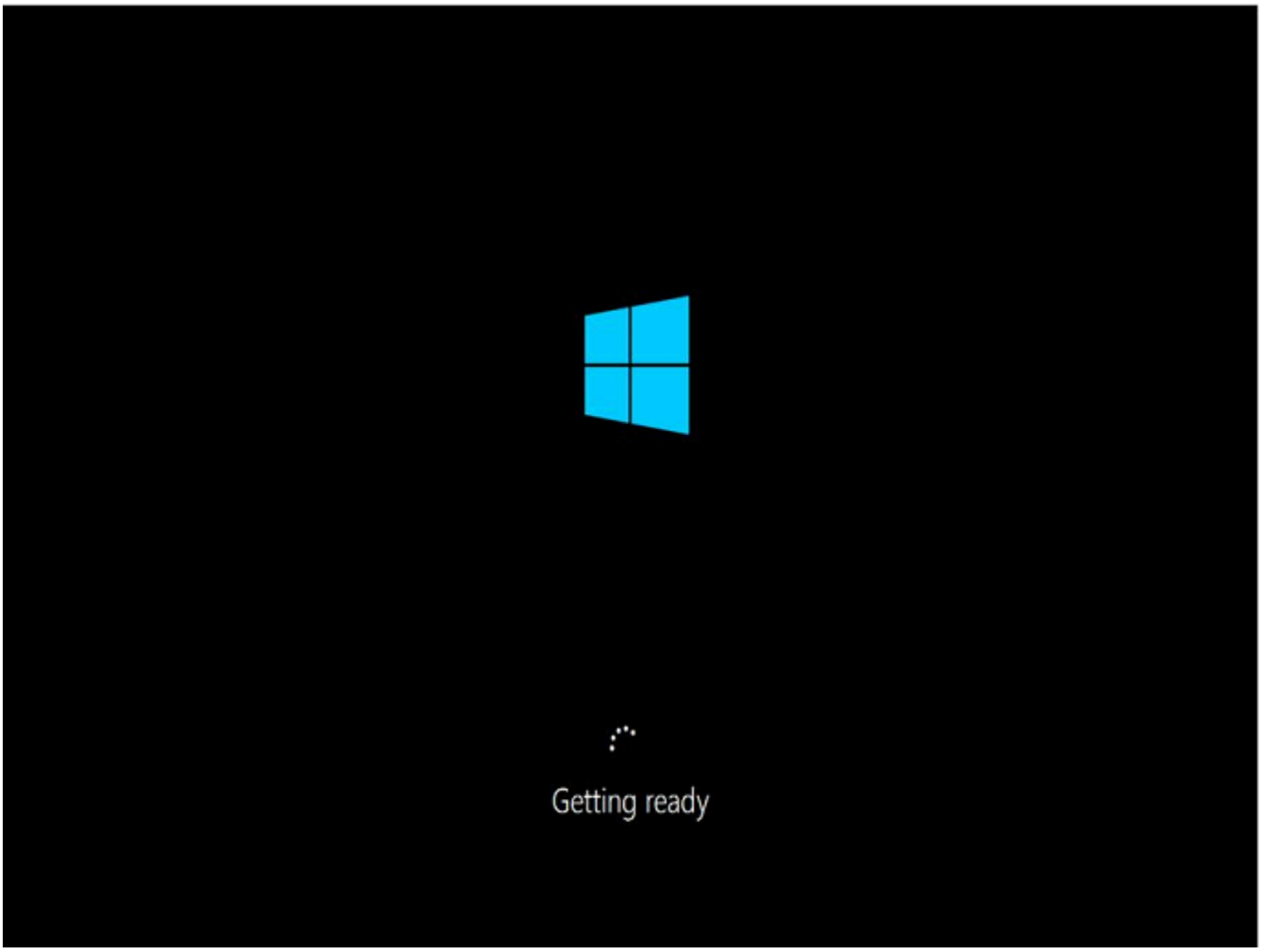


Potresti visualizzare questa schermata se non hai utilizzato il servizio EC2Config per chiamare Sysprep o se il sistema operativo ha riscontrato un errore nell'esecuzione di Sysprep. È possibile

reimpostare la password utilizzando EC2Rescue. In caso contrario, consulta Creare un'AMI con Windows Sysprep.

Schermata di preparazione

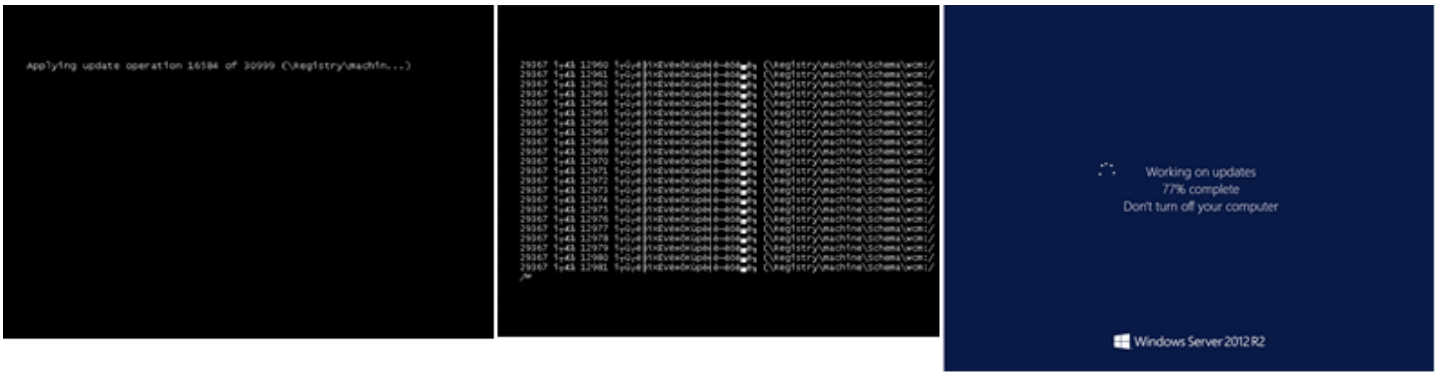
Il servizio di acquisizione di screenshot della console ha restituito quanto segue.



Aggiorna il servizio di acquisizione di screenshot della console dell'istanza ripetutamente per verificare che l'anello di avanzamento stia girando. In tal caso, attendi che il sistema operativo si avvii. Puoi anche controllare la metrica di utilizzo della CPU (massimo) sulla tua istanza utilizzando Amazon CloudWatch per vedere se il sistema operativo è attivo. Se l'anello di avanzamento non sta girando, l'istanza potrebbe essere bloccata a livello del processo di avvio. Riavviare l'istanza. Se il riavvio non risolve il problema, recupera l'istanza da un'AMI di backup recente o avvia un'istanza di sostituzione. Se è necessario accedere ai dati dell'istanza, distacca il volume root dall'istanza irraggiungibile, acquisisci una snapshot del volume o crea un'AMI da esso. Quindi, collegalo a un'altra istanza nella stessa zona di disponibilità come volume secondario.

Schermata Windows Update

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.

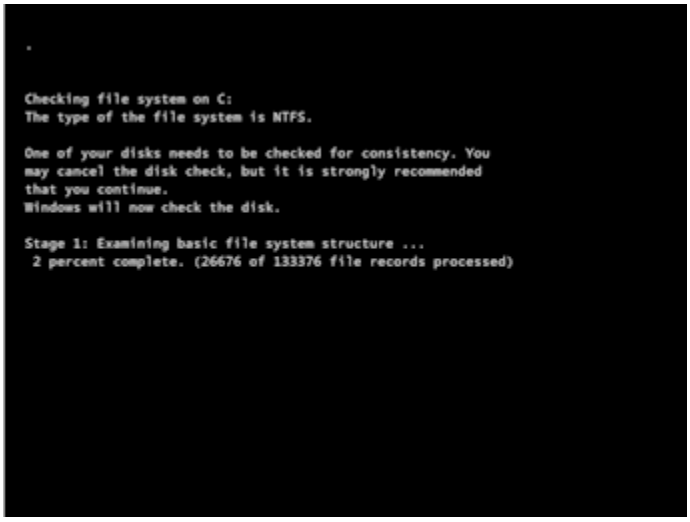


Il processo Windows Update sta aggiornando il registro. Attendi la fine dell'aggiornamento. Non riavviare o arrestare l'istanza perché ciò potrebbe danneggiare i dati durante l'aggiornamento.

> **Note**
>
> Il processo Windows Update può utilizzare le risorse sul server durante l'aggiornamento. Se riscontri spesso questo problema, considera la possibilità di usare tipi di istanza e volumi EBS più veloci.

Chkdsk

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.



Windows sta eseguendo lo strumento di sistema chkdsk sull'unità per verificare l'integrità del file system e correggerne gli errori logici Attendi il completamento del processo.

Ripristino delle istanze in caso di errori del computer host

Se si presenta un problema irrecuperabile con l'hardware di un computer host sottostante, è possibile che AWS pianifichi un evento di arresto delle istanze. Tale evento ti viene notificato in anticipo tramite e-mail.

Per ripristinare un'istanza supportata da Amazon EBS in esecuzione su un computer host in stato di errore

1. Eseguire il backup di tutti i dati importanti contenuti nei volumi instance store in Amazon EBS o Amazon S3.
2. Arrestare l'istanza.
3. Avviare l'istanza.
4. Ripristinare i dati importanti.

Per ulteriori informazioni, consulta Arresta e avvia le istanze Amazon EC2.

Per ripristinare un'istanza supportata da instance store in esecuzione su un computer host in stato di errore

1. Creare un'AMI dall'istanza.
2. Caricare l'immagine su Amazon S3.
3. Eseguire il backup dei dati importanti in Amazon EBS o Amazon S3.
4. Terminare l'istanza.
5. Avviare una nuova istanza dall'AMI.
6. Ripristinare i dati importanti sulla nuova istanza.

Risoluzione dei problemi di arresto dell'istanza

Se è stata arrestata un'istanza supportata da Amazon EBS e questa appare bloccata nello stato `stopping`, è possibile che vi sia un problema con il computer host sottostante.

Non viene addebitato alcun costo per l'utilizzo dell'istanza se questa non si trova nello stato `stopping` o in qualsiasi altro stato, tranne `running`. I costi per l'utilizzo dell'istanza vengono addebitati solo quando un'istanza è nello stato `running`.

Forzare l'arresto dell'istanza

Forzare l'istanza per arrestarla utilizzando la console o l AWS CLI.

> **Note**
>
> È possibile forzare un'istanza a interrompere l'utilizzo della console solo mentre l'istanza è nello stato `stopping`. È possibile forzare un'istanza a interrompere l'utilizzo della AWS CLI mentre l'istanza è in uno stato qualsiasi, tranne `shutting-down` e `terminated`.

Console

Per forzare l'arresto dell'istanza utilizzando la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza bloccata.
3. Scegliere Instance state (Stato istanza), quindi Force stop instance (Forza arresto istanza) e Stop (Arresta).

   Nota che Force stop instance (Forza arresto istanza) è disponibile solo nella console se l'istanza è nello stato `stopping`. Se la tua istanza si trova in un altro stato (tranne `shutting-down eterminated`) puoi usare AWS CLI per forzare l'arresto dell'istanza.

AWS CLI

Per forzare l'arresto dell'istanza, utilizzare il AWS CLI

Utilizzare il comando stop-instances e l'opzione `--force` come segue:

```
aws ec2 stop-instances --instance-ids i-0123ab456c789d01e --force
```

Se dopo 10 minuti l'istanza non si è arrestata, pubblica una richiesta di assistenza su AWS re:Post. Per velocizzare la risoluzione, includere l'ID dell'istanza e descrivere le fasi già eseguite. In

alternativa, se si dispone di un piano di supporto, creare un caso di supporto tecnico presso il Centro di supporto.

Creare un'istanza sostitutiva

Per tentare di risolvere il problema in attesa di assistenza da AWS re:Post o dal Centro di supporto, crea un'istanza sostitutiva. Creare un AMI dell'istanza bloccata e avviare una nuova istanza utilizzando la nuova AMI.

> **Important**
>
> La creazione di un'istanza sostitutiva è consigliata se si registrano solo i controlli di stato del sistema, poiché i controlli dello stato delle istanze comporteranno la copia dell'AMI su una replica esatta del sistema operativo danneggiato. Dopo aver confermato il messaggio di stato, crea l'AMI e avvia una nuova istanza utilizzando la nuova AMI.

Console

Per creare un'istanza sostitutiva utilizzando la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza bloccata.
3. Scegliere Actions (Operazioni), Image and templates (Immagine e modelli), Create image (Crea immagine).
4. Nella pagina Create image (Crea un'immagine), eseguire le operazioni seguenti:
   a. Immettere un nome e una descrizione per l'AMI.
   b. Scegliere No reboot (Non riavviare).
   c. Scegliere Create Image (Crea immagine).

   Per ulteriori informazioni, consulta the section called “Creare un AMI da un'istanza”.
5. Avviare una nuova istanza dall'AMI e verificare che funzioni.
6. Selezionare l'istanza bloccata e scegliere Actions (Operazioni), Instance state (Stato istanza), Terminate instance (Termina istanza). Se l'istanza si blocca anche durante il processo di terminazione, Amazon EC2 la forza automaticamente perché termini entro poche ore.

AWS CLI

Per creare un'istanza sostitutiva utilizzando la CLI

1. Creare un'AMI dall'istanza bloccata utilizzando il comando create-image (AWS CLI) e l'opzione `--no-reboot` come segue:

```
aws ec2 create-image --instance-id i-0123ab456c789d01e --name "AMI" --
description "AMI for replacement instance" --no-reboot
```

2. Avviare una nuova istanza dall'AMI utilizzando il comando run-instances (AWS CLI) come segue:

```
aws ec2 run-instances --image-id ami-1a2b3c4d --count 1 --instance-type c3.large
 --key-name MyKeyPair --security-groups MySecurityGroup
```

3. Verificare che la nuova istanza funzioni.
4. Terminare l'istanza bloccata utilizzando il comando terminate-instances (AWS CLI) come segue:

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

Se non è possibile creare un'AMI dall'istanza come descritto nella procedura precedente, è possibile configurare un'istanza sostitutiva come segue:

(In alternativa) Per creare un'istanza sostitutiva utilizzando la console

1. Selezionare l'istanza e scegliere Description (Descrizione), Block devices (Dispositivi a blocchi). Selezionare ciascun volume e prendere nota del relativo ID del volume. Accertarsi di annotarsi il volume root.
2. Nel riquadro di navigazione, selezionare Volumes (Volumi). Selezionare ogni volume dell'istanza e scegliere Actions (Operazioni), Create Snapshot (Crea snapshot).
3. Nel riquadro di navigazione, selezionare Snapshots (Snapshot). Selezionare la snapshot appena creata, quindi scegliere Actions (Operazioni), Create Volume (Crea volume).
4. Avviare un'istanza con lo stesso sistema operativo di quella bloccata. Prendere nota dell'ID del volume e del nome del dispositivo del relativo volume root.

5. Nel riquadro di navigazione scegliere Instances (Istanze), selezionare l'istanza appena avviata, scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).
6. Nel riquadro di navigazione scegliere Volumes (Volumi), selezionare il volume root dall'istanza arrestata, quindi scegliere Actions (Operazioni), Detach Volume (Distacca volume).
7. Selezionare il volume root creato a partire dall'istanza bloccata, scegliere Actions (Operazioni), Attach Volume (Collega volume), quindi collegarlo alla nuova istanza come suo volume root (utilizzando il nome del dispositivo di cui si è preso nota). Collegare eventuali altri volumi non root all'istanza.
8. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza sostitutiva. Scegli Instance state (Stato istanza), Start instance (Avvia istanza). Verificare che l'istanza funzioni.
9. Seleziona l'istanza bloccata e scegli Instance state (Stato istanza), Terminate instance (Termina istanza). Se l'istanza si blocca anche durante il processo di terminazione, Amazon EC2 la forza automaticamente perché termini entro poche ore.

Risoluzione dei problemi relativi alla terminazione delle istanze (arresto)

Non viene addebitato alcun costo per l'utilizzo di un'istanza se questa non si trova nello stato `running`. In altre parole, quando un'istanza viene terminata, non appena il suo stato passa a non viene più addebitato alcun cost `shutting-down`.

Terminazione immediata dell'istanza

All'avvio, diversi problemi possono causare la chiusura immediata dell'istanza. Per ulteriori informazioni, consulta Terminazione immediata dell'istanza.

Ritardo della terminazione dell'istanza

Se l'istanza rimane nello stato `shutting-down` più a lungo di alcuni minuti, è possibile che subisca un ritardo dovuto all'esecuzione degli script di chiusura da parte dell'istanza stessa.

Un'altra possibile causa è un problema con il computer host sottostante. Se l'istanza rimane nello stato `shutting-down` per molte ore, Amazon EC2 la considera come un'istanza bloccata e ne forza la terminazione.

Se la terminazione dell'istanza si blocca e rimane in questa condizione per molte ore, pubblica una richiesta di assistenza su AWS re:Post. Per velocizzare la risoluzione, includere l'ID dell'istanza e descrivere le fasi già eseguite. In alternativa, se si dispone di un piano di supporto, creare un caso di supporto tecnico presso il Centro di supporto.

L'istanza terminata rimane visualizzata

Dopo essere stata terminata, un'istanza rimane visibile per un breve periodo prima di essere eliminata. Lo stato indicato è `terminated`. Se dopo molte questa voce non viene eliminata, contattare il supporto.

Errore: l'istanza non può essere terminata. Modifica il suo attributo di istanza disableApiTermination "

Quando provi a terminare un'istanza, appare il messaggio di errore `The instance instance_id may not be terminated. Modify its 'disableApiTermination' instance attribute` nel quale è indicato che l'istanza è stata abilitata per la protezione da terminazione. La protezione da terminazione impedisce la terminazione involontaria dell'istanza. Per ulteriori informazioni, consulta Abilitare la protezione da cessazione.

Per terminare l'istanza, devi innanzitutto disabilitare tale protezione.

Per disabilitare la protezione da terminazione utilizzando la console Amazon EC2, seleziona l'istanza, quindi scegli Operazioni, Impostazioni dell'istanza, Cambia la protezione da terminazione.

Per disabilitare la protezione dalla terminazione utilizzando il AWS CLI, utilizzare il comando seguente.

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-disable-api-
termination
```

Istanze avviate o terminate automaticamente

In genere i seguenti comportamenti indicano che sono stati utilizzati Amazon EC2 Auto Scaling, un parco istanze EC2 o un parco istanze Spot per dimensionare automaticamente le risorse di calcolo in base ai criteri che hai definito:

- Termina un'istanza e una nuova istanza viene avviata automaticamente.
- Avvia un'istanza e una delle istanze viene terminata automaticamente.

- Arresta un'istanza e terminala e una nuova istanza viene avviata automaticamente.

Per arrestare il dimensionamento automatico, consulta la Guida per l'utente di Amazon EC2 Auto Scaling, EC2 Fleet o Creare una richiesta di parco istanze spot.

Risolvi i problemi relativi alle istanze Linux con controlli di stato non riusciti

> **Note**
>
> Questo argomento si applica solo alle istanze Linux.

Le seguenti informazioni possono aiutarti a risolvere i problemi se la tua istanza Linux non supera il controllo dello stato. Determina innanzitutto se le applicazioni in uso presentano dei problemi. Se risulta che l'istanza non esegue le applicazioni come previsto, esamina le informazioni di verifica dello stato e i log di sistema.

Per vedere degli esempi di problemi che causano il mancato superamento dei controlli dello stato, vedere Verifiche dello stato delle istanze.

Indice

- fsck: No such file or directory while trying to open... file system non trovato
- General error mounting filesystems (errore di montaggio)
- VFS: Unable to mount root fs on unknown-block (mancata corrispondenza del file system root)
- Error: Unable to determine major/minor number of root device... (mancata corrispondenza file system/dispositivo root)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (verifica del file system richiesta)
- fsck died with exit status... (dispositivo mancante)
- Prompt di GRUB (grubdom>)
- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (indirizzo MAC hardcoded)
- Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (configurazione SELinux errata)
- XENBUS: Timeout connecting to devices (timeout di Xenbus)

Esame delle informazioni di verifica dello stato

Per analizzare le istanze danneggiate utilizzando la console di Amazon EC2

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e seleziona l'istanza desiderata.
3. Nel riquadro dei dettagli scegliere Stato e allarmi per visualizzare i singoli risultati di tutte le Verifiche dello stato del sistema e le Verifiche dello stato delle istanze.

Se una verifica dello stato del sistema ha avuto esito negativo, provare una delle seguenti opzioni:

- Creare un allarme di ripristino istanze. Per ulteriori informazioni, consulta Creazione di allarmi che arrestano, terminano, riavviano o recuperano un'istanza.
- Se hai cambiato il tipo di istanza con un'istanza basata sul sistema AWS Nitro, i controlli di stato hanno esito negativo se hai eseguito la migrazione da un'istanza che non dispone dei driver ENA e NVMe richiesti. Per ulteriori informazioni, consulta Compatibilità per la modifica del tipo di istanza.
- Arrestare e riavviare un'istanza se utilizza un'AMI supportata da Amazon EBS.
- Terminare un'istanza e avviarne una sostitutiva se utilizza un'AMI supportata da instance store.

- Attendere che Amazon EC2 risolva il problema.
- Pubblica un post relativo alla tua problematica su AWS re:Post.
- Se l'istanza è in un gruppo Auto Scaling, il servizio Amazon EC2 Auto Scaling avvia automaticamente un'istanza in sostituzione. Per ulteriori informazioni, consulta Controlli dello stato per le istanze Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.
- Recuperare il log di sistema e individuare eventuali errori.

Recupero dei log di sistema

Se la verifica dello stato di un'istanza ha esito negativo, è possibile riavviare l'istanza e recuperare i log di sistema. Questi log possono rivelare la presenza di un errore che può aiutare a risolvere il problema. Il riavvio elimina le informazioni inutili dai log.

Per riavviare un'istanza e recuperare il log di sistema

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza desiderata.
3. Scegliere Instance state (Stato istanza), Reboot instance (Riavvia istanza). Per il riavvio dell'istanza possono essere necessari alcuni minuti.
4. Verificare se il problema è ancora presente; talvolta il riavvio consente di risolvere il problema.
5. Quando l'istanza è in stato `running`, selezionare Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), Get system log (Ottieni il log di sistema).
6. Esaminare il log visualizzato e utilizzare l'elenco delle dichiarazioni di errore note del log di sistema per risolvere il problema.
7. Se la problematica non si risolve, puoi pubblicare un post relativo a tale problematica su AWS re:Post.

Risolvi gli errori del registro di sistema per le istanze Linux

Per le istanze Linux che non hanno superato un controllo dello stato dell'istanza, ad esempio il controllo di raggiungibilità dell'istanza, verifica di aver seguito i passaggi precedenti per recuperare il registro di sistema. L'elenco seguente contiene alcuni errori comuni del log di sistema e suggerisce alcune operazioni che potrebbero risolvere il problema di ogni errore.

Errori di memoria

- Out of memory: kill process
- ERROR: mmu_update failed (aggiornamento della gestione della memoria non riuscito)

Errori dei dispositivi

- I/O Error (errore dei dispositivi a blocchi)
- I/O ERROR: neither local nor remote disk (rottura del dispositivo a blocchi distribuito)

Errori del kernel

- request_module: runaway loop modprobe (looping del modprobe del kernel legacy sulle versioni precedenti di Linux)
- "FATAL: kernel too old" e "fsck: No such file or directory while trying to open /dev" (mancata corrispondenza di kernel e AMI)
- «FATAL: impossibile caricare /lib/modules" o "BusyBox" (moduli del kernel mancanti)
- ERROR Invalid kernel (kernel non compatibile con EC2)

Errori del file system

- fsck: No such file or directory while trying to open... file system non trovato
- General error mounting filesystems (errore di montaggio)
- VFS: Unable to mount root fs on unknown-block (mancata corrispondenza del file system root)
- Error: Unable to determine major/minor number of root device... (mancata corrispondenza file system/dispositivo root)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (verifica del file system richiesta)
- fsck died with exit status... (dispositivo mancante)

Errori del sistema operativo

- Prompt di GRUB (grubdom>)
- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (indirizzo MAC hardcoded)

- Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (configurazione SELinux errata)
- XENBUS: Timeout connecting to devices (timeout di Xenbus)

Out of memory: kill process

Un out-of-memory errore viene indicato da una voce del registro di sistema simile a quella mostrata di seguito.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

Causa potenziale

Memoria esaurita

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Scegliere una delle seguenti operazioni: • Arrestare l'istanza e modificarla per utilizzar ne un tipo diverso, quindi avviare nuovament e l'istanza. Ad esempio un tipo di istanza più grande o ottimizzata per la memoria. • Riavviare l'istanza affinché torni a uno stato non danneggiato. Se non si cambia il tipo di istanza, probabilmente il problema si ripeterà.
Supportata da instance store	Scegliere una delle seguenti operazioni: • Terminare l'istanza e avviarne una nuova, specificando un tipo di istanza diverso. Ad esempio un tipo di istanza più grande o ottimizzata per la memoria.

Per questo tipo di istanza	Eseguire questa operazione
	• Riavviare l'istanza affinché torni a uno stato non danneggiato. Se non si cambia il tipo di istanza, probabilmente il problema si ripeterà.

ERROR: mmu_update failed (aggiornamento della gestione della memoria non riuscito)

Gli errori relativi all'aggiornamento della gestione della memoria sono indicati da una voce del log di sistema simile alla seguente:

```
...
Press `ESC' to enter the menu... 0   [H[J  Booting 'Amazon Linux 2011.09
 (2.6.35.14-95.38.amzn1.i686)'


root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=

en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

Causa potenziale

Problema con Amazon Linux

Operazione suggerita

Pubblicare il problema sui forum per sviluppatori oppure contattare AWS Support.

I/O Error (errore dei dispositivi a blocchi)

Un errore di ingressi/uscite viene indicato da una voce del log di sistema simile all'esempio riportato di seguito:

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

Cause potenziali

Tipo di istanza	Causa potenziale
Supportata da Amazon EBS	Un volume Amazon EBS in stato di errore
Supportata da instance store	Un'unità fisica in stato di errore

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Attenersi alla seguente procedura:

Per questo tipo di istanza	Eseguire questa operazione
	1. Arrestare l'istanza. 2. Distaccare il volume. 3. Tentare di ripristinare il volume. **Note** È buona norma eseguire spesso una snapshot dei volumi Amazon EBS per ridurre notevolmente il rischio di perdite di dati dovuti a guasti. 4. Ricollegare il volume all'istanza. 5. Avviare l'istanza.
Supportata da instance store	Terminare l'istanza e avviarne una nuova. **Note** Non è possibile ripristinare i dati. Eseguire il ripristino dai backup. **Note** Per i backup, è buona norma utilizzare Amazon S3 o Amazon EBS. I volumi instance store sono legati direttamente agli errori dei singoli host e dei singoli dischi.

I/O ERROR: neither local nor remote disk (rottura del dispositivo a blocchi distribuito)

Un errore di ingressi/uscite sul dispositivo viene indicato da una voce del log di sistema simile all'esempio riportato di seguito:

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

Cause potenziali

Tipo di istanza	Causa potenziale
Supportata da Amazon EBS	Un volume Amazon EBS in stato di errore
Supportata da instance store	Un'unità fisica in stato di errore

Operazione suggerita

Terminare l'istanza e avviarne una nuova.

Per un'istanza supportata da Amazon EBS, è possibile ripristinare i dati da una snapshot recente creando un'immagine a partire da essa. I dati eventualmente aggiunti dopo la snapshot non possono essere ripristinati.

request_module: runaway loop modprobe (looping del modprobe del kernel legacy sulle versioni precedenti di Linux)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto. L'utilizzo di un kernel Linux instabile o datato (ad esempio 2.6.16-xenU) può causare una condizione di loop interminabile all'avvio.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007

BIOS-provided physical RAM map:

 Xen: 0000000000000000 - 0000000026700000 (usable)

0MB HIGHMEM available.
...

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c
```

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Utilizzare un kernel più recente, basato su GRUB o statico, impiegando una delle opzioni seguenti: Opzione 1: terminare l'istanza e avviarne una nuova, specificando i parametri `-kernel` e `-ramdisk`. Opzione 2:

Per questo tipo di istanza	Eseguire questa operazione
	1. Arrestare l'istanza. 2. Modificare gli attributi di kernel e ramdisk per utilizzare un kernel più recente. 3. Avviare l'istanza.
Supportata da instance store	Terminare l'istanza e avviarne una nuova, specificando i parametri `-kernel` e `-ramdisk`.

"FATAL: kernel too old" e "fsck: No such file or directory while trying to open /dev" (mancata corrispondenza di kernel e AMI)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

Cause potenziali

Kernel e userland non compatibili

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Modificare la configurazione per utilizzare un kernel più recente. 3. Avviare l'istanza.

Per questo tipo di istanza	Eseguire questa operazione
Supportata da instance store	Attenersi alla seguente procedura: 1. Creare un'AMI che utilizza un kernel più recente. 2. Terminare l'istanza. 3. Avviare una nuova istanza dall'AMI creata.

«FATAL: impossibile caricare /lib/modules" o "BusyBox" (moduli del kernel mancanti)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or
 directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No
 such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device.  Common problems:
 - Boot args (cat /proc/cmdline)
   - Check rootdelay= (did the system wait long enough?)
   - Check root= (did the system wait for the right device?)
```

```
 - Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!


BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

Cause potenziali

Questo problema può essere causato da una o più delle condizioni seguenti:

- Ramdisk mancante
- Moduli corretti mancanti nel ramdisk
- Volume root Amazon EBS non collegato correttamente come `/dev/sda1`

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Attenersi alla seguente procedura: 1. Selezionare il ramdisk corretto per il volume Amazon EBS. 2. Arrestare l'istanza. 3. Distaccare il volume e ripararlo. 4. Collegare il volume all'istanza. 5. Avviare l'istanza. 6. Modificare l'AMI per utilizzare il ramdisk corretto;
Supportata da instance store	Attenersi alla seguente procedura:

Per questo tipo di istanza	Eseguire questa operazione
	1. Terminare l'istanza e avviarne una nuova con il ramdisk corretto. 2. Creare una nuova AMI con il ramdisk corretto.

ERROR Invalid kernel (kernel non compatibile con EC2)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
...
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'

root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

Cause potenziali

Questo problema può essere causato da una o entrambe le condizioni seguenti:

- Il kernel fornito non è supportato da GRUB

- Il kernel di fallback non esiste

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Sostituire con un kernel funzionante. 3. Installare un kernel di fallback. 4. Modificare l'AMI correggendo il kernel.
Supportata da instance store	Attenersi alla seguente procedura: 1. Terminare l'istanza e avviarne una nuova con il kernel corretto. 2. Creare un'AMI con il kernel corretto. 3. (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite AWS Support.

fsck: No such file or directory while trying to open... file system non trovato

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
  Welcome to Fedora
  Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [  OK  ]

Starting udev: [  OK  ]

Setting hostname localhost:  [  OK  ]

No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[  OK  ]
```

```
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]


*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

Cause potenziali

- È presente un bug nelle definizioni del file system del ramdisk /etc/fstab
- Le definizioni del file system non sono configurate correttamente in /etc/fstab
- Unità mancante o in stato di errore

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Attenersi alla seguente procedura: 1. Arrestare l'istanza, distaccare il volume root, riparare o modificare il file di configurazione /etc/fstab del volume, collegare il volume all'istanza e avviare l'istanza.

Per questo tipo di istanza	Eseguire questa operazione
	2. Correggere il ramdisk per includere il file /etc/fstab modificato (se applicabile). 3. Modificare l'AMI per utilizzare un ramdisk più recente. Il sesto campo nel file fstab definisce i requisiti di disponibilità del punto di montaggio (un valore diverso da zero implica l'esecuzione di un fsck su quel volume che deve avere esito positivo). L'uso di questo campo può risultare problematico in Amazon EC2 in quanto un errore solitamente comporta un prompt interatti vo della console che non è correntemente disponibile in Amazon EC2. Prestare attenzione a questa caratteristica e leggere la pagina man di Linux relativa al file fstab.
Supportata da instance store	Attenersi alla seguente procedura: 1. Terminare l'istanza e avviarne una nuova. 2. Distaccare eventuali volumi Amazon EBS errati e riavviare l'istanza. 3. (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite AWS Support.

General error mounting filesystems (errore di montaggio)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
```

```
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting.  Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

Cause potenziali

Tipo di istanza	Causa potenziale
Supportata da Amazon EBS	• Volume Amazon EBS distaccato o in stato di errore. • File system danneggiato. • Combinazione di ramdisk e AMI non corrispondente (ad esempio, ramdisk Debian con AMI SUSE).

Tipo di istanza	Causa potenziale
Supportata da instance store	• Unità in stato di errore. • File system danneggiato. • Combinazione di ramdisk e AMI non corrispondente (ad esempio, ramdisk Debian con AMI SUSE).

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Distaccare il volume root. 3. Collegare il volume root a un'istanza funzionante nota. 4. Esegui il controllo del file system (fsck -a /dev/...). 5. Correggere eventuali errori. 6. Distaccare il volume dall'istanza funzionante nota. 7. Collegare il volume all'istanza arrestata. 8. Avviare l'istanza. 9. Verificare di nuovo lo stato dell'istanza.
Supportata da instance store	Provare con una delle seguenti operazioni: • Avviare una nuova istanza. • (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite AWS Support.

VFS: Unable to mount root fs on unknown-block (mancata corrispondenza del file system root)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
 20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line:  root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

Cause potenziali

Tipo di istanza	Causa potenziale
Supportata da Amazon EBS	• Dispositivo non collegato correttamente. • Dispositivo root non collegato al punto corretto. • File system non nel formato previsto. • Uso del kernel legacy (come 2.6.16-XenU). • Aggiornamento recente del kernel sull'istanza (aggiornamento errato o bug dell'aggiornamento).
Supportata da instance store	Errore dei dispositivi hardware.

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Scegliere una delle seguenti operazioni: • Arrestare e riavviare l'istanza.

Per questo tipo di istanza	Eseguire questa operazione
	• Modificare il volume root da collegare al punto dispositivi corretto, possibilmente /dev/sda1 invece di /dev/sda. • Arrestare e modificare per usare un kernel moderno. • Per controllare i bug di aggiornamento noti, consultare la documentazione della distribuzione Linux in uso. Cambiare o reinstallare il kernel.
Supportata da instance store	Terminare l'istanza e avviarne una nuova utilizzando un kernel moderno.

Error: Unable to determine major/minor number of root device... (mancata corrispondenza file system/dispositivo root)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Cause potenziali

- Driver dispositivi a blocchi virtuali mancante o configurato in modo non corretto
- Conflitto di enumerazione dei dispositivi (sda versus xvda o sda invece di sda1)
- Scelta errata del kernel dell'istanza

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Distaccare il volume. 3. Correggere il problema di mappatura dei dispositivi. 4. Avviare l'istanza. 5. Modificare l'AMI per risolvere i problemi di mappatura dei dispositivi.
Supportata da instance store	Attenersi alla seguente procedura: 1. Creare una nuova AMI con la soluzione appropriata (mappare correttamente il dispositivo a blocchi). 2. Terminare l'istanza e avviarne una nuova dall'AMI creata.

XENBUS: Device with no driver...

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
```

```
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Cause potenziali

- Driver dispositivi a blocchi virtuali mancante o configurato in modo non corretto
- Conflitto di enumerazione dei dispositivi (sda versus xvda)
- Scelta errata del kernel dell'istanza

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Distaccare il volume. 3. Correggere il problema di mappatura dei dispositivi. 4. Avviare l'istanza. 5. Modificare l'AMI per risolvere i problemi di mappatura dei dispositivi.
Supportata da instance store	Attenersi alla seguente procedura: 1. Creare un'AMI con la soluzione appropria ta (mappare correttamente il dispositivo a blocchi).

Per questo tipo di istanza	Eseguire questa operazione
	2. Terminare l'istanza e avviarne una nuova utilizzando l'AMI creata.

... days without being checked, check forced (verifica del file system richiesta)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

Cause potenziali

Il momento della verifica del file system è trascorso; viene forzata una verifica del file system.

Operazioni suggerite

- Attendere il completamento della verifica del file system. Una verifica del file system può richiedere molto tempo a seconda delle dimensioni del file system root.
- Modificare i file system per rimuovere l'applicazione della relativa verifica (fsck) utilizzando tune2fs o strumenti appropriati al file system in uso.

fsck died with exit status... (dispositivo mancante)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Cleaning up ifupdown....
Loading kernel modules...done.
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
```

```
[31mfailed (code 8).[39;49m
```

Cause potenziali

- Ramdisk in cerca di unità mancante
- Verifica di consistenza del file system forzata
- Unità in stato di errore o distaccata

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Tentare una o più delle operazioni seguenti per risolvere il problema: • Arrestare l'istanza e collegare il volume a un'istanza in esecuzione esistente. • Eseguire manualmente le verifiche di coerenza. • Correggere il ramdisk per includere le utility pertinenti. • Modificare i parametri di ottimizzazione del file system per rimuovere i requisiti di coerenza (operazione non consigliata).
Supportata da instance store	Tentare una o più delle operazioni seguenti per risolvere il problema: • Ricompilare il ramdisk con gli strumenti corretti. • Modificare i parametri di ottimizzazione del file system per rimuovere i requisiti di coerenza (operazione non consigliata). • Terminare l'istanza e avviarne una nuova.

Per questo tipo di istanza	Eseguire questa operazione
	• (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite AWS Support.

Prompt di GRUB (grubdom>)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
    GNU GRUB  version 0.97  (629760K lower / 0K upper memory)

       [ Minimal BASH-like line editing is supported.   For

         the   first   word,  TAB  lists  possible  command

         completions.  Anywhere else TAB lists the possible

         completions of a device/filename. ]

grubdom>
```

Cause potenziali

Tipo di istanza	Cause potenziali
Supportata da Amazon EBS	• File di configurazione GRUB mancante. • Utilizzata immagine GRUB errata, in attesa di file di configurazione GRUB in un percorso diverso. • Usato file system non supportato per archiviare il file di configurazione GRUB (ad esempio, conversione del file system root in un tipo non supportato da una precedente versione di GRUB).
Supportata da instance store	• File di configurazione GRUB mancante.

Tipo di istanza	Cause potenziali
	• Utilizzata immagine GRUB errata, in attesa di file di configurazione GRUB in un percorso diverso. • Usato file system non supportato per archiviare il file di configurazione GRUB (ad esempio, conversione del file system root in un tipo non supportato da una precedente versione di GRUB).

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Opzione 1: modificare l'AMI e riavviare l'istanza: 1. Modificare l'AMI di origine per creare un file di configurazione GRUB nel percorso standard (/boot/grub/menu.lst). 2. Verificare che la versione in uso di GRUB supporti il tipo di file system sottostante e, se necessario, aggiornare GRUB. 3. Scegliere l'immagine GRUB appropriata (hd0-1a unità o hd00 – 1a unità, 1a partizione). 4. Terminare l'istanza e avviarne una nuova utilizzando l'AMI creata. Opzione 2: correggere l'istanza esistente: 1. Arrestare l'istanza. 2. Distaccare il file system root. 3. Collegare il file system root a un'istanza funzionante nota.

Per questo tipo di istanza	Eseguire questa operazione
	4. Montare il file system. 5. Creare un file di configurazione GRUB. 6. Verificare che la versione in uso di GRUB supporti il tipo di file system sottostante e, se necessario, aggiornare GRUB. 7. Distaccare il file system. 8. Collegare all'istanza originale. 9. Modificare l'attributo del kernel per utilizzare l'immagine GRUB appropriata (1a unità o 1a partizione sul 1° disco). 10 Avviare l'istanza.
Supportata da instance store	Opzione 1: modificare l'AMI e riavviare l'istanza: 1. Creare la nuova AMI con un file di configurazione GRUB nel percorso standard (/boot/grub/menu.lst). 2. Scegliere l'immagine GRUB appropriata (hd0-1a unità o hd00 – 1a unità, 1a partizione). 3. Verificare che la versione in uso di GRUB supporti il tipo di file system sottostante e, se necessario, aggiornare GRUB. 4. Terminare l'istanza e avviarne una nuova utilizzando l'AMI creata. Opzione 2: terminare l'istanza e avviarne una nuova specificando il kernel corretto. **Note** Per ripristinare i dati dell'istanza esistente, contatta AWS Support.

Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (indirizzo MAC hardcoded)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
...
Bringing up loopback interface:  [  OK  ]

Bringing up interface eth0:  Device eth0 has different MAC address than expected,
 ignoring.
[FAILED]

Starting auditd: [  OK  ]
```

Cause potenziali

È presente un MAC con interfaccia hardcoded nella configurazione AMI.

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Scegliere una delle seguenti operazioni: • Modificare l'AMI per rimuovere l'impostazione hardcoded e riavviare l'istanza. • Modificare l'istanza per rimuovere l'indirizzo MAC hardcoded. O Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Distaccare il volume root. 3. Collegare il volume a un'altra istanza e modificare il volume per rimuovere l'indirizzo MAC hardcoded.

Per questo tipo di istanza	Eseguire questa operazione
	4. Collegare il volume all'istanza originale. 5. Avviare l'istanza.
Supportata da instance store	Scegliere una delle seguenti operazioni: • Modificare l'istanza per rimuovere l'indirizzo MAC hardcoded. • Terminare l'istanza e avviarne una nuova.

Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (configurazione SELinux errata)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

Cause potenziali

SELinux è stato abilitato per errore:

- Il kernel fornito non è supportato da GRUB
- Il kernel di fallback non esiste

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Attenersi alla seguente procedura: 1. Arrestare l'istanza non riuscita. 2. Distaccare il volume root dell'istanza non riuscita.

Per questo tipo di istanza	Eseguire questa operazione
	3. Collegare il volume root a un'altra istanza Linux in esecuzione (in seguito detta istanza di ripristino). 4. Connettersi all'istanza di ripristino e montare il volume root dell'istanza non riuscita. 5. Disabilitare SELinux sul volume root montato. Questo processo varia tra le distribuzioni Linux; per ulteriori informazioni, consultare la documentazione specifica del sistema operativo in uso. **Note** Su alcuni sistemi, per disabilitare SELinux occorre impostare `SELINUX=disabled` nel file `/mount_point /etc/sysconfig/selinux`, dove *mount_point* è la posizione in cui il volume è stato montato sull'istanza di ripristino. 6. Smontare e distaccare il volume root dall'istanza di ripristino e ricollegarlo all'istanza originale. 7. Avviare l'istanza.
Supportata da instance store	Attenersi alla seguente procedura: 1. Terminare l'istanza e avviarne una nuova. 2. (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite AWS Support.

XENBUS: Timeout connecting to devices (timeout di Xenbus)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found.  Try passing init= option to kernel.
```

Cause potenziali

- Il dispositivo a blocchi non è connesso all'istanza
- L'istanza utilizza un kernel datato.

Operazioni suggerite

Per questo tipo di istanza	Eseguire questa operazione
Supportata da Amazon EBS	Scegliere una delle seguenti operazioni: • Modificare l'AMI e l'istanza per utilizzare un kernel moderno e riavviare l'istanza. • Riavviare l'istanza.
Supportata da instance store	Scegliere una delle seguenti operazioni: • Terminare l'istanza. • Modificare l'AMI per utilizzare un kernel moderno e avviare una nuova istanza utilizzando questa AMI.

Risolvi i problemi relativi all'avvio di un'istanza Linux da un volume errato

> **Note**
>
> Questo argomento sulla risoluzione dei problemi si applica solo alle istanze Linux.

In alcune situazioni, potresti scoprire che un volume diverso da quello collegato a `/dev/xvda` o `/dev/sda` è diventato il volume root della tua istanza. Questo può succedere se hai collegato il volume root di un'altra istanza o un volume creato dalla snapshot di un volume root a un'istanza con un volume root esistente.

Ciò è dovuto al modo in cui il ramdisk iniziale funziona in Linux: Sceglie il volume definito come `/` nel file `/etc/fstab`, e in alcune distribuzioni; ciò è determinato dall'etichetta collegata alla partizione di volume. Nello specifico, puoi notare che il file `/etc/fstab` si presenta nel modo seguente:

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Se controlli l'etichetta di entrambi i volumi, vedrai che per tutti e due contiene `/`:

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

In questo esempio, `/dev/xvdf1` potrebbe diventare il dispositivo root su cui si avvia l'istanza dopo l'esecuzione iniziale del ramdisk, invece del volume `/dev/xvda1` da cui intendevi eseguire l'avvio. Per risolvere questo problema, utilizzare lo stesso comando e2label per modificare l'etichetta del volume collegato dal quale non si desidera eseguire l'avvio.

In alcuni casi, specificare un UUID in `/etc/fstab` può risolvere il problema. Tuttavia, se entrambi i volumi provengono dalla stessa snapshot o se quello secondario viene creato da una snapshot del volume principale, condivideranno un UUID.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

Per modificare l'etichetta di un volume ext4 collegato

1. Utilizzare il comando e2label per modificare l'etichetta del volume in modo diverso da /.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1 old/
   ```

2. Verificare che il volume abbia la nuova etichetta.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1
   old/
   ```

Per modificare l'etichetta di un volume xfs collegato

- Utilizzare il comando xfs_admin per modificare l'etichetta del volume in modo diverso da /.

  ```
  [ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
  writing all SBs
  new label = "old/"
  ```

Dopo avere modificato l'etichetta del volume come mostrato, è possibile riavviare l'istanza con il volume corretto selezionato dal ramdisk iniziale all'avvio dell'istanza.

> **Important**
>
> Se desideri distaccare il volume con la nuova etichetta e collegarlo a un'altra istanza per utilizzarlo come volume root, devi eseguire nuovamente la procedura di cui sopra e riportare l'etichetta del volume al suo valore originale. Diversamente, l'altra istanza non si avvia in quanto il ramdisk non è in grado di individuare il volume con l'etichetta /.

Risolvi i problemi di Sysprep con le istanze di Windows

> **Note**
>
> Questo argomento di risoluzione dei problemi si applica solo alle istanze di Windows.

Se si riscontrano problemi o si ricevono messaggi di errore durante la preparazione dell'immagine, analizzare i registri seguenti. Il percorso del log varia a seconda che si stia eseguendo EC2Config, EC2Launch v1 o EC2Launch v2 con Sysprep.

- `%WINDIR%\Panther\Unattendgc` (EC2Config, EC2Launch v1 e EC2Launch v2)
- `%WINDIR%\System32\Sysprep\Panther` (EC2Config, EC2Launch v1 e EC2Launch v2)
- `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` (solo EC2Config)
- `C:\ProgramData\Amazon\Ec2Config\Logs` (solo EC2Config)
- `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log` (solo EC2Launch v1)
- `%ProgramData%\Amazon\EC2Launch\log\agent.log` (solo EC2Launch v2)

Se si riceve un messaggio di errore durante la preparazione dell'immagine con Sysprep, il SO potrebbe non essere raggiungibile. Per rivedere i file di log, è necessario arrestare l'istanza, collegarne il volume principale a un'altra istanza sana come volume secondario, quindi analizzare i log menzionati in precedenza sul volume secondario. Per ulteriori informazioni sulle finalità dei file di log per nome, vedere File di log relativi alla configurazione di Windows nella documentazione di Microsoft.

Se si individuano errori nel file di log Unattendgc, utilizzare Microsoft Error Lookup Tool (Strumento di ricerca errori Microsoft) per ulteriori dettagli sull'errore. Il seguente problema riportato nel file di log Unattendgc in genere è il risultato di uno o più profili utente danneggiati sull'istanza:

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Sono disponibili due opzioni per la risoluzione di questo problema:

Opzione 1

Utilizza Regedit sull'istanza per cercare la chiave seguente. Verifica che non vi siano chiavi di registro di profilo per un utente eliminato.

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
\ProfileList\
```

Opzione 2

1. Modifica il file come segue:
   - Windows Server 2012 R2 e versioni precedenti: modifica il file di risposta di EC2Config (`C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml`).
   - Windows Server 2016 e 2019: modifica il file di risposta unattend.xml (`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`).
   - Windows Server 2022: modifica il file di risposta unattend.xml (`C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml`).
2. Passare da `<CopyProfile>true</CopyProfile>` a `<CopyProfile>false</CopyProfile>`.
3. Eseguire Sysprep nuovamente. Questa modifica alla configurazione cancellerà il profilo utente amministratore integrato dopo il completamento di Sysprep.

Utilizzo di EC2Rescue per Linux

EC2Rescue for Linux è uno easy-to-use strumento open source che può essere eseguito su un'istanza Amazon EC2 Linux per diagnosticare e risolvere problemi comuni utilizzando la sua libreria di oltre 100 moduli. Alcuni casi d'uso generalizzati di EC2Rescue per Linux includono la raccolta dei registri syslog e del gestore dei pacchetti, la raccolta dei dati di utilizzo sulla risorsa e la diagnosi/correzione dei parametri noti del kernel problematici e dei problemi comuni di OpenSSH.

Il runbook `AWSSupport-TroubleshootSSH` installa EC2Rescue per Linux e quindi utilizza lo strumento per controllare o provare a risolvere problemi comuni che impediscono una connessione remota a una macchina Linux tramite SSH. Per ulteriori informazioni e per eseguire questa automazione, consulta AWS Support-TroubleshootSSH.

Se utilizzi un'istanza Windows, consulta. the section called “EC2Rescue for Windows Server”

Indice

- Utilizzo di EC2Rescue per Linux
- Sviluppo dei moduli EC2Rescue

Installazione di EC2Rescue per Linux

Lo strumento EC2Rescue per Linux può essere installato su un'istanza Linux Amazon EC2 in grado di rispettare i prerequisiti seguenti.

Prerequisiti

- Sistemi operativi supportati:
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7 e versioni successive
  - Ubuntu 16.04+
- Requisiti software:
  - Python 2.7.9 e versioni successive o 3.2 e versioni successive

Il runbook `AWSSupport-TroubleshootSSH` installa EC2Rescue per Linux e quindi utilizza lo strumento per controllare o provare a risolvere problemi comuni che impediscono una connessione remota a una macchina Linux tramite SSH. Per ulteriori informazioni e per eseguire questa automazione, consulta AWS Support-TroubleshootSSH.

Se il sistema ha la versione Python richiesta, puoi installare la build standard. Altrimenti, puoi installare la build in bundle, che include una copia minima di Python.

Per installare la build standard

1. Da un'istanza Linux attiva, scaricare lo strumento EC2Rescue per Linux:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
   ```

2. (Facoltativo) Prima di procedere, è possibile scegliere di verificare la firma del file di installazione EC2Rescue per Linux. Per ulteriori informazioni, consulta (Facoltativo) Verifica della firma di EC2Rescue per Linux.
3. Scaricare il file di hash sha256:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
```

4. Verificare l'identità del tarball:

```
sha256sum -c ec2rl.tgz.sha256
```

5. Decomprimere il tarball:

```
tar -xzvf ec2rl.tgz
```

6. Verificare l'installazione elencando il file della guida:

```
cd ec2rl-<version_number>
./ec2rl help
```

Per installare la build in bundle

Per il collegamento di download e l'elenco delle limitazioni, consulta EC2Rescue per Linux su Github.

(Facoltativo) Verifica della firma di EC2Rescue per Linux

Di seguito si riporta il processo consigliato per la verifica della validità del pacchetto EC2Rescue per Linux per i sistemi operativi basati su Linux.

Quando si esegue il download di un'applicazione da Internet, ti consigliamo di autenticare l'identità dell'autore del software e di controllare che l'applicazione non risulti modificata o danneggiata rispetto alla versione pubblicata. Ciò consente di evitare di installare una versione dell'applicazione contenente un virus o altro malware.

Se dopo aver eseguito la procedura descritta in questo argomento risulta che il software di EC2Rescue per Linux è alterato o danneggiato, non eseguire il file di installazione. In caso contrario, contatta Amazon Web Services.

I file di EC2Rescue per Linux per i sistemi operativi basati su Linux sono firmati usando lo standard di crittografia GnuPG, un'implementazione open source dello standard Pretty Good Privacy (OpenPGP) per le firme digitali sicure. GnuPG (noto anche come GPG) fornisce l'autenticazione e il controllo dell'integrità tramite una firma digitale. AWS pubblica una chiave pubblica e delle firme che è possibile utilizzare per verificare il pacchetto EC2Rescue for Linux scaricato. Per ulteriori informazioni su PGP e GnuPG (GPG), consulta http://www.gnupg.org.

La prima fase prevede la verifica dell'affidabilità dell'autore del software. Scarica la chiave pubblica dell'autore del software, controlla l'autenticità di tale proprietario e quindi aggiungi la chiave pubblica al keyring. Il keyring è una raccolta di chiavi pubbliche nota. Dopo aver confermato l'autenticità della chiave pubblica, puoi usarla per verificare la firma dell'applicazione.

Attività

- Installazione degli strumenti GPG
- Autenticazione e importazione della chiave pubblica
- Verifica della firma del pacchetto

Installazione degli strumenti GPG

Se il sistema operativo è Linux o Unix, gli strumenti GPG potrebbero essere già installati. Per sapere se gli strumenti sono installati nel sistema, immetti gpg2 al prompt dei comandi. Se gli strumenti GPG sono installati, viene visualizzato un prompt dei comandi GPG. Se gli strumenti GPG non sono installati, verrà visualizzato un messaggio di errore che indica che il comando non è disponibile. Puoi installare il pacchetto GnuPG da un repository.

Per installare gli strumenti GPG su un computer Linux basato su Debian

- Da un terminale, esegui il comando seguente:

```
apt-get install gnupg2
```

Per installare gli strumenti GPG su un computer Linux basato su Red Hat

- Da un terminale, esegui il comando seguente:

```
yum install gnupg2
```

Autenticazione e importazione della chiave pubblica

La successiva fase del processo prevede l'autenticazione della chiave pubblica di EC2Rescue per Linux e la sua aggiunta come chiave affidabile nel keyring GPG.

Per eseguire l'autenticazione e l'importazione della chiave pubblica di EC2Rescue per Linux

1. In un prompt dei comandi, utilizzare il comando seguente per ottenere una copia della chiave pubblica GPG:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
   ```

2. In un prompt dei comandi, nella directory in cui è stata salvata `ec2rl.key`, utilizzare il comando seguente per importare la chiave pubblica di EC2Rescue per Linux nel keyring:

   ```
   gpg2 --import ec2rl.key
   ```

   Il comando restituisce risultati simili ai seguenti:

   ```
   gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
   gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
    imported
   gpg: Total number processed: 1
   gpg:               imported: 1  (RSA: 1)
   ```

Verifica della firma del pacchetto

Dopo aver installato gli strumenti GPG, avere autenticato e importato la chiave pubblica di EC2Rescue per Linux e avere verificato che la chiave pubblica di EC2Rescue per Linux sia affidabile, puoi verificare la firma dello script di installazione di EC2Rescue per Linux.

Per verificare la firma dello script di installazione di EC2Rescue per Linux

1. Al prompt dei comandi esegui il comando seguente per scaricare il file SIGNATURE per lo script di installazione:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
   ```

2. Verifica la firma utilizzando il comando seguente al prompt dei comandi nella directory in cui hai salvato `ec2rl.tgz.sig` e il file di installazione EC2Rescue per Linux. Entrambi i file devono essere presenti.

   ```
   gpg2 --verify ./ec2rl.tgz.sig
   ```

L'output deve essere simile al seguente:

```
gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
     Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
```

Se l'output contiene la frase `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`, significa che la firma è stata verificata correttamente ed è possibile eseguire lo script di installazione di EC2Rescue per Linux.

Se l'output include la frase `BAD signature`, controlla di avere eseguito la procedura correttamente. Se il problema persiste, contatta Amazon Web Services e non eseguire il file di installazione scaricato in precedenza.

Di seguito sono elencati i dettagli sugli avvisi che potrebbero comparire:

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner. Questo messaggio fa riferimento al livello di affidabilità valutato personalmente in merito al possesso di una chiave pubblica autentica per EC2Rescue per Linux. In un mondo ideale, l'utente visita un ufficio Amazon Web Services e riceve la chiave personalmente. Tuttavia, la prassi normale è scaricare la chiave da un sito Web. In questo caso, il sito Web è un sito Web di Amazon Web Services.
- gpg2: no ultimately trusted keys found. Questo messaggio indica che la chiave specifica non è ritenuta affidabile da te o da un'altra persona da te considerata affidabile.

Per ulteriori informazioni, consulta http://www.gnupg.org.

Utilizzo di EC2Rescue per Linux

Di seguito sono riportate le attività più comuni che puoi eseguire per prendere dimestichezza con questo strumento.

Attività

- Esegui EC2Rescue per Linux

- Caricamento dei risultati
- Creazione di backup
- Chiedere aiuto

Esegui EC2Rescue per Linux

Puoi eseguire EC2Rescue per Linux come mostrato negli esempi seguenti.

Example Esempio: esecuzione di tutti i moduli

Per eseguire tutti i moduli, esegui EC2Rescue per Linux senza opzioni:

```
./ec2rl run
```

Alcuni moduli richiedono l'accesso root. Se non sei un utente root, utilizza sudo per eseguire i moduli come segue:

```
sudo ./ec2rl run
```

Example Esempio: esecuzione di un modulo specifico

Per eseguire solo moduli specifici, utilizza il parametro --only-modules:

```
./ec2rl run --only-modules=module_name --arguments
```

Ad esempio, questo comando esegue il modulo dig per eseguire query sul dominio `amazon.com`:

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Example Esempio: visualizzazione dei risultati

Puoi visualizzare i risultati in `/var/tmp/ec2rl`:

```
cat /var/tmp/ec2rl/logfile_location
```

Ad esempio, visualizza il file di log per il modulo dig:

```
cat /var/tmp/ec2rl/2017-05-11T15_39_21.893145/mod_out/run/dig.log
```

Caricamento dei risultati

Se AWS Support ha richiesto i risultati o desidera condividerli da un bucket S3, caricali utilizzando lo strumento CLI EC2Rescue for Linux. Nell'output dei comandi di EC2Rescue per Linux sono riportati i comandi da utilizzare.

Example Esempio: carica i risultati su AWS Support

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --support-url="URLProvidedByAWSSupport"
```

Example Esempio: caricamento dei risultati in un bucket S3

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --presigned-url="YourPresignedS3URL"
```

Per ulteriori informazioni sulla generazione di URL prefirmati per Amazon S3, consulta la sezione relativa al caricamento degli oggetti tramite URL prefirmati.

Creazione di backup

Crea un backup per la tua istanza, uno o più volumi o un ID dispositivo specifico tramite i comandi seguenti.

Example Esempio: backup di un'istanza con un'Amazon Machine Image (AMI)

```
./ec2rl run --backup=ami
```

Example Esempio: backup di tutti i volumi associati all'istanza

```
./ec2rl run --backup=allvolumes
```

Example Esempio: backup di un volume specifico

```
./ec2rl run --backup=volumeID
```

Chiedere aiuto

EC2Rescue per Linux include un file della guida contenente le informazioni e la sintassi di ciascun comando disponibile.

Example Esempio: visualizzazione della guida generale

```
./ec2rl help
```

Example Esempio: elenco dei moduli disponibili

```
./ec2rl list
```

Example Esempio: visualizzazione della guida di un modulo specifico

```
./ec2rl help module_name
```

Ad esempio, utilizza il seguente comando per visualizzare il file della guida per il modulo dig:

```
./ec2rl help dig
```

Sviluppo dei moduli EC2Rescue

I moduli sono scritti in YAML, uno standard di serializzazione dei dati. Il file YAML di un modulo è formato da un singolo documento che rappresenta il modulo e i relativi attributi.

Aggiunta di attributi di modulo

Nella tabella seguente vengono elencati gli attributi di modulo disponibili.

Attributo	Descrizione
name	Il nome del modulo. Il nome non deve superare i 18 caratteri.
version	Il numero di versione del modulo.
title	Un breve titolo descrittivo del modulo. Questo valore non deve superare i 50 caratteri.
helptext	La descrizione estesa del modulo. Ogni riga non deve superare i 75 caratteri. Se il modulo consuma argomenti, obbligatori o facoltativi, includili nel valore helptext.

Attributo	Descrizione

	Ad esempio:
	
	`helptext: !!str |`
	`  Collect output from ps for system analysis`
	`  Consumes --times= for number of times to repeat`
	`  Consumes --period= for time period between repetition`

placement	La fase in cui eseguire il modulo. Valori supportati: • prediagnostic • run • postdiagnostic
linguaggio	Il linguaggio in cui è scritto il codice del modulo. Valori supportati: • bash • python **Note** Il codice Python deve essere compatibile con Python 2.7.9 e versioni successive e Python 3.2 e versioni successive.

Attributo	Descrizione
remediation	Indica se il modulo supporta le azioni di correzione. I valori supportati sono `True` o `False`. Il modulo viene impostato su `False` per impostazione predefinita se questo valore è assente, rendendo l'attributo facoltativo per i moduli che non supportano le azioni di correzione.
content	L'interezza del codice dello script.
vincolo	Il nome dell'oggetto contenente i valori di vincolo.
domain	Un descrittore del raggruppamento o della classificazione del modulo. L'insieme dei moduli inclusi utilizza i domini seguenti: • applicazione • net • so • prestazioni
classe	Un descrittore del tipo di attività effettuato dal modulo. L'insieme dei moduli inclusi utilizza le classi seguenti: • collect (raccoglie l'output dai programmi) • diagnose (riuscita/errore in base a un insieme di criteri) • gather (copia i file e li scrive su un file specifico)

Attributo	Descrizione
distro	L'elenco delle distribuzioni Linux supportate da questo modulo. Il set di moduli inclusi utilizza le distribuzioni seguenti: • alami (Amazon Linux) • rhel • ubuntu • suse
obbligatorio	Gli argomenti obbligatori che il modulo consuma dalle opzioni della CLI.
facoltativo	Gli argomenti facoltativi che il modulo può utilizzare.
software	I file eseguibili del software utilizzati nel modulo. Questo attributo è progettato per specificare un software non installato per impostazione predefinita. La logica EC2Rescue per Linux assicura che tali programmi siano presenti ed eseguibili prima di eseguire il modulo.
package	Il pacchetto software di origine di un file eseguibile. Questo attributo è progettato per fornire dettagli estesi sul pacchetto con il software, incluso un URL per ottenere o scaricare ulteriori informazioni.

Attributo	Descrizione
sudo	Indica se l'accesso root è obbligatorio per l'esecuzione del modulo. Non è necessario implementare i controlli sudo nello script del modulo. Se il valore è true, la logica EC2Rescue per Linux esegue il modulo soltanto se l'utente che lo esegue dispone dell'accesso root.
perfimpact	Indica se il modulo può avere un significativo impatto sulle prestazioni nell'ambiente in cui viene eseguito. Se il valore è true e l'argomento `--perfimpact=true` non è presente, il modulo viene ignorato.
parallelexclusive	Specifica un programma che richiede reciproca esclusività. Ad esempio, tutti i moduli con la specifica "bpf" vengono eseguiti in modo seriale.

Aggiunta di variabili di ambiente

Nella tabella seguente vengono elencate le variabili di ambiente disponibili.

Variabile di ambiente	Descrizione
`EC2RL_CALLPATH`	Il percorso a `ec2rl.py`. Questo percorso può essere utilizzato per individuare la directory lib e per utilizzare i moduli Python gestiti da un fornitore.
`EC2RL_WORKDIR`	La directory tmp principale dello strumento di diagnostica. Valore predefinito: `/var/tmp/ec2rl` .

Variabile di ambiente	Descrizione
EC2RL_RUNDIR	La directory in cui viene archiviato tutto l'output. Valore predefinito: /var/tmp/ec2rl/<date&timestamp> .
EC2RL_GATHEREDDIR	La directory root in cui inserire i dati raccolti sul modulo. Valore predefinito:/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/ .
EC2RL_NET_DRIVER	Il driver in uso per la prima interfaccia di rete non virtuale sull'istanza (in ordine alfabetico). Esempi: • xen_netfront • ixgbevf • ena
EC2RL_SUDO	Impostato su true se EC2Rescue per Linux è in esecuzione come root; altrimenti, è impostato su false.
EC2RL_VIRT_TYPE	Il tipo di virtualizzazione fornito dai metadati dell'istanza. Esempi: • default-hvm • default-paravirtual

Variabile di ambiente	Descrizione
`EC2RL_INTERFACES`	Un elenco enumerato delle interfacce sul sistema. Il valore è una stringa contenente nomi, come `eth0`, `eth1` e così via. Viene generato tramite `functions.bash` ed è disponibile soltanto per i moduli da cui ha avuto origine.

Utilizzo della sintassi YAML

Annota quanto riportato di seguito durante la costruzione dei file YAML del modulo:

- I trattini tripli (`---`) denotano l'inizio esplicito di un documento.
- Il tag `!ec2rlcore.module.Module` comunica al parser YAML il costruttore da richiamare durante la creazione dell'oggetto dal flusso di dati. È possibile trovare il costruttore nel file `module.py`.
- Il tag `!!str` comunica al parser YAML di non tentare di determinare il tipo di dati, ma di interpretare i contenuti come un valore letterale di stringa.
- Il carattere barra verticale (`|`) comunica al parser YAML che il valore è un valore scalare di stile letterale. In questo caso, il parser include tutti gli spazi vuoti. Ciò è importante per i moduli perché vengono mantenuti i caratteri di rientro e nuova riga.
- Come puoi vedere negli esempi seguenti, il rientro standard di YAML è di due spazi. Assicurati di mantenere il rientro standard (ad esempio, quattro spazi per Python) nello script e di far rientrare di due spazi tutto il contenuto all'interno del file del modulo.

Moduli di esempio

Esempio uno (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
```

```
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
 $period seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
  sudo: !!str False
  perfimpact: !!str False
  parallelexclusive: !!str
```

Utilizzo di EC2Rescue for Windows Server

EC2Rescue for Windows Server è easy-to-use uno strumento che puoi eseguire su un'istanza Amazon EC2 Windows Server per diagnosticare e risolvere possibili problemi. Si tratta di uno strumento utile per raccogliere i file di log e risolvere i problemi, nonché per individuare in modo

proattivo le possibili aree problematiche. Consente inoltre di esaminare i volumi root Amazon EBS di altre istanze e raccogliere i log rilevanti per la risoluzione dei problemi delle istanze Windows Server che utilizzano tali volumi.

EC2Rescue for Windows Server dispone di due moduli diversi: un modulo di raccolta dati per la raccolta dei dati da tutte le varie origini e un modulo di analisi per l'analisi dei dati raccolti in base a una serie di regole predefinite per identificare gli eventuali problemi e fornire suggerimenti per la risoluzione.

Lo strumento EC2Rescue for Windows Server funziona solo su istanze Amazon EC2 che eseguono Windows Server 2012 e versioni successive. All'avvio lo strumento controlla se viene eseguito su un'istanza Amazon EC2.

Il runbook `AWSSupport-ExecuteEC2Rescue` utilizza lo strumento EC2Rescue per risolvere i problemi e, laddove possibile correggere i guasti alla connettività con l'istanza EC2 specificata. Per ulteriori informazioni e per eseguire questa automazione, consulta -Exec2Rescue. AWSSupport

Se si utilizza un'istanza Linux, vedere. the section called “EC2Rescue for Linux”

Indice

Utilizzo della GUI EC2Rescue for Windows Server

EC2Rescue for Windows Server può eseguire le seguenti analisi su istanze offline:

Opzione	Descrizione
Diagnose and Rescue (Esegui diagnostica e recupero)	EC2Rescue for Windows Server può rilevare e risolvere dei problemi con le seguenti impostazioni del servizio: • System Time (Ora di sistema) • RealTimeisUniversal - Rileva se la chiave di `RealTimeisUniversal` registro è

Opzione	Descrizione

	abilitata. Se è disabilitata, l'ora del sistema Windows cambia quando il fuso orario viene impostato su un valore diverso da UTC.
	
	• Windows Firewall
	  • Domain networks (Reti di dominio): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato.
	  • Private networks (Reti private): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato.
	  • Guest or public networks (Guest o reti pubbliche): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato.
	
	• Remote Desktop (Desktop remoto)
	  • Service Start (Avvio servizio): rileva se il servizio Remote Desktop (Desktop remoto) è abilitato.
	  • Connessione Desktop remoto: rileva se questo servizio è abilitato.
	  • TCP Port (Porta TCP): rileva su quale porta il Remote Desktop (Desktop remoto) è in ascolto.
	
	• EC2Config (Windows Server 2012 R2 e versioni precedenti)
	  • Installation (Installazione): rileva quale versione di EC2Config è installata.
	  • Service Start (Avvio servizio): rileva se il servizio EC2Config è abilitato.

Opzione	Descrizione
	• Ec2 SetPassword - Genera una nuova password di amministratore. • Ec2 HandleUser Data - Consente di eseguire uno script di dati utente al successivo avvio dell'istanza. • EC2Launch (Windows Server 2016 e versioni successive) • Installation (Installazione): rileva quale versione di EC2Launch è installata. • Ec2 SetPassword - Genera una nuova password di amministratore. • Interfaccia di rete • DHCP Service Startup (Avvio servizio DHCP): rileva se il servizio DHCP è abilitato. • Ethernet detail (Dettagli Ethernet): visualizza le informazioni sulla versione del driver di rete, se rilevata. • DHCP on Ethernet (DHCP su Ethernet): rileva se DHCP è abilitato. • Stato della firma su disco • Firma su disco e Firma sul database di configurazione di avvio (BCD): rileva se la firma del disco e la firma BCD sono uguali. Se i valori sono diversi, EC2Rescue prova a sovrascrivere la firma del disco con la firma su BCD.

Opzione	Descrizione
Ripristino	Eseguire una delle seguenti operazioni: • Last Known Good Configuration (Ultima configurazione valida nota): cerca di avviare l'istanza con l'ultimo stato avviabile noto. • Restore registry from backup (Ripristina registro da backup): ripristina il registro da `\Windows\System32\config\RegBack` .
Capture Logs (Acquisisci log)	Permette di acquisire i log relativi all'istanza per l'analisi.

EC2Rescue for Windows Server può raccogliere i seguenti dati dalle istanze attive e offline:

Elemento	Descrizione
Event Log (Log eventi)	Raccoglie i log degli eventi relativi ad applicazione, sistema ed EC2Config.
Registry	Raccoglie gli hive `SYSTEM` e `SOFTWARE`.
Windows Update Log (Log aggiornamenti di Windows)	Raccoglie i file di log generati da Windows Update. **Note** In Windows Server 2016 e versioni successive, il log viene raccolto in formato Event Tracing for Windows (ETW).
Sysprep Log (Log Sysprep)	Raccoglie i file di log generati dallo strumento di preparazione del sistema Windows (Sysprep).

Elemento	Descrizione
Driver Setup Log	Raccoglie i log di Windows SetupAPI (`setupapi.dev.log` e `setupapi.setup.log`).
Boot Configuration (Configurazione di avvio)	Raccoglie l'hive `HKEY_LOCAL_MACHINE\BCD00000000`.
Memory Dump (Dump memoria)	Raccoglie i file dei dump della memoria esistenti sull'istanza.
EC2Config File (File EC2Config)	Raccoglie i file di log generati dal servizio EC2Config.
EC2Launch File (File EC2Launch)	Raccoglie i file di log generati dagli script EC2Launch.
SSM Agent File (File agente SSM)	Raccoglie i file di log generati dai log SSM Agent e Patch Manager.
File EC2 ElasticGPUs	Raccoglie i log degli eventi relativi alle GPU elastiche.
ECS	Raccoglie i log relativi ad Amazon ECS.
CloudEndure	Raccoglie i file di registro relativi all'agente. CloudEndure

EC2Rescue for Windows Server può raccogliere i seguenti dati aggiuntivi da istanze attive:

Elemento	Descrizione
System Information (Informazioni sul sistema)	Raccoglie MSInfo32.
Group Policy Result	Raccoglie un report relativo alle policy del gruppo.

Analisi di un'istanza offline

L'opzione Offline Instance (Istanza offline) risulta utile per eseguire il debug dei problemi di avvio con le istanze di Windows.

Per eseguire un'operazione su un'istanza offline

1. Da un'istanza di Windows Server in esecuzione, scaricare lo strumento EC2Rescue for Windows Server ed estrarre i file.

   È possibile eseguire il seguente PowerShell comando per scaricare EC2Rescue senza modificare la configurazione di sicurezza avanzata (ESC) di Internet Explorer:

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Con questo comando verrà scaricato il file .zip EC2Rescue sul desktop dell'utente che ha attualmente eseguito l'accesso.

   > **Note**
   >
   > Se ricevi un errore durante il download del file e utilizzi Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il seguente comando e riprovare:
   >
   > ```
   > [Net.ServicePointManager]::SecurityProtocol =
   >  [Net.SecurityProtocolType]::Tls12
   > ```

2. Arrestare l'istanza in errore, se non è già stata arrestata.
3. Scollegare il volume root EBS dall'istanza in errore e collegare il volume a un'istanza Windows in esecuzione in cui sia installato EC2Rescue for Windows Server.
4. Eseguire lo strumento EC2Rescue for Windows Server sull'istanza in esecuzione e scegliere Offline Instance (Istanza offline).
5. Selezionare il disco del volume appena montato e scegliere Next (Successivo).
6. Confermare la selezione del disco e scegliere Yes (Sì).

7. Scegliere l'opzione relativa all'istanza offline da eseguire e selezionare Next (Successivo).

Lo strumento EC2Rescue for Windows Server analizza il volume e raccoglie le informazioni relative alla risoluzione dei problemi in base ai file di log selezionati.

Raccolta di dati da un'istanza attiva

Puoi raccogliere i log e altri dati da un'istanza attiva.

Per raccogliere dati da un'istanza attiva

1. Connettersi all'istanza Windows.
2. Scaricare lo strumento EC2Rescue for Windows Server nell'istanza Windows corrente ed estrarre i file.

   È possibile eseguire il seguente PowerShell comando per scaricare EC2Rescue senza modificare la configurazione di sicurezza avanzata (ESC) di Internet Explorer:

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Con questo comando verrà scaricato il file .zip EC2Rescue sul desktop dell'utente che ha attualmente eseguito l'accesso.

   > **Note**
   >
   > Se ricevi un errore durante il download del file e utilizzi Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il seguente comando e riprovare:
   >
   > ```
   > [Net.ServicePointManager]::SecurityProtocol =
   >  [Net.SecurityProtocolType]::Tls12
   > ```

3. Aprire l'applicazione EC2Rescue for Windows Server e accettare l'accordo di licenza.
4. Scegliere Next (Successivo), Current instance (Istanza corrente), Capture logs (Acquisisci log).

5. Selezionare i tipi di dati da raccogliere e scegliere Collect... (Raccogli...). Leggere l'avviso e scegliere Yes (Sì) per continuare.
6. Scegliere un nome di file e la posizione per il file .zip, quindi selezionare Save (Salva).
7. Quando EC2Rescue for Windows Server ha completato l'operazione, scegliere Open Containing Folder (Apri cartella superiore) per visualizzare il file .zip file.
8. Scegliere Finish (Fine).

Utilizzo di EC2Rescue for Windows Server con la riga di comando

L'interfaccia a riga di comando (CLI) di EC2Rescue for Windows Server ti permette di eseguire un plugin EC2Rescue for Windows Server (noto anche come "operazione") a livello di programmazione.

Lo strumento EC2Rescue for Windows Server è caratterizzato da due modalità di esecuzione:

- /online – Permette di eseguire l'operazione sull'istanza su cui è installato EC2Rescue for Windows Server, ad esempio la raccolta dei file di log.
- /offline<device_id> – Permette di eseguire l'operazione sul volume root offline collegato a un'istanza Amazon EC2 di Windows distinta, su sui è installato EC2Rescue for Windows Server.

Scaricare lo strumento EC2Rescue for Windows Server nell'istanza Windows corrente ed estrarre i file. Puoi visualizzare il file di aiuto con il seguente comando:

```
EC2RescueCmd.exe /help
```

EC2Rescue for Windows Server può eseguire le seguenti operazioni su un'istanza Amazon EC2 di Windows:

- Operazione di raccolta
- Operazione di recupero
- Operazione di ripristino

Operazione di raccolta

> **Note**
>
> Puoi raccogliere tutti i log, un intero gruppo di log oppure un singolo log all'interno di un gruppo.

EC2Rescue for Windows Server può raccogliere i seguenti dati dalle istanze attive e offline.

Gruppo di log	Log disponibili	Descrizione
`all`		Raccoglie tutti i log disponibili.
`eventlog`	• `'Application'` • `'System'` • `'EC2ConfigService'`	Raccoglie i log degli eventi relativi ad applicazione, sistema ed EC2Config.
`memory-dump`	• `'Memory Dump File'` • `'Mini Dump Files'`	Raccoglie i file dei dump della memoria esistenti sull'istanza.
`ec2config`	• `'Log Files'` • `'Configuration Files'`	Raccoglie i file di log generati dal servizio EC2Config.
`ec2launch`	• `'Logs'` • `'Config'`	Raccoglie i file di log generati dagli script EC2Launch.
`ssm-agent`	• `'Log Files'` • `'Patch Baseline Logs'` • `'InstanceData'`	Raccoglie i file di log generati dai log SSM Agent e Patch Manager.
`sysprep`	`'Log Files'`	Raccoglie i file di log generati dallo strumento di preparazione del sistema Windows (Sysprep).

Gruppo di log	Log disponibili	Descrizione
`driver-setup`	• `'SetupAPI Log Files'` • `'DPInst Log File'` • `'AWS PV Setup Log File'`	Raccoglie i log di Windows SetupAPI (`setupapi.dev.log` e `setupapi.setup.log`).
`registry`	• `'SYSTEM'` • `'SOFTWARE'` • `'BCD'`	Raccoglie gli hive `SYSTEM` e `SOFTWARE`.
`egpu`	• `'Event Log'` • `'System Files'`	Raccoglie i log degli eventi relativi alle GPU elastiche.
`boot-config`	`'BCDEDIT Output'`	Raccoglie l'hive `HKEY_LOCAL_MACHINE\BCD00000000` .
`windows-update`	`'Log Files'`	Raccoglie i file di log generati da Windows Update. **Note** In Windows Server 2016 e versioni successive, il log viene raccolto in formato Event Tracing for Windows (ETW).
`cloudendure`	• `'Migrate Script Logs'` • `'Driver Logs'` • `'CloudEndure File List'`	Raccoglie i file di registro relativi all'agente. CloudEndure

EC2Rescue for Windows Server può raccogliere i seguenti dati aggiuntivi da istanze attive.

Gruppo di log	Log disponibili	Descrizione
`system-info`	`'MSInfo32 Output'`	Raccoglie `MSInfo32`.
`gpresult`	`'GPResult Output'`	Raccoglie un report relativo alle policy del gruppo.

Sono disponibili le seguenti opzioni:

- /output: <output FilePath > - Posizione del percorso del file di destinazione richiesta per salvare i file di registro raccolti in formato zip.
- /no-offline: attributo opzionale utilizzato in modalità non in linea. Non imposta il volume sullo stato offline dopo il completamento dell'operazione.
- /no-fix-signature: attributo opzionale utilizzato in modalità non in linea. Non corregge un possibile conflitto di firma del disco dopo il completamento dell'operazione.

Esempi

Di seguito sono elencati alcuni esempi di utilizzo della CLI EC2Rescue for Windows Server.

Esempi della modalità online

Per raccogliere tutti i log disponibili:

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Per raccogliere solo un gruppo di log specifico:

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Per raccogliere singoli log all'interno di un gruppo di log:

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI
 Log Files' /output:<outputFilePath>
```

Esempi della modalità offline

Per raccogliere tutti i log disponibili da un volume EBS. Il volume è specificato dal valore device_id.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Per raccogliere solo un gruppo di log specifico:

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Operazione di recupero

EC2Rescue for Windows Server può rilevare e risolvere dei problemi con le seguenti impostazioni del servizio:

Gruppo di servizi	Operazioni disponibili	Descrizione
`all`		
`system-time`	`'RealTimeIsUniversal'`	System Time (Ora di sistema) • RealTimeisUniversal - Rileva se la chiave di `RealTimeisUniversal` registro è abilitata. Se è disabilitata, l'ora del sistema Windows cambia quando il fuso orario viene impostato su un valore diverso da UTC.
`firewall`	• `'Domain networks'` • `'Private networks'` • `'Guest or public networks'`	Windows Firewall • Domain networks (Reti di dominio): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato.

Gruppo di servizi	Operazioni disponibili	Descrizione
		• Private networks (Reti private): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato. • Guest or public networks (Guest o reti pubbliche): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato.
rdp	• `'Service Start'` • `'Remote Desktop Connections'` • `'TCP Port'`	Remote Desktop (Desktop remoto) • Service Start (Avvio servizio): rileva se il servizio Remote Desktop (Desktop remoto) è abilitato. • Connessione Desktop remoto: rileva se questo servizio è abilitato. • TCP Port (Porta TCP): rileva su quale porta il Remote Desktop (Desktop remoto) è in ascolto.

Gruppo di servizi	Operazioni disponibili	Descrizione
`ec2config`	• `'Service Start'` • `'Ec2SetPassword'` • `'Ec2HandleUserData'`	EC2Config • Service Start (Avvio servizio): rileva se il servizio EC2Config è abilitato. • Ec2 SetPassword - Genera una nuova password di amministratore. • Ec2 HandleUser Data - Consente di eseguire uno script di dati utente al successivo avvio dell'istanza.
`ec2launch`	`'Reset Administrator Password'`	Genera una nuova password per l'amministratore di Windows.
`network`	`'DHCP Service Startup'`	Interfaccia di rete • DHCP Service Startup (Avvio servizio DHCP): rileva se il servizio DHCP è abilitato.

Sono disponibili le seguenti opzioni:

- /level:<level>: attributo opzionale per il livello di controllo che l'operazione deve attivare. I valori consentiti sono: `information`, `warning`, `error`, `all`. Per impostazione predefinita, è impostato su `error`.
- /check-only: attributo opzionale che genera un report, ma non apporta modifiche al volume non in linea.

> **Note**
>
> Se EC2Rescue for Windows Server rileva una possibile collisione tra le firme del disco, per impostazione predefinita corregge la firma dopo il completamento del processo offline, anche quando si utilizza l'opzione. `/check-only` È necessario utilizzare l'opzione per impedire la correzione. `/no-fix-signature`

- /no-offline: attributo opzionale che impedisce l'impostazione del volume sullo stato non in linea dopo il completamento dell'operazione.
- /no-fix-signature: attributo opzionale che non corregge un possibile conflitto di firma del disco dopo il completamento dell'operazione.

Esempi di recupero

Di seguito sono elencati alcuni esempi di utilizzo della CLI EC2Rescue for Windows Server. Il volume è specificato dal valore device_id.

Per tentare di correggere tutti i problemi rilevati su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Per tentare di correggere tutti i problemi all'interno di un gruppo di servizi su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Per tentare di correggere un problema specifico all'interno di un gruppo di servizi su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Per specificare più problemi da risolvere su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Operazione di ripristino

EC2Rescue for Windows Server può rilevare e risolvere dei problemi con le seguenti impostazioni del servizio:

Gruppo di servizi	Operazioni disponibili	Descrizione
Restore Last Known Good Configuration (Ripristina ultima configurazione valida nota)	`lkgc`	Last Known Good Configura tion (Ultima configurazione valida nota): cerca di avviare l'istanza con l'ultimo stato avviabile noto.
Restore Windows registry from latest backup (Ripristina registro di Windows da ultimo backup)	`regback`	Restore registry from backup (Ripristina registro da backup): ripristina il registro da `\Windows\System32\ config\RegBack` .

Sono disponibili le seguenti opzioni:

- /no-offline – Attributo opzionale che impedisce l'impostazione del volume sullo stato offline dopo il completamento dell'operazione.
- /no-fix-signature – Attributo opzionale che non corregge un possibile conflitto di firma del disco dopo il completamento dell'operazione.

Esempi di ripristino

Di seguito sono elencati alcuni esempi di utilizzo della CLI EC2Rescue for Windows Server. Il volume è specificato dal valore device_id.

Per ripristinare l'ultima configurazione valida nota su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Per ripristinare l'ultimo backup del registro di Windows su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Utilizzo di EC2Rescue for Windows Server con Run Command per Systems Manager

AWS Support fornisce un documento Systems Manager Run Command per interfacciarsi con l'istanza abilitata a Systems Manager per eseguire EC2Rescue for Windows Server. Il documento Run Command è denominato `AWSSupport-RunEC2RescueForWindowsTool`.

Questo documento Run Command per Systems Manager esegue le seguenti attività:

- Scarica e verifica EC2Rescue for Windows Server.
- Importa un PowerShell modulo per facilitare l'interazione con lo strumento.
- Esegue EC2 RescueCmd con il comando e i parametri forniti.

Il documento Run Command per Systems Manager accetta tre parametri:

- Comando – L'azione EC2Rescue for Windows Server. I valori consentiti correnti sono:
  - ResetAccess—Reimposta la password dell'amministratore locale. La password dell'amministratore locale dell'istanza corrente verrà reimpostata; la password generata casualmente verrà archiviata in modo sicuro in Parameter Store come `/EC2Rescue/Password/<INSTANCE_ID>`. Se selezioni questa operazione e non specifichi alcun parametro, le password vengono crittografate automaticamente con la Chiave KMS predefinita. Facoltativamente, puoi specificare l'ID Chiave KMS nel parametro Parameters per crittografare la password con una chiave personalizzata.
  - CollectLogs—Esegue EC2Rescue per Windows Server con l'azione. `/collect:all` Se selezioni questa operazione, `Parameters` deve includere un nome bucket Amazon S3 in cui caricare i log.
  - FixAll—Esegue EC2Rescue per Windows Server con l'azione. `/rescue:all` Se selezioni questa operazione, `Parameters` deve includere il nome del dispositivo a blocchi da recuperare.
- Parametri: i PowerShell parametri da passare per il comando specificato.

> **Note**
>
> Affinché l'ResetAccessazione funzioni, la tua istanza Amazon EC2 deve avere la seguente policy allegata per scrivere la password crittografata in Parameter Store. Attendi alcuni minuti prima di provare a reimpostare la password di un'istanza dopo che hai associato questa policy al ruolo IAM correlato.

Utilizzo della Chiave KMS predefinita:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    }
  ]
}
```

Utilizzo di una Chiave KMS personalizzata:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
        ]
      },
      {
      "Effect": "Allow",
      "Action": [
      "kms:Encrypt"
      ],
      "Resource": [
        "arn:aws:kms:region:account_id:key/<kmskeyid>"
      ]
    }
  ]
```

```
}
```

La procedura seguente descrive come visualizzare il file JSON per questo documento nella console Amazon EC2.

Per visualizzare il file JSON per il documento Run Command per Systems Manager

1. Aprire la console Systems Manager all'indirizzo https://console.aws.amazon.com/systems-manager/home.
2. Nel riquadro di navigazione, espandere Shared Services (Servizi condivisi di Systems Manager) e scegliere Documents (Documenti).
3. Nella barra di ricerca, impostare Owner (Proprietario) come Owned by Me or Amazon (Di mia proprietà o di proprietà di Amazon) e impostare il Document name prefix (Prefisso del nome del documento) su `AWSSupport-RunEC2RescueForWindowsTool`.
4. Selezionare il documento `AWSSupport-RunEC2RescueForWindowsTool`, scegliere Contents (Indice), quindi visualizzare il file JSON.

Esempi

Di seguito sono descritti alcuni esempi su come utilizzare il documento Run Command di Systems Manager per eseguire EC2Rescue for Windows Server utilizzando AWS CLI. Per ulteriori informazioni sull'invio di comandi con AWS CLI, consulta il AWS CLI Command Reference.

Tentare di correggere tutti i problemi rilevati su un volume root offline

Tentare di correggere tutti i problemi rilevati su un volume root offline collegati a un'istanza Amazon EC2 Windows:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline volume xvdf" --parameters
 "Command=FixAll, Parameters='xvdf'" --output text
```

Raccolta dei log dall'istanza Amazon EC2 Windows corrente

Raccogliere tutti i log dall'istanza di Amazon EC2 Windows online corrente e caricarli su un bucket Amazon S3:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online log collection to S3" --
parameters "Command=CollectLogs, Parameters='YOURS3BUCKETNAME'" --output text
```

Raccolta dei log da un volume offline dell'istanza Amazon EC2 Windows

Per raccogliere tutti i log da un volume offline collegato a un'istanza di Amazon EC2 Windows e caricarli in Amazon S3 con un URL prefirmato:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline log collection to S3"
 --parameters "Command=CollectLogs, Parameters=\"-Offline -BlockDeviceName xvdf -
S3PreSignedUrl 'YOURS3PRESIGNEDURL'\"" --output text
```

Reimpostazione della password dell'amministratore locale

Gli esempi seguenti illustrano i metodi che puoi utilizzare per reimpostare la password dell'amministratore locale. L'output restituisce un collegamento a Parameter Store, dove è disponibile la password sicura generata causalmente che potrai utilizzare per eseguire una connessione RDP all'istanza Amazon EC2 Windows come amministratore locale.

Per reimpostare la password dell'amministratore locale di un'istanza online utilizzando l'alias/aws/ssm della AWS KMS key predefinita:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess" --output text
```

Per reimpostare la password dell'amministratore locale di un'istanza online utilizzando una Chiave KMS:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess, Parameters=a133dc3c-a2g4-4fc6-a873-6c0720104bf0" --output text
```

> **Note**
>
> In questo esempio la Chiave KMS è `a133dc3c-a2g4-4fc6-a873-6c0720104bf0`.

Console seriale EC2 per istanze Amazon EC2

Con la console seriale EC2, è possibile accedere alla porta seriale dell'istanza Amazon EC2 e utilizzarla per risolvere problemi di avvio, configurazione di rete e di altro tipo. La console seriale non richiede che l'istanza abbia funzionalità di rete. Con la console seriale, è possibile immettere comandi a un'istanza come se la tastiera e il monitor fossero collegati direttamente alla porta seriale dell'istanza. La sessione della console seriale resta attiva durante il riavvio e l'arresto dell'istanza. Durante il riavvio, sarà possibile visualizzare tutti i messaggi di avvio dall'inizio.

L'accesso alla console seriale non è disponibile per impostazione predefinita. L'organizzazione deve concedere l'accesso dell'account alla console seriale e configurare le policy IAM per concedere agli utenti l'accesso alla console seriale. L'accesso alla console seriale può essere controllato a livello granulare utilizzando ID istanza, tag delle risorse e altre leve IAM. Per ulteriori informazioni, consulta Configurazione dell'accesso alla console seriale EC2.

È possibile accedere alla console seriale utilizzando la console EC2 o la console AWS CLI.

La console seriale è disponibile senza costi aggiuntivi.

Argomenti

Prerequisiti per la console seriale EC2

Per connettersi alla console seriale EC2, devono sussistere i prerequisiti seguenti:

- Regioni AWS
- Zone Wavelength e AWS Outposts
- Zone locali
- Tipi di istanza
- Concessione dell'accesso
- Supporto per client basati su browser

- Stato istanza
- Amazon EC2 Systems Manager
- Configura lo strumento di risoluzione dei problemi scelto

Regioni AWS

Supportata in tutto. Regioni AWS

Zone Wavelength e AWS Outposts

Non supportato.

Zone locali

Supportato nelle zone locali.

Tipi di istanza

Tipi di istanze supportati:

- Linux
  - Tutte le istanze virtualizzate basate sul sistema Nitro.
  - Tutte le istanze bare metal eccetto:
    - Uso generale: `a1.metal`, `mac1.metal`, `mac2.metal`
    - Calcolo accelerato: `g5g.metal`
    - Memoria ottimizzata: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, `u-24tb1.metal`
- Windows

  Tutte le istanze virtualizzate basate sul sistema Nitro. Non supportato sulle istanze bare metal.

Concessione dell'accesso

Per concedere l'accesso alla Console seriale EC2 è necessario completare le seguenti attività di configurazione. Per ulteriori informazioni, consulta Configurazione dell'accesso alla console seriale EC2.

Supporto per client basati su browser

Per connettersi alla console seriale utilizzando il client basato su browser, il browser deve supportare. WebSocket Se il tuo browser non lo supporta WebSocket, connettiti alla console seriale utilizzando la tua chiave e un client SSH.

Stato istanza

Deve essere `running`.

Non è possibile connettersi alla console seriale se l'istanza è nello stato `pending`, `stopping`, `stopped`, `shutting-down` o `terminated`.

Per ulteriori informazioni sugli stati delle istanze, consulta Ciclo di vita dell'istanza.

Amazon EC2 Systems Manager

Se l'istanza utilizza Amazon EC2 Systems Manager, nell'istanza deve essere installato SSM Agent versione 3.0.854.0 o successiva. Per ulteriori informazioni su SSM Agent, consulta Utilizzo di SSM Agent nella Guida per l'utente di AWS Systems Manager .

Configura lo strumento di risoluzione dei problemi scelto

Per risolvere i problemi dell'istanza tramite la console seriale, è possibile utilizzare GRUB o SysRq su istanze Linux e Special Admin Console (SAC) su istanze Windows. Prima di poter utilizzare questi strumenti, devi prima eseguire i passaggi di configurazione su ogni istanza in cui li utilizzerai.

Usa le istruzioni relative al sistema operativo dell'istanza per configurare lo strumento di risoluzione dei problemi che hai scelto.

(istanze Linux) Configura GRUB

Per configurare GRUB, seleziona una delle procedure seguenti in base all'AMI utilizzata per avviare l'istanza.

Amazon Linux 2

Per configurare GRUB su un'istanza Amazon Linux 2

1. Connessione all'istanza di Linux
2. Aggiungi o modifica le seguenti opzioni in `/etc/default/grub`:

- Imposta `GRUB_TIMEOUT=1`.
- Add `GRUB_TERMINAL="console serial"`.
- Add `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

Di seguito è riportato un esempio di `/etc/default/grub`. Potrebbe essere necessario modificare la configurazione in base alle impostazioni del sistema.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
GRUB_TIMEOUT=1
GRUB_DISABLE_RECOVERY="true"
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Applica la configurazione aggiornata emettendo il comando seguente.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Ubuntu

Per configurare GRUB su un'istanza Ubuntu

1. Connettiti alla tua istanza.
2. Aggiungi o modifica le seguenti opzioni in `/etc/default/grub.d/50-cloudimg-settings.cfg`:
   - Imposta `GRUB_TIMEOUT=1`.
   - Add `GRUB_TIMEOUT_STYLE=menu`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Remove `GRUB_HIDDEN_TIMEOUT`.
   - Add `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Di seguito è riportato un esempio di `/etc/default/grub.d/50-cloudimg-settings.cfg`. Potrebbe essere necessario modificare la configurazione in base alle impostazioni del sistema.

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process

# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295"

# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Applica la configurazione aggiornata emettendo il comando seguente.

```
[ec2-user ~]$ sudo update-grub
```

RHEL

Per configurare GRUB su un'istanza RHEL

1. Connettiti alla tua istanza.
2. Aggiungi o modifica le seguenti opzioni in `/etc/default/grub`:
   - Remove `GRUB_TERMINAL_OUTPUT`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Add `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Di seguito è riportato un esempio di `/etc/default/grub`. Potrebbe essere necessario modificare la configurazione in base alle impostazioni del sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
```

```
GRUB_DISABLE_SUBMENU=true
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Applica la configurazione aggiornata emettendo il comando seguente.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

CentOS

Per le istanze avviate utilizzando un'AMI CentOS, GRUB per la console seriale è configurato per impostazione predefinita.

Di seguito è riportato un esempio di `/etc/default/grub`. La configurazione potrebbe essere diversa in base alle impostazioni del sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

(Istanze Linux) Configura SysRq

Per configurare SysRq, si abilitano i SysRq comandi per il ciclo di avvio corrente. Per rendere persistente la configurazione, puoi anche abilitare i SysRq comandi per gli avvii successivi.

Per abilitare tutti SysRq i comandi per il ciclo di avvio corrente

1. Connettiti alla tua istanza.
2. Esegui il comando riportato qui di seguito.

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

> **Note**
>
> Questa impostazione sarà cancellata al riavvio successivo.

Per abilitare tutti i SysRq comandi per gli avvii successivi

1. Crea il file `/etc/sysctl.d/99-sysrq.conf` e aprilo nel tuo editor preferito.

```
[ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
```

2. Aggiungi la seguente riga.

```
kernel.sysrq=1
```

3. Riavvia l'istanza per applicare le modifiche.

```
[ec2-user ~]$ sudo reboot
```

4. Al prompt di `login`, specifica il nome utente dell'utente con password configurato in precedenza quindi premi Invio.
5. Al prompt di `Password`, specifica la password e premi Invio.

(Istanze Windows) Abilita SAC e il menu di avvio

> **Note**
>
> Se si abilita SAC su un'istanza, i servizi EC2 che si basano sul recupero della password non funzioneranno dalla console Amazon EC2. Gli agenti di avvio di Windows su Amazon EC2 (EC2Config, EC2Launch v1 e EC2Launch v2) si affidano alla console seriale per eseguire varie attività. Queste attività non vengono eseguite correttamente quando si abilita SAC su un'istanza. Per ulteriori informazioni sugli agenti di lancio di Windows on Amazon EC2, consulta. the section called “Configura le istanze Windows” Se abiliti SAC, puoi disabilitarlo in un secondo momento. Per ulteriori informazioni, consulta Disabilitazione di SAC e del menu di avvio.

Utilizzare uno dei seguenti metodi per abilitare SAC e il menu di avvio su un'istanza.

PowerShell

Per abilitare SAC e il menu di avvio in un'istanza di Windows

1. Connect all'istanza ed esegui i seguenti passaggi da una riga di PowerShell comando elevata.
2. Abilita SAC.

```
bcdedit /ems '{current}' on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Abilita il menu di avvio.

```
bcdedit /set '{bootmgr}' displaybootmenu yes
bcdedit /set '{bootmgr}' timeout 15
bcdedit /set '{bootmgr}' bootems yes
```

4. Applica la configurazione aggiornata riavviando l'istanza.

```
shutdown -r -t 0
```

Command prompt

Per abilitare SAC e il menu di avvio in un'istanza di Windows

1. Connettiti all'istanza ed esegui la procedura dal prompt dei comandi.
2. Abilita SAC.

```
bcdedit /ems {current} on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Abilita il menu di avvio.

```
bcdedit /set {bootmgr} displaybootmenu yes
bcdedit /set {bootmgr} timeout 15
bcdedit /set {bootmgr} bootems yes
```

4. Applica la configurazione aggiornata riavviando l'istanza.

```
shutdown -r -t 0
```

Configurazione dell'accesso alla console seriale EC2

Per configurare l'accesso alla console seriale, è necessario concedere l'accesso alla console a livello di account e quindi configurare le policy IAM per concedere l'accesso agli utenti. Per le istanze Linux è inoltre necessario configurare un utente basato su password su ogni istanza in modo che gli utenti possano utilizzare la console seriale per la risoluzione dei problemi.

Prima di iniziare, assicurati di controllare ilprerequisiti.

Argomenti

- Livelli di accesso alla console seriale EC2
- Gestione dell'accesso con account alla console seriale EC2
- Configurazione di policy IAM per l'accesso alla console seriale EC2
- Imposta una password utente del sistema operativo su un'istanza Linux

Livelli di accesso alla console seriale EC2

Per impostazione predefinita, non è possibile accedere alla console seriale a livello di account. L'accesso alla console seriale a livello di account va concesso esplicitamente. Per ulteriori informazioni, consulta Gestione dell'accesso con account alla console seriale EC2.

È possibile utilizzare una policy di controllo dei servizi (SCP) per consentire l'accesso alla console seriale all'interno dell'organizzazione. È quindi possibile avere un controllo di accesso granulare a livello utente utilizzando una policy IAM per il controllo dell'accesso. Utilizzando una combinazione di policy SCP e IAM, si avranno diversi livelli di controllo dell'accesso alla console seriale.

Livello di organizzazione

> È possibile utilizzare una policy di controllo dei servizi (SCP) per consentire l'accesso alla console seriale per gli account membri all'interno dell'organizzazione. Per ulteriori informazioni sulle SCP, consulta Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

Livello di istanza

È possibile configurare le politiche di accesso alla console seriale utilizzando IAM PrincipalTag e ResourceTag costruzioni e specificando le istanze in base al loro ID. Per ulteriori informazioni, consulta Configurazione di policy IAM per l'accesso alla console seriale EC2.

Livello utente

È possibile configurare l'accesso a livello di utente configurando una policy IAM per consentire o negare a un utente specificato l'autorizzazione per eseguire il push della chiave pubblica SSH al servizio della console seriale di una determinata istanza. Per ulteriori informazioni, consulta Configurazione di policy IAM per l'accesso alla console seriale EC2.

Livello di sistema operativo (solo istanze Linux)

È possibile impostare una password utente a livello del sistema operativo guest. In questo modo è possibile accedere alla console seriale per alcuni casi d'uso. Tuttavia, per monitorare i log, non è necessario un utente con password. Per ulteriori informazioni, consulta Imposta una password utente del sistema operativo su un'istanza Linux.

Gestione dell'accesso con account alla console seriale EC2

Per impostazione predefinita, non è possibile accedere alla console seriale a livello di account. L'accesso alla console seriale a livello di account va concesso esplicitamente.

Argomenti

- Concessione dell'autorizzazione agli utenti per gestire l'accesso con account
- Visualizzazione dello stato di accesso account alla console seriale
- Concessione dell'accesso con account alla console seriale
- Negare l'accesso con account alla console seriale

Concessione dell'autorizzazione agli utenti per gestire l'accesso con account

Per consentire agli utenti di gestire l'accesso con account alla console seriale EC2, è necessario concedere loro le autorizzazioni IAM necessarie.

La policy seguente concede le autorizzazioni per visualizzare lo stato dell'account e per consentire e impedire l'accesso con account alla console seriale EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

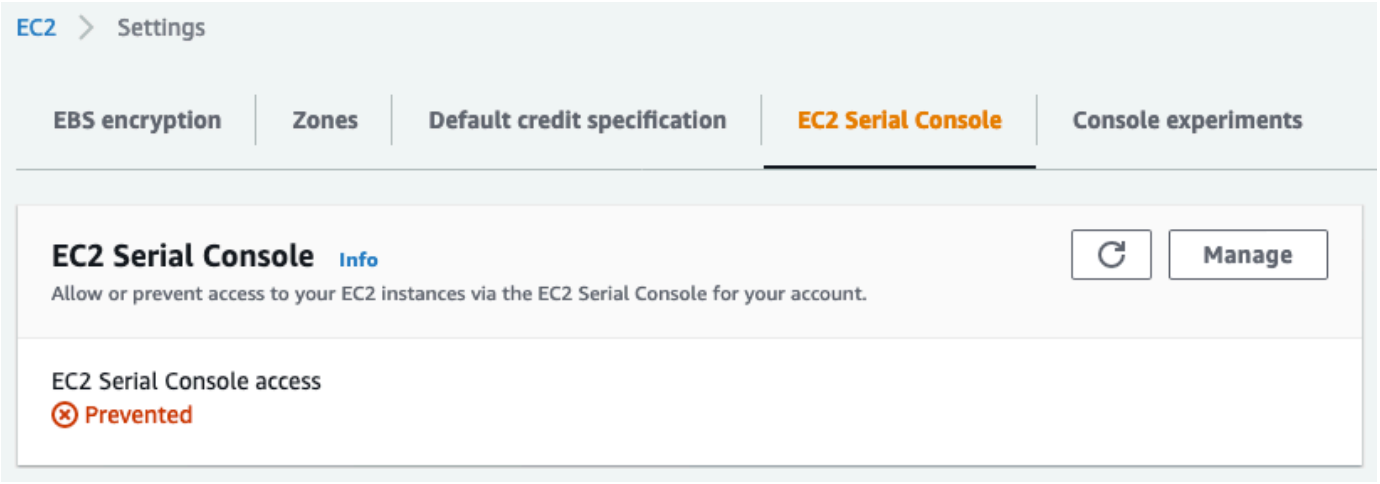
Visualizzazione dello stato di accesso account alla console seriale

Per visualizzare lo stato di accesso con account alla console seriale (console)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, selezionare EC2 Dashboard (Pannello di controllo EC2).
3. Da Attributi account, seleziona Console seriale EC2.

   Il campo di Accesso alla console seriale EC2 indica se l'accesso con account è consentito o impedito.

   La seguente schermata mostra che l'account non può utilizzare la console seriale EC2.



Per visualizzare lo stato di accesso con account alla console seriale (AWS CLI)

Utilizzare il comando get-serial-console-access-status per visualizzare lo stato di accesso all'account sulla console seriale.

```
aws ec2 get-serial-console-access-status --region us-east-1
```

Nell'output seguente, `true` indica che all'account è consentito accedere alla console seriale.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Concessione dell'accesso con account alla console seriale

Per concedere l'accesso con account alla console seriale (console)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, selezionare EC2 Dashboard (Pannello di controllo EC2).
3. Da Attributi account, seleziona Console seriale EC2.
4. Scegliere Gestisci.
5. Per consentire l'accesso alla console seriale EC2 di tutte le istanze dell'account, seleziona la casella di controllo Consenti.
6. Scegliere Update (Aggiorna).

Per concedere l'accesso con account alla console seriale (AWS CLI)

Usa il enable-serial-console-accesscomando per consentire l'accesso dell'account alla console seriale.

```
aws ec2 enable-serial-console-access --region us-east-1
```

Nell'output seguente, `true` indica che all'account è consentito accedere alla console seriale.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Negare l'accesso con account alla console seriale

Per negare l'accesso con account alla console seriale (console)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, selezionare EC2 Dashboard (Pannello di controllo EC2).
3. Da Attributi account, seleziona Console seriale EC2.
4. Scegliere Gestisci.
5. Per impedire l'accesso alla console seriale EC2 di tutte le istanze dell'account, deseleziona la casella di controllo Consenti.
6. Scegliere Update (Aggiorna).

Per negare l'accesso con account alla console seriale (AWS CLI)

Usa il disable-serial-console-accesscomando per impedire l'accesso dell'account alla console seriale.

```
aws ec2 disable-serial-console-access --region us-east-1
```

Nell'output seguente, `false` indica che all'account viene negato l'accesso alla console seriale.

```
{
    "SerialConsoleAccessEnabled": false
}
```

Configurazione di policy IAM per l'accesso alla console seriale EC2

Per impostazione predefinita, gli utenti non hanno accesso alla console seriale. L'organizzazione deve configurare le policy IAM per concedere agli utenti di accedere. Per ulteriori informazioni, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per l'accesso alla console seriale, crea un documento di policy JSON che includa l'operazione `ec2-instance-connect:SendSerialConsoleSSHPublicKey`. Questa operazione concede a un utente l'autorizzazione per eseguire il push della chiave pubblica al servizio della console seriale, che avvia una sessione della console. Consigliamo di limitare l'accesso a specifiche istanze EC2. In caso contrario, tutti gli utenti con questa autorizzazione potranno connettersi alla console seriale di tutte le istanze EC2.

Policy IAM di esempio

- Consenti esplicitamente l'accesso alla console seriale
- Negare esplicitamente l'accesso alla console seriale
- Utilizzo di tag di risorse per controllare l'accesso alla console seriale

Consenti esplicitamente l'accesso alla console seriale

Per impostazione predefinita, nessuno ha accesso alla console seriale. Per concedere l'accesso alla console seriale, è necessario configurare una policy in modo da consentirlo esplicitamente. Si consiglia di configurare una policy che limiti l'accesso a istanze specifiche.

La seguente policy consente di accedere alla console seriale di un'istanza specifica, identificata dal relativo ID istanza.

Tieni presente che le operazioni `DescribeInstances`, `DescribeInstanceTypes` e `GetSerialConsoleAccessStatus` non supportano le autorizzazioni a livello di risorsa e pertanto tutte le risorse contrassegnate da `*` (asterisco) devono essere specificate per queste operazioni.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Negare esplicitamente l'accesso alla console seriale

La seguente policy IAM consente l'accesso alla console seriale di tutte le istanze, indicata con * (asterisco), e nega esplicitamente l'accesso alla console seriale di un'istanza specifica, identificata dal relativo ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Utilizzo di tag di risorse per controllare l'accesso alla console seriale

È possibile utilizzare i tag delle risorse per controllare l'accesso alla console seriale di un'istanza.

Il controllo degli accessi basato sugli attributi è una strategia di autorizzazione che definisce le autorizzazioni in base a tag che possono essere allegati a utenti e risorse. AWS Ad esempio, la policy seguente consente a un utente di avviare una connessione alla console seriale per un'istanza solo se il tag risorsa dell'istanza e il tag dell'entità hanno lo stesso valore `SerialConsole` per la chiave di tag.

Per ulteriori informazioni sull'utilizzo dei tag per controllare l'accesso alle AWS risorse, consulta Controlling access to AWS resources nella IAM User Guide.

Tieni presente che le operazioni `DescribeInstances`, `DescribeInstanceTypes` e `GetSerialConsoleAccessStatus` non supportano le autorizzazioni a livello di risorsa e pertanto tutte le risorse contrassegnate da * (asterisco) devono essere specificate per queste operazioni.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole":
 "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

Imposta una password utente del sistema operativo su un'istanza Linux

> **Note**
>
> Questa sezione si applica solo alle istanze Linux.

È possibile connettersi alla console seriale senza utilizzare una password. Tuttavia, per utilizzare la console seriale per la risoluzione dei problemi di un'istanza Linux, l'istanza deve avere un utente del sistema operativo basato su password.

È possibile impostare la password per qualsiasi utente del sistema operativo, incluso l'utente root. Tieni presente che l'utente root può modificare tutti i file, mentre ogni utente del sistema operativo potrebbe avere autorizzazioni limitate.

È necessario impostare una password utente per ogni istanza per la quale si utilizzerà la console seriale. Si tratta di una procedura da eseguire una volta sola per ciascuna istanza.

> **Note**
>
> Le seguenti istruzioni sono applicabili solo se l'istanza è stata avviata utilizzando un'AMI Linux fornita da AWS perché, per impostazione predefinita, le AMI fornite da non AWS sono configurate con un utente basato su password. Se l'istanza è stata avviata utilizzando un'AMI che dispone già della password utente root configurata, è possibile ignorare queste istruzioni.

Per impostare una password utente del sistema operativo su un'istanza Linux

1. Connettiti alla tua istanza. È possibile utilizzare qualsiasi metodo per il collegamento all'istanza ad eccezione del metodo di connessione della console seriale EC2.
2. Per impostare la password per un utente, utilizza il comando passwd. Nell'esempio seguente, l'utente è `root`.

   ```
   [ec2-user ~]$ sudo passwd root
   ```

   Di seguito è riportato un output di esempio.

   ```
   Changing password for user root.
   ```

```
New password:
```

3. Al prompt di `New password`, specifica la nuova password.
4. Al prompt, immetti di nuovo la password.

Connessione alla console seriale EC2

Puoi connetterti alla console seriale dell'istanza EC2 utilizzando la console Amazon EC2 o tramite SSH. Dopo la connessione alla console seriale, sarà possibile utilizzarla per la risoluzione dei problemi di avvio, di configurazione di rete e di altro tipo. Per ulteriori informazioni sulla risoluzione dei problemi, consulta Risolvi i problemi della tua istanza Amazon EC2 utilizzando la console seriale EC2.

Considerazioni

- È supportata 1 sola connessione alla console seriale attiva per istanza.
- La connessione alla console seriale dura in genere 1 ora, a meno che non venga interrotta. Tuttavia, durante la manutenzione del sistema, Amazon EC2 interromperà la sessione della console.
- Perché possa essere avviata una nuova sessione dopo la disconnessione dalla console seriale, sono necessari 30 secondi.
- Porte console seriali supportate: `ttyS0` (istanze Linux) e `COM1` (istanze Windows)
- Quando ti connetti alla console seriale, è possibile che vi sia un leggero calo della velocità effettiva dell'istanza.

Argomenti

- Connessione tramite client basato su browser
- Connessione tramite la propria chiave e un client SSH
- Endpoint e impronte digitali della console seriale EC2

Connessione tramite client basato su browser

Puoi connetterti alla console seriale dell'istanza EC2 utilizzando il client basato su browser. A tale scopo, seleziona l'istanza nella console Amazon EC2 e sceglie di connetterti alla console seriale. Il client basato su browser gestisce le autorizzazioni e garantisce una corretta connessione.

La console seriale EC2 funziona dalla maggior parte dei browser e supporta l'input di tastiera e mouse.

Prima di effettuare la connessione, assicurati di avere soddisfatto tutti i prerequisiti.

Per connettersi alla porta seriale dell'istanza utilizzando il client basato su browser (console Amazon EC2)

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Puoi selezionare l'istanza e scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), EC2 Serial Console (Console seriale EC2), Connect (Connetti).

   In alternativa, puoi selezionare l'istanza e scegliere Connect (Connetti), EC2 Serial Console (Console seriale EC2), Connect (Connetti).

   Verrà aperta una finestra del terminale nel browser.
4. Premi Invio. Se viene restituito un prompt di accesso, allora significa che sei connesso alla console seriale.

   Se lo schermo rimane nero, potrai utilizzare le seguenti informazioni per risolvere i problemi relativi alla connessione alla console seriale:

   - Verifica di aver configurato l'accesso alla console seriale. Per ulteriori informazioni, consulta Configurazione dell'accesso alla console seriale EC2.
   - (Solo istanze Linux) Utilizzare SysRq per connettersi alla console seriale. SysRq non richiede la connessione tramite il client basato su browser. Per ulteriori informazioni, consulta (istanze Linux) Utilizzatelo SysRq per risolvere i problemi della vostra istanza.
   - (Solo istanze Linux) Riavvia getty. Se hai accesso SSH alla tua istanza, connettiti alla tua istanza usando SSH e riavvia getty usando il seguente comando.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```
   - Riavviare l'istanza. Puoi riavviare l'istanza utilizzando SysRq (istanze Linux), la console EC2 o il. AWS CLI Per ulteriori informazioni, consulta (istanze Linux) Utilizzatelo SysRq per risolvere i problemi della vostra istanza (istanze Linux) o. Riavvio dell'istanza

5. (Solo istanze Linux) Al **`login`** prompt, immettete il nome utente dell'utente basato su password che avete impostato in precedenza, quindi premete Invio.
6. (Solo istanze Linux) Al **`Password`** prompt, immettete la password, quindi premete Invio.

Ora sei connesso all'istanza e puoi utilizzare la console seriale per la risoluzione dei problemi.

Connessione tramite la propria chiave e un client SSH

Puoi utilizzare la tua chiave SSH e connetterti all'istanza dal client SSH preferito durante l'utilizzo dell'API della console seriale. In questo modo, potrai sfruttare la capacità della console seriale di inviare una chiave pubblica all'istanza.

Prima di effettuare la connessione, assicurati di avere soddisfatto tutti i prerequisiti.

Per connettersi alla console seriale di un'istanza utilizzando SSH

1. Invia la tua chiave pubblica SSH nell'istanza per avviare una sessione di console seriale

   Usa il comando send-serial-console-ssh-public-key per inviare la tua chiave pubblica SSH all'istanza. Verrà avviata una sessione di console seriale.

   Se per questa istanza è già stata avviata una sessione della console seriale, il comando avrà esito negativo perché è possibile aprire una sola sessione alla volta. Perché possa essere avviata una nuova sessione dopo la disconnessione dalla console seriale, sono necessari 30 secondi.

   ```
   aws ec2-instance-connect send-serial-console-ssh-public-key \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --serial-port 0 \
       --ssh-public-key file://my_key.pub \
       --region us-east-1
   ```

2. Connessione alla console seriale utilizzando la chiave privata

   Utilizza il comando ssh per connetterti alla console seriale prima che la chiave pubblica venga rimossa dal servizio della console seriale. Hai 60 secondi prima che la chiave venga rimossa.

   Utilizza la chiave privata corrispondente alla chiave pubblica.

   Il formato del nome utente è `instance-id.port0`, che comprende l'ID istanza e la porta 0. Nell'esempio seguente, il nome utente è `i-001234a4bf70dec41EXAMPLE.port0`.

L'endpoint del servizio della console seriale è diverso per ogni Regione. Consulta la tabella Endpoint e impronte digitali della console seriale EC2 per l'endpoint di ogni regione. Nell'esempio seguente, il servizio della console seriale si trova nella regione *us-est-1*.

```
ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
```

3. (Facoltativo) Verifica dell'impronta digitale

   Quando ti connetti per la prima volta alla console seriale, ti sarà richiesto di confermare l'impronta digitale. Puoi confrontare l'impronta digitale della console seriale con l'impronta digitale visualizzata per la verifica. Se queste impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco "». man-in-the-middle Se corrispondono, potrai tranquillamente connetterti alla console seriale.

   La seguente impronta digitale è per il servizio della console seriale nella regione us-est-1. Per le impronte digitali di ciascuna regione, consulta Endpoint e impronte digitali della console seriale EC2.

   ```
   SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
   ```

   > **Note**
   >
   > L'impronta digitale viene visualizzata solo la prima volta che ci si connette alla console seriale.

4. Premi Invio. Se viene restituito un prompt, allora significa che sei connesso alla console seriale.

   Se lo schermo rimane nero, potrai utilizzare le seguenti informazioni per risolvere i problemi relativi alla connessione alla console seriale:

   - Verifica di aver configurato l'accesso alla console seriale. Per ulteriori informazioni, consulta Configurazione dell'accesso alla console seriale EC2.
   - (Solo istanze Linux) Utilizzare SysRq per connettersi alla console seriale. SysRq non richiede la connessione tramite SSH. Per ulteriori informazioni, consulta (istanze Linux) Utilizzatelo SysRq per risolvere i problemi della vostra istanza.
   - (Solo istanze Linux) Riavvia getty. Se hai accesso SSH alla tua istanza, connettiti alla tua istanza usando SSH e riavvia getty usando il seguente comando.

```
[ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
```

- Riavviare l'istanza. Puoi riavviare l'istanza utilizzando SysRq (solo istanze Linux), la console EC2 o il. AWS CLI Per ulteriori informazioni, consulta (istanze Linux) Utilizzatelo SysRq per risolvere i problemi della vostra istanza (solo istanze Linux) o. Riavvio dell'istanza

5. (Solo istanze Linux) Al **`login`** prompt, immettete il nome utente dell'utente basato su password che avete impostato in precedenza, quindi premete Invio.
6. (Solo istanze Linux) Al **`Password`** prompt, immettete la password, quindi premete Invio.

Ora sei connesso all'istanza e puoi utilizzare la console seriale per la risoluzione dei problemi.

Endpoint e impronte digitali della console seriale EC2

Di seguito sono riportati gli endpoint e le impronte digitali del servizio per la console seriale EC2. Per connettersi a livello di codice alla console seriale di un'istanza, viene utilizzato un endpoint della console seriale EC2. Gli endpoint e le impronte digitali della console seriale EC2 sono unici per ogni Regione AWS .

Nome della regione	Regione	Endpoint	Impronta digitale
Stati Uniti orientali (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256: TY7TRSZZ26xBB0/HVV9JRM7MCZN0xW/d/0EhwPkTzRt
US East (N. Virginia)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256DiJa: DXWN5mA/xadvmebzgerU5L2GX+Yi5L LucZ0fMMW
US West (N. Californi a)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256:OH ldlcMET8u 7QLSX3jmR TRAPFHVtq byoLZBMUCqiH3Y

Nome della regione	Regione	Endpoint	Impronta digitale
US West (Oregon)	us-west-2	serial-console.ec2-instance-connect.us-west-2.aws	SHA256: EMCIE23 Bi6yg AVhA1O2Jx VUC TqKa HainqZcMwqNkDhh
Africa (Cape Town)	af-south-1	ec2-serial-console.af-south-1.api.aws	SHA256: RMWWZ2 jUqZJo5JL2K 21ED00BiIWI fVePe IgXsczoHlz
Asia Pacifico (Hong Kong)	ap-east-1	ec2-serial-console.ap-east-1.api.aws	SHA256: T0Q1 Z P7TKM2xxVIC9BJ lpiXxCho HplnAkjb FsjYnifk
Asia Pacific (Hyderabad)	ap-south-2	ec2-serial-console.ap-south-2.api.aws	SHA256: WJGPBSWv4/SHN +OPIT ValoewAuYj 15dVW845jeHDKRS
Asia Pacifico (Giacarta)	ap-southeast-3	ec2-serial-console.ap-southeast-3.api.aws	SHA 256:5+LFN S32xiTQL/4o0ziFBX4 BzgSyFQY3o8MiK ZwgrCh
Asia Pacifico (Melbourne)	ap-southeast-4	ec2-serial-console.ap-southeast-4.api.aws	SHA hFgLvjn 256: AVAQ27 5GTsSHz0o V7h90p0gg 46wfoET6zJVM
Asia Pacific (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256: OBL Heblia XcYmklq H8ISO51re zTPIsm35bsu40 RxEg

Nome della regione	Regione	Endpoint	Impronta digitale
Asia Pacifico (Osaka-Locale)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256: AM0/JiBK9 AXsGEV3G8TU/ VVHFXE/3uCYJSQ BnBuFnHr
Asia Pacifico (Seul)	ap-northeast-2	serial-console.ec2-instance-connect.ap-northeast-2.aws	SHA256:FoqWXNX +DZ++GuNTztg9 PK49WYMqBX +FrcZM2dSrqrI
Asia Pacific (Singapore)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256: PLFNN7WNC QDHx3QMWLu1GY/ O8TUx7L QgZua C6L45COY
Asia Pacific (Sydney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256: UK9LEUQJQ TRoxXZUN+CW9/ VSE9W984CF5TGZ O4 yFvMw
Asia Pacifico (Tokyo)	ap-northeast-1	serial-console.ec2-instance-connect.ap-northeast-1.aws	SHA256: RQFSDCZT TRDV1T9EM/ HMRFQE+crLiot5um4 K OfQawew
Canada (Central)	ca-central-1	serial-console.ec2-instance-connect.ca-central-1.aws	SHA256: P2O2jo O6YW738Fi OthDU ZwmpMwkp 2gCzYmMo7S4 TyEv

Nome della regione	Regione	Endpoint	Impronta digitale
China (Beijing)	cn-north-1	ec2-serial-console.cn-north-1.api.amazonwebservices.com.cn	SHA 256:2 GHvFY4H7U U3+WAFUXD28V/ LGGT+y ggMeqjvSl gngpg
Cina (Ningxia)	cn-northwest-1	ec2-serial-console.cn-northwest-1.api.amazonwebservices.com.cn	SHA OdVf 256: TDGRNZKIQ YeBUHO4SZ UA09VWI5R yozgToGPWMIM
Europe (Frankfurt)	eu-central-1	serial-console.ec2-instance-connect.eu-central-1.aws	SHA256: ACMFS/ yIcOd OlkXvOl 8aMz1TOE+ BBNRJJ3FY 0K0DE2C
Europa (Irlanda)	eu-west-1	serial-console.ec2-instance-connect.eu-west-1.aws	SHA256: h2aagawo4 hAThhtm6eZs3bj7udg uxi2 qTrHj ZaWCw6e
Europe (London)	eu-west-2	serial-console.ec2-instance-connect.eu-west-2.aws	SHA256: RnJg A69rd5ce/ AEG4AMM53 i6LKD1ZPVS/BCV3ttp W2 8
Europa (Milano)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256: LC0KOV JnpgFy BVRxn0a7n 99eclbxsx95cuus7x7 qk30
Europe (Paris)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:q8ldnAf9pym eNe8BnFVngY3RPAr/ kxswJUzfrlxeEWs

Nome della regione	Regione	Endpoint	Impronta digitale
Europa (Spagna)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256: gocw2dfrl u669q R6fzUz/4f 4n7t45 NxqFxEcs ZcwoEc
Europa (Stoccolma)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256: tkgffuVU gss3cu8gDL6w2ui32e pnpKFKLwx84 DvocDi
Europa (Zurigo)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA 256:8 PPx2mbmF6 0N M4/4OaxFu TQXWP6mK WdCw UlzKfw IfRz
Israele (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256: NvtYy JR6Q8V6KN NPI8+QSFQ 4DJ5DimNM ZPTGWGSM1S U
Medio Oriente (Bahrein)	me-south-1	ec2-serial-console .me-south-1.api.aws	SHA256: npjllkhu2 QnLdUq 2kvarsok5 xVPjomrjkcbzcdqc3k8
Medio Oriente (Emirati Arabi Uniti)	me-central-1	ec2-serial-console .me-central-1.api.aws	SHA256: ZPB5DUKIB Z+L0 B4MP di dFwPeyyk HI/xzxnef sdkbvle
Sud America (São Paulo)	sa-east-1	serial-console.ec2-instance-connect.sa-east-1.aws	SHA256: RD2+/32OG NJEW1YVieMe NaQz C+BOTBIH6 2OQAPDQ1DI

Nome della regione	Regione	Endpoint	Impronta digitale
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	serial-console.ec2-instance-connect.us-gov-east-1.amazonaws.com	SHA256: TIWE19IkqnDcZnmtebvGWSOYLCLRTVU38yeeh+DH F 28
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	serial-console.ec2-instance-connect.us-gov-west-1.amazonaws.com	SHA256: KFOFRWLAOZFB+UTBD3BRF88ngO2YZLQx 5DQOlPf ZiIw

Disconnettiti dalla console seriale EC2

Se non è più necessario essere connessi alla console seriale EC2 dell'istanza, è possibile disconnettersi da essa. Quando ci si disconnette dalla console seriale, qualsiasi sessione di shell in esecuzione sull'istanza continuerà a essere eseguita. Se vuoi terminare la sessione shell, dovrai terminarla prima di disconnetterti dalla console seriale.

Considerazioni

- La connessione alla console seriale dura in genere 1 ora, a meno che non venga interrotta. Tuttavia, durante la manutenzione del sistema, Amazon EC2 interromperà la sessione della console.
- Perché possa essere avviata una nuova sessione dopo la disconnessione dalla console seriale, sono necessari 30 secondi.

Il modo per disconnettersi dalla console seriale dipende dal client.

Client basato su browser

Per terminare la sessione della console seriale, è sufficiente chiudere la finestra del terminale della console seriale nel browser.

Client OpenSSH standard

Per terminare la sessione della console seriale, utilizza il comando riportato di seguito per chiudere la connessione SSH. Questo comando deve essere eseguito immediatamente dopo una nuova riga.

```
~.
```

Il comando utilizzato per chiudere una connessione SSH potrebbe essere diverso a seconda del client SSH utilizzato.

Risolvi i problemi della tua istanza Amazon EC2 utilizzando la console seriale EC2

Grazie alla console seriale EC2, puoi risolvere i problemi di avvio, configurazione di rete e di altro tipo semplicemente collegandoti alla porta seriale dell'istanza.

Utilizza le istruzioni relative al sistema operativo dell'istanza e allo strumento che hai configurato sull'istanza.

> **Note**
>
> Prima di iniziare, assicurati di aver completato i prerequisiti, inclusa la configurazione dello strumento di risoluzione dei problemi scelto.

(istanze Linux) Usa GRUB per risolvere i problemi della tua istanza

GNU GRUB (abbreviazione di GNU Grand Unified Bootloader, comunemente chiamato GRUB) è il boot loader predefinito per la maggior parte dei sistemi operativi Linux. Dal menu di GRUB, è possibile selezionare il kernel in cui avviare o modificare le voci del menu per cambiare il modo in cui il kernel verrà avviato. Ciò può essere utile durante la risoluzione dei problemi di un'istanza con esito negativo.

Il menu di GRUB viene visualizzato durante il processo di avvio. Non è possibile accedere al menu tramite il normale SSH ma è possibile accedervi tramite la console seriale EC2.

È possibile eseguire l'avvio in modalità utente singolo o in modalità di emergenza. La modalità utente singolo avvierà il kernel con un runlevel inferiore. Ad esempio, potrebbe montare il filesystem ma non attivare la rete, dandoti la possibilità di eseguire la manutenzione necessaria per correggere l'istanza. La modalità di emergenza è simile alla modalità utente singolo tranne per il fatto che il kernel viene eseguito al runlevel più basso possibile.

Per eseguire l'avvio in modalità utente singolo

1. Connettiti alla console seriale dell'istanza.
2. Riavviare l'istanza utilizzando il comando seguente.

   ```
   [ec2-user ~]$ sudo reboot
   ```
3. Durante il riavvio, quando appare il menu di GRUB, premi un tasto qualsiasi per interrompere il processo di avvio.
4. Nel menu di GRUB, utilizzare i tasti freccia per selezionare il kernel in cui eseguire l'avvio, quindi premi e sulla tastiera.
5. Utilizza i tasti freccia per posizionare il cursore sulla riga contenente il kernel. La riga inizia con `linux` o `linux16` a seconda dell'AMI utilizzata per avviare l'istanza. Per Ubuntu, due righe iniziano con `linux` ed entrambe devono essere modificate nel passaggio successivo.
6. Alla fine della riga, aggiungi la parola `single`.

   Di seguito è riportato un esempio per Amazon Linux 2.

   ```
   linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
   dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
   s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
   ll=0 single
   ```
7. Premi Ctrl+X per eseguire l'avvio in modalità utente singolo.
8. Al prompt di `login`, specifica il nome utente dell'utente con password configurato in precedenza quindi premi Invio.
9. Al prompt di `Password`, specifica la password e premi Invio.

Per avviare la modalità di emergenza

Segui gli stessi passaggi della modalità utente singolo, ma al passaggio 6 aggiungi la parola `emergency` anzichésingle.

(istanze Linux) Utilizzatelo SysRq per risolvere i problemi della vostra istanza

La chiave System Request (SysRq), a volte chiamata «magic SysRq «, può essere usata per inviare un comando direttamente al kernel, all'esterno di una shell, e il kernel risponderà indipendentemente

da ciò che sta facendo il kernel. Ad esempio, se l'istanza ha smesso di rispondere, puoi usare la SysRq chiave per dire al kernel di bloccarsi o riavviarsi. Per ulteriori informazioni, consulta Magic SysRq key in Wikipedia.

È possibile utilizzare SysRq i comandi nel client basato su browser della console seriale EC2 o in un client SSH. Il comando per inviare una richiesta di interruzione è diverso per ogni client.

Per utilizzarli SysRq, scegli una delle seguenti procedure in base al client che stai utilizzando.

Browser-based client

Da utilizzare SysRq nella console seriale (client basato su browser)

1. Connettiti alla console seriale dell'istanza.
2. Per inviare una richiesta di interruzione, premi il tasto `CTRL+0` (zero). Se la tastiera lo supporta, puoi inviare una richiesta di interruzione anche utilizzando il tasto Pausa o Interrompi.

   ```
   [ec2-user ~]$ CTRL+0
   ```

3. Per impartire un SysRq comando, premi il tasto sulla tastiera che corrisponde al comando richiesto. Ad esempio, per visualizzare un elenco di SysRq comandi, premeteh.

   ```
   [ec2-user ~]$ h
   ```

   L'output del comando h è simile al seguente.

   ```
   [ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
   tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
   (j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
   tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
   ) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
   buffer(z)
   ```

SSH client

Da utilizzare SysRq in un client SSH

1. Connettiti alla console seriale dell'istanza.

2. Per inviare una richiesta di interruzione, premi ~B (tilde, seguita da B maiuscolo).

```
[ec2-user ~]$ ~B
```

3. Per impartire un SysRq comando, premi il tasto sulla tastiera che corrisponde al comando richiesto. Ad esempio, per visualizzare un elenco di SysRq comandi, premeteh.

```
[ec2-user ~]$ h
```

L'output del comando h è simile al seguente.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

> **Note**
>
> Il comando utilizzato per l'invio di una richiesta di interruzione potrebbe essere diverso a seconda del client SSH che si sta utilizzando.

(Istanze Windows) Utilizzate SAC per risolvere i problemi dell'istanza

La funzionalità Special Admin Console (SAC) di Windows consente di risolvere i problemi relativi a un'istanza di Windows. Collegandosi alla console seriale dell'istanza e utilizzando SAC, potrai interrompere il processo di avvio e avviare Windows in modalità provvisoria.

> **Note**
>
> Se si abilita SAC su un'istanza, i servizi EC2 che si basano sul recupero della password non funzioneranno dalla console Amazon EC2. Gli agenti di avvio di Windows su Amazon EC2 (EC2Config, EC2Launch v1 e EC2Launch v2) si affidano alla console seriale per eseguire varie attività. Queste attività non vengono eseguite correttamente quando si abilita SAC su un'istanza. Per ulteriori informazioni sugli agenti di lancio di Windows on Amazon EC2, consulta. the section called “Configura le istanze Windows” Se abiliti SAC, puoi disabilitarlo in

un secondo momento. Per ulteriori informazioni, consulta Disabilitazione di SAC e del menu di avvio.

Argomenti

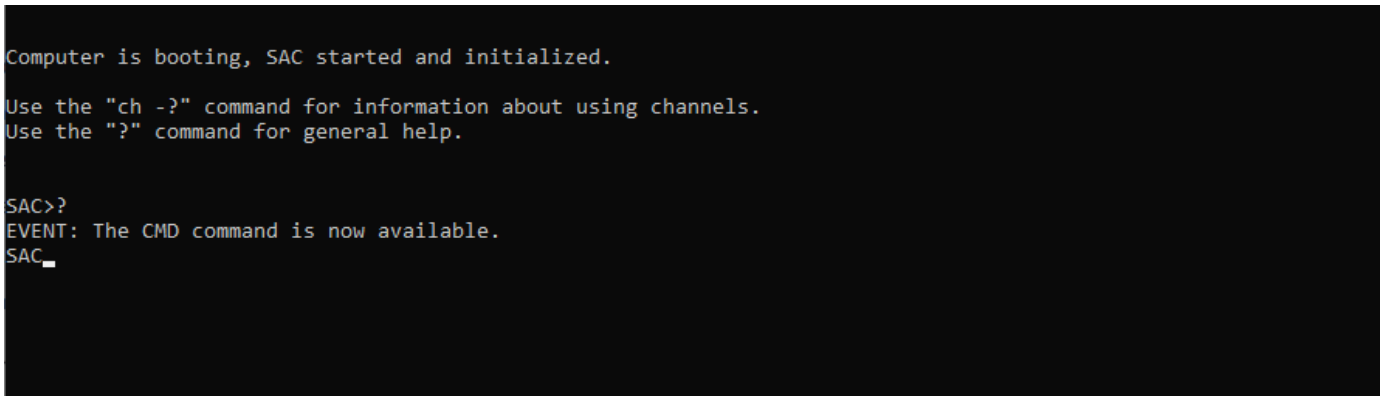
- Utilizzo di SAC
- Utilizzo del menu di avvio
- Disabilitazione di SAC e del menu di avvio

Utilizzo di SAC

Per utilizzare SAC

1. Collegarsi alla console seriale.

   Se SAC è abilitato sull'istanza, la console seriale visualizza il prompt SAC>.



2. Per visualizzare i comandi SAC, immettere **?**, quindi premere Invio.

   Output previsto

```
SAC>?
ch                    Channel management commands.  Use ch -? for more help.
cmd                   Create a Command Prompt channel.
d                     Dump the current kernel log.
f                     Toggle detailed or abbreviated tlist info.
? or help             Display this list.
i                     List all IP network numbers and their IP addresses.
i <#> <ip> <subnet> <gateway> Set IPv4 addr., subnet and gateway.
id                    Display the computer identification information.
k <pid>               Kill the given process.
l <pid>               Lower the priority of a process to the lowest possible.
lock                  Lock access to Command Prompt channels.
m <pid> <MB-allow>    Limit the memory usage of a process to <MB-allow>.
p                     Toggle paging the display.
r <pid>               Raise the priority of a process by one.
s                     Display the current time and date (24 hour clock used).
s mm/dd/yyyy hh:mm    Set the current time and date (24 hour clock used).
t                     Tlist.
restart               Restart the system immediately.
shutdown              Shutdown the system immediately.
crashdump             Crash the system. You must have crash dump enabled.
```

3. Per creare un canale del prompt dei comandi (ad esempio `cmd0001` o `cmd0002`), immettere **`cmd`**, quindi premere Invio.
4. Per visualizzare il canale del prompt dei comandi, premere ESC, quindi premere SCHEDA.

   Output previsto

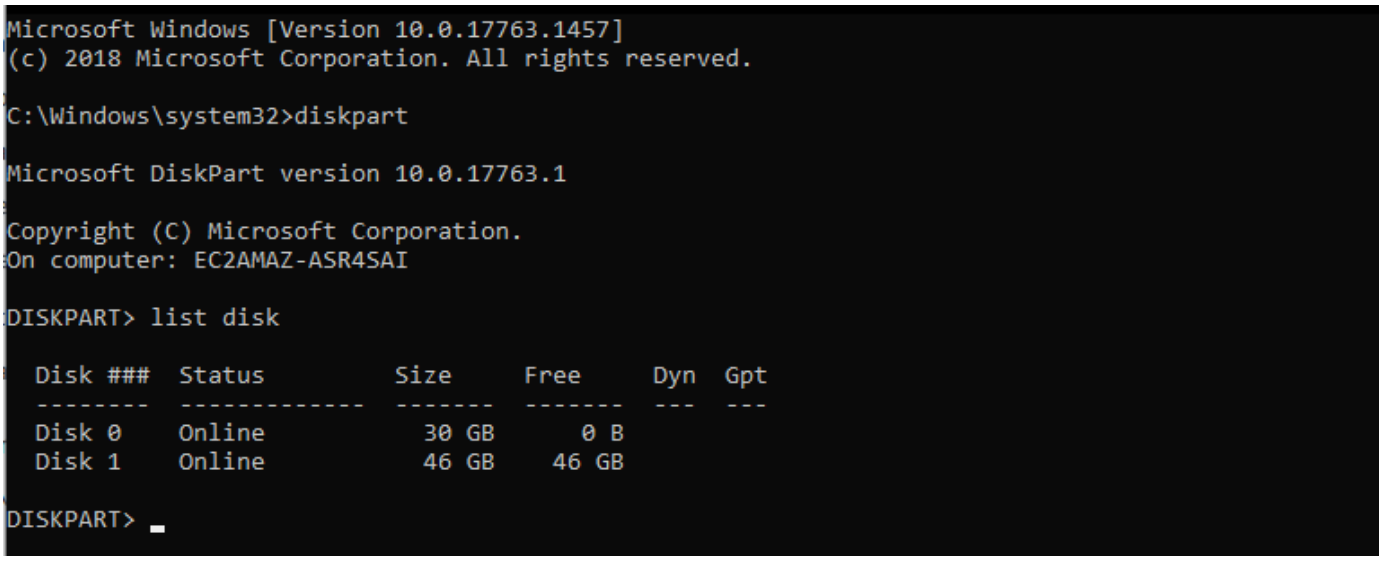
```
Name:                 Cmd0001
Description:          Command
Type:                 VT-UTF8
Channel GUID:         ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Per cambiare canale, premere ESC+TAB+numero canale insieme. Ad esempio, per passare al canale `cmd0002` (se è stato creato), premere ESC+TAB+2.
6. Immettere le credenziali richieste dal canale del prompt dei comandi.

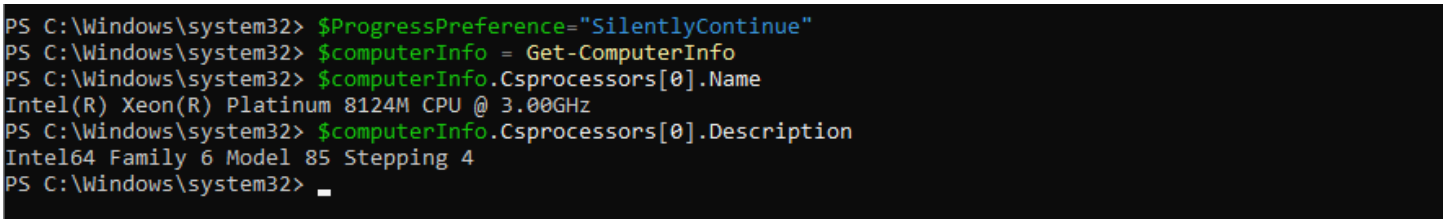
```
Please enter login credentials.
Username: Administrator
Domain  : .
Password: *******
```

Il prompt dei comandi è la stessa shell dei comandi completa che si ottiene su un desktop ma con l'eccezione che non consente la lettura di caratteri che erano già stati emessi.



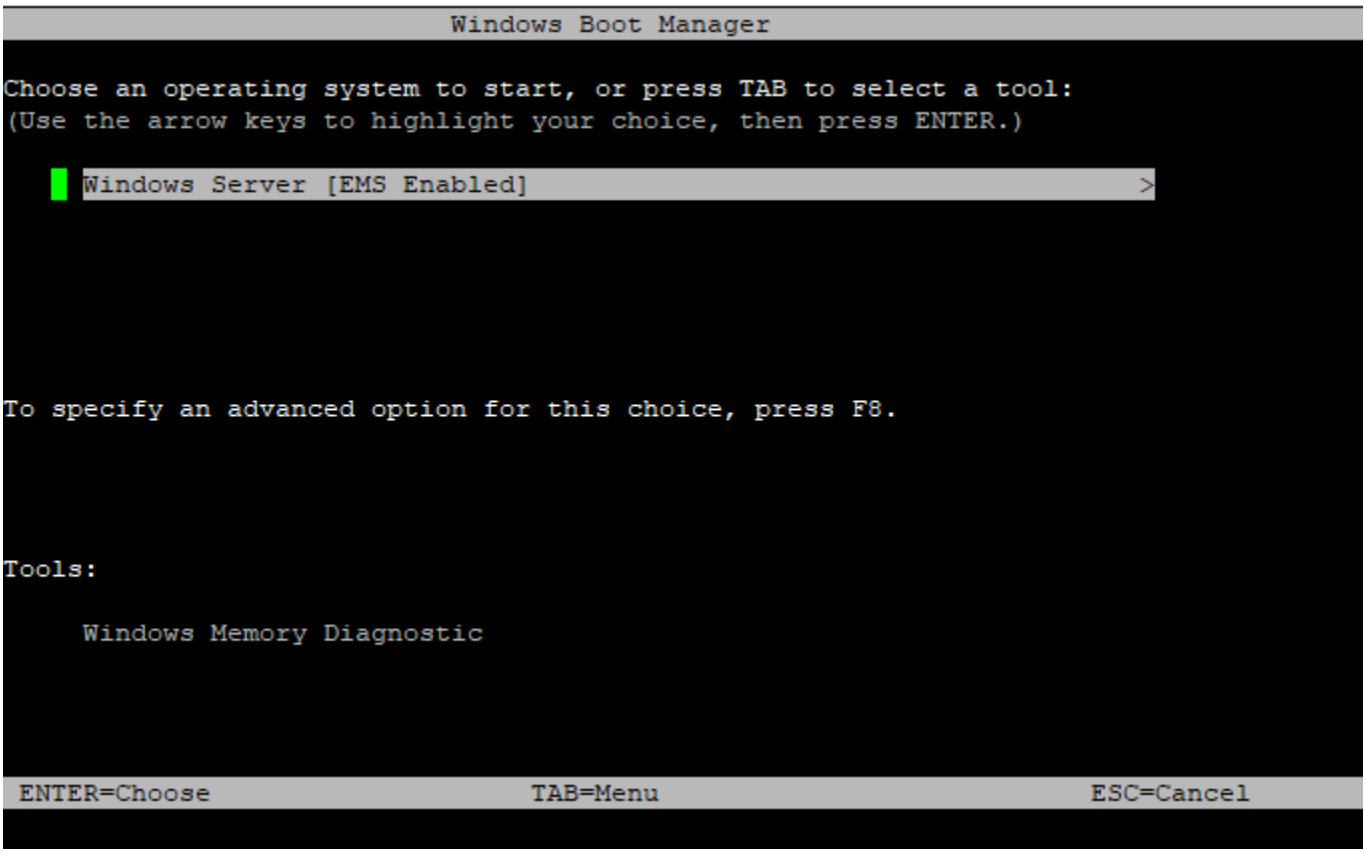
PowerShell può essere utilizzato anche dal prompt dei comandi.

Tieni presente che potrebbe essere necessario impostare la preferenza di avanzamento sulla modalità silenziosa.



Utilizzo del menu di avvio

Se l'istanza ha il menu di avvio abilitato e viene riavviata dopo la connessione tramite SSH, il menu di avvio dovrebbe essere visualizzato come riportato di seguito.



Comandi del menu di avvio

INVIO

Avvia la voce selezionata del sistema operativo.

Tasto TAB

Passa al menu Strumenti.

ESC

Annulla e riavvia l'istanza.

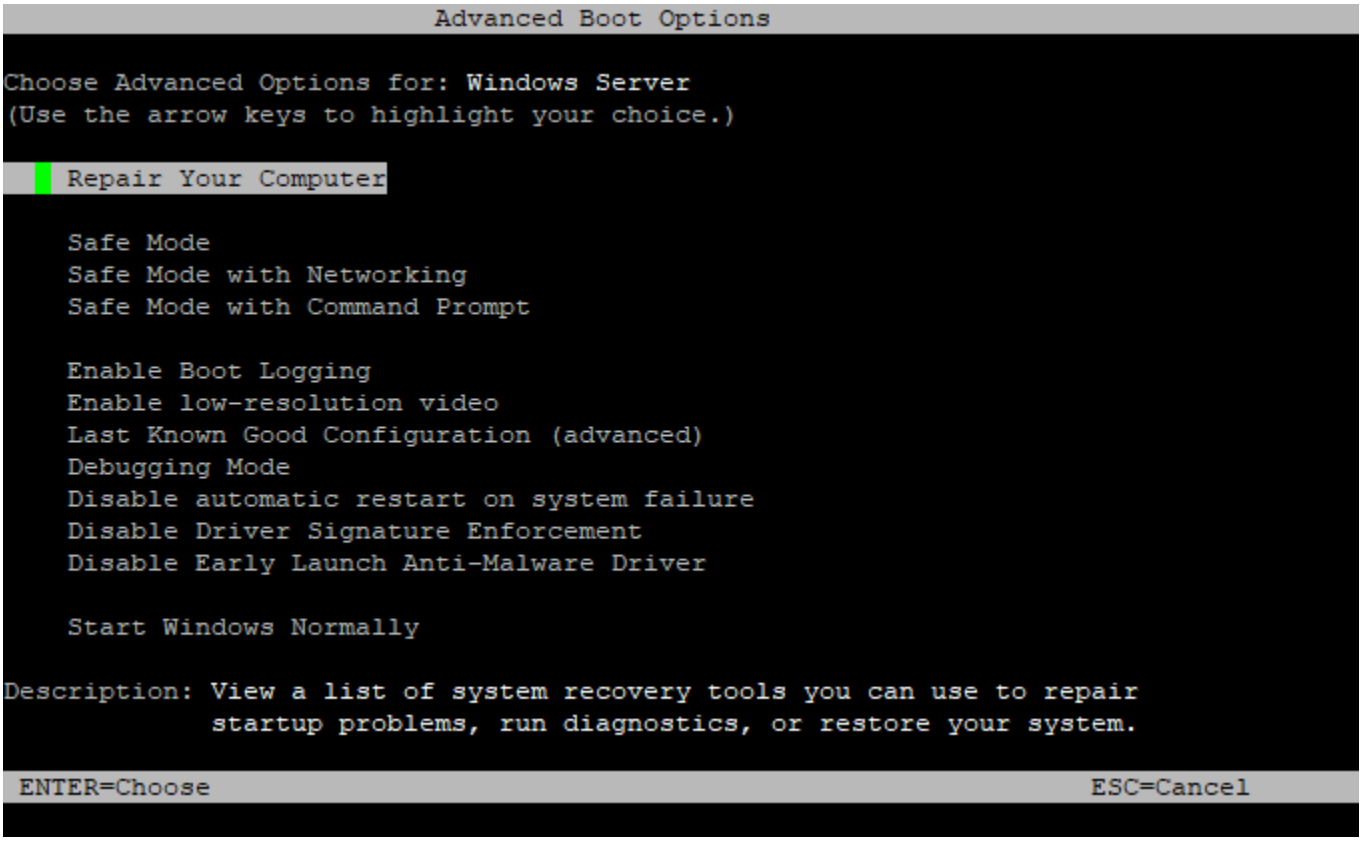
ESC seguito da 8

Equivalente a premere F8. Mostra le opzioni avanzate per l'elemento selezionato.

Tasto ESC + freccia sinistra

Torna al menu di avvio iniziale.

> **Note**
>
> Il tasto ESC da solo non consente di tornare al menu principale perché Windows resta in attesa di vedere se è in corso una sequenza di escape.



Disabilitazione di SAC e del menu di avvio

Se abiliti SAC e il menu di avvio, puoi disabilitare queste funzionalità in un secondo momento.

Utilizza uno dei metodi seguenti per disabilitare SAC e il menu di avvio su un'istanza.

PowerShell

Per disabilitare SAC e il menu di avvio in un'istanza di Windows

1. Connect all'istanza ed esegui i seguenti passaggi da una riga di PowerShell comando elevata.
2. Per prima cosa disabilita il menu di avvio modificando il valore in no.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. Modifica quindi il valore in `off` per disabilitare SAC.

```
bcdedit /ems '{current}' off
```

4. Applica la configurazione aggiornata riavviando l'istanza.

```
shutdown -r -t 0
```

Command prompt

Per disabilitare SAC e il menu di avvio in un'istanza di Windows

1. Connettiti all'istanza ed esegui la procedura dal prompt dei comandi.
2. Per prima cosa disabilita il menu di avvio modificando il valore in no.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. Modifica quindi il valore in `off` per disabilitare SAC.

```
bcdedit /ems {current} off
```

4. Applica la configurazione aggiornata riavviando l'istanza.

```
shutdown -r -t 0
```

Invio di un'interruzione della diagnostica (solo utenti avanzati)

> **Warning**
>
> Le interruzioni della diagnostica sono destinate all'uso da parte di utenti avanzati. Un utilizzo errato potrebbe influire negativamente sull'istanza. L'invio di un'interruzione della diagnostica a un'istanza potrebbe innescare l'arresto anomalo e il riavvio di della stessa, il che potrebbe causare la perdita di dati.

È possibile inviare un'interruzione diagnostica a un'istanza irraggiungibile o che non risponde per attivare manualmente un kernel panic per un'istanza Linux o un errore di arresto (comunemente denominato errore di schermata blu) per un'istanza di Windows.

Istanze Linux

I sistemi operativi Linux in genere si arrestano e vengono riavviati quando si verifica un kernel panic. Il comportamento specifico del sistema operativo dipende dalla sua configurazione. Un kernel panic può anche essere utilizzato per fare in modo che il kernel del sistema operativo dell'istanza esegua delle attività, come generare un file dump di arresto. Puoi quindi usare le informazioni del file dump di arresto per condurre un'analisi delle cause root ed eseguire il debugging dell'istanza. I dati dump di arresto vengono generati localmente dal sistema operativo sull'istanza stessa.

Istanze Windows

In generale, i sistemi operativi Windows si arrestano e vengono riavviati quando si verifica uno stop error, ma il comportamento specifico dipende dalla sua configurazione. Uno stop error può anche portare il sistema operativo a scrivere informazioni di debugging, come il dump di una memoria kernel, su file. È quindi possibile utilizzare questa informazione per eseguire analisi della causa root per effettuare il debugging dell'istanza. I dati dump della memoria vengono generati localmente dal sistema operativo sull'istanza stessa.

Prima di inviare un'interruzione della diagnostica all'istanza, si consiglia di consultare la documentazione del sistema operativo in uso e quindi apportare le modifiche necessarie alla configurazione.

Indice

Tipi di istanze supportati

L'interruzione di diagnostica è supportata su tutti i tipi di istanze basate su Nitro, ad eccezione di quelle alimentate da processori Graviton. AWS Per ulteriori informazioni, consulta le istanze basate su AWS Nitro System e Graviton.AWS

Prerequisiti

Prima di utilizzare l'interruzione della diagnostica, è necessario configurare il sistema operativo dell'istanza. Ciò garantisce che esegua le azioni necessarie quando si verifica un errore di kernel panic (istanze Linux) o di arresto (istanze Windows).

Istanze Linux

Per configurare Amazon Linux 2 e generare un dump di arresto quando si verifica un kernel panic

1. Connettiti alla tua istanza.
2. Installa kexec e kdump.

   ```
   [ec2-user ~]$ sudo yum install kexec-tools -y
   ```

3. Configura il kernel per prenotare una quantità di memoria adeguata per il kernel secondario. La quantità di memoria da prenotare dipende dalla memoria totale disponibile dell'istanza. Apri il file `/etc/default/grub` con l'editor di testo che preferisci, individua la riga che inizia con `GRUB_CMDLINE_LINUX_DEFAULT` e quindi aggiungi il parametro `crashkernel` nel formato seguente: `crashkernel=`*`memory_to_reserve`*. Ad esempio, per prenotare `160MB`, modifica il file `grub` come segue:

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=160M console=tty0 console=ttyS0,115200n8
    net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
    rd.shell=0"
   GRUB_TIMEOUT=0
   GRUB_DISABLE_RECOVERY="true"
   ```

4. Salva i cambiamenti e chiudi il file `grub`.
5. Ricompila il file di configurazione GRUB2.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

6. Nelle istanze basate sui processori Intel e AMD, il comando `send-diagnostic-interrupt` invia una unknown non-maskable interrupt (NMI) all'istanza. Devi configurare il kernel in modo che si arresti quando riceve una NMI sconosciuta. Apri il file `/etc/sysctl.conf` utilizzando qualsiasi editor di testo e aggiungi il seguente script.

   ```
   kernel.unknown_nmi_panic=1
   ```

7. Riavvia e riconnettiti all'istanza.
8. Verifica che il kernel sia stato riavviato con il parametro `crashkernel` corretto.

```
$ grep crashkernel /proc/cmdline
```

Il seguente output di esempio indica una configurazione corretta.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=160M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0
```

9. Verifica che il servizio kdump sia in esecuzione.

```
[ec2-user ~]$ systemctl status kdump.service
```

Il seguente output di esempio mostra il risultato se il servizio kdump è in esecuzione.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
 enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 2503 (code=exited, status=0/SUCCESS)
```

> **Note**
>
> Per impostazione predefinita, il file dump di arresto viene salvato su `/var/crash/`. Per cambiare la posizione, modifica il file `/etc/kdump.conf` tramite l'editor di testo che preferisci.

Per configurare Amazon Linux e generare un dump dell'arresto quando si verifica un kernel panic

1. Connettiti alla tua istanza.
2. Installa kexec e kdump.

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. Configura il kernel per prenotare una quantità di memoria adeguata per il kernel secondario. La quantità di memoria da prenotare dipende dalla memoria totale disponibile dell'istanza.

   ```
   $ sudo grubby --args="crashkernel=memory_to_reserve" --update-kernel=ALL
   ```

   Ad esempio, per riservare `160MB` per il kernel di arresto, utilizzare il comando seguente.

   ```
   $ sudo grubby --args="crashkernel=160M" --update-kernel=ALL
   ```

4. Nelle istanze basate sui processori Intel e AMD, il comando `send-diagnostic-interrupt` invia una unknown non-maskable interrupt (NMI) all'istanza. Devi configurare il kernel in modo che si arresti quando riceve una NMI sconosciuta. Apri il file `/etc/sysctl.conf` utilizzando qualsiasi editor di testo e aggiungi il seguente script.

   ```
   kernel.unknown_nmi_panic=1
   ```

5. Riavvia e riconnettiti all'istanza.
6. Verifica che il kernel sia stato riavviato con il parametro `crashkernel` corretto.

   ```
   $ grep crashkernel /proc/cmdline
   ```

   Il seguente output di esempio indica una configurazione corretta.

   ```
   root=LABEL=/ console=tty1 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295
    LANG=en_US.UTF-8 KEYTABLE=us crashkernel=160M
   ```

7. Verifica che il servizio kdump sia in esecuzione.

   ```
   [ec2-user ~]$ sudo service kdump status
   ```

   Se il servizio è in esecuzione, il comando restituisce la risposta `Kdump is operational`.

> **Note**
>
> Per impostazione predefinita, il file dump di arresto viene salvato su `/var/crash/`. Per cambiare la posizione, modifica il file `/etc/kdump.conf` tramite l'editor di testo che preferisci.

Per configurare SUSE Linux Enterprise, Ubuntu o Red Hat Enterprise Linux

Nelle istanze basate sui processori Intel e AMD, il comando `send-diagnostic-interrupt` invia una unknown non-maskable interrupt (NMI) all'istanza. È necessario configurare il kernel in modo che si blocchi quando riceve l'NMI sconosciuto modificando il file di configurazione per il sistema operativo in uso. Per informazioni su come configurare il kernel in modo che si blocchi, consultate la documentazione del sistema operativo in uso:

- SUSE Linux Enterprise
- Ubuntu
- Red Hat Enterprise Linux (RHEL)

Istanze Windows

Per configurare Windows e generare un dump della memoria quando si verifica uno stop error

1. Connettiti alla tua istanza.
2. Apri il Pannello di controllo e seleziona Sistema, Impostazioni avanzate di sistema.
3. Nella finestra di dialogo Proprietà di sistema, selezionare la scheda Avanzate.
4. Nella sezione Avvio e ripristino, selezionare Impostazioni....
5. Nella sezione Arresto sistema, configurare le impostazioni richieste e scegliere OK.

Per ulteriori informazioni sulla configurazione degli stop error di Windows consulta Panoramica delle opzioni del file dump di memoria per Windows.

Invio di un'interruzione della diagnostica

Dopo aver completato le modifiche alla configurazione necessarie, puoi inviare un'interruzione diagnostica alla tua istanza utilizzando l'API AWS CLI o Amazon EC2.

AWS CLI

Per inviare un'interruzione della diagnostica all'istanza (AWS CLI)

Usa il send-diagnostic-interruptcomando e specifica l'ID dell'istanza.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

Per inviare un'interruzione della diagnostica all'istanza (AWS Tools for Windows PowerShell)

Utilizzate il Send-EC2DiagnosticInterruptcmdlt e specificate l'ID dell'istanza.

```
PS C:\> Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Cronologia dei documenti

La tabella seguente descrive importanti aggiunte alla Guida per l'utente di Amazon EC2 a partire dal 2019. Inoltre, aggiorniamo frequentemente la guida per rispondere al feedback che ci invii.

Modifica	Descrizione	Data
Tipi di istanze aggiuntivi supportati per Credential Guard	Ora puoi abilitare Credential Guard per le istanze C7i, C7-Flex, M7i, M7i-Flex, R7i, R7i-Flex e T3.	26 giugno 2024
Istanze EC2 M1 Ultra Mac	Nuovo tipo di istanza generica con processori Apple M1 Ultra.	17 giugno 2024
Strumento di ricerca del tipo di istanza EC2: parametri aggiuntivi	Lo strumento di ricerca del tipo di istanza EC2 ora fornisce parametri aggiuntiv i per specificare requisiti più dettagliati per il carico di lavoro.	5 giugno 2024
Istanze U7i-12TB, U7in-16TB, U7in-24TB e U7in-32TB	Nuovi tipi di istanze ad alta memoria con processori scalabili Intel Xeon di quarta generazione.	28 maggio 2024
Nuova politica gestita per EC2 Fast Launch	È stata aggiunta la EC2FastLa unchFullAccess policy per eseguire azioni API relative alla funzionalità EC2 Fast Launch da un'istanza.	14 maggio 2024
Protezione dalla cancellazione della registrazione AMI	Puoi attivare la protezion e dall'annullamento della registrazione su un'AMI per	23 aprile 2024

	impedirne l'eliminazione accidentale o dolosa.	
Orologio hardware PTP: supporto per tipi di istanze	L'orologio hardware PTP è ora disponibile sui tipi di istanza C7a, C7i, M7a, M7g, M7i, R7a e R7i.	22 aprile 2024
Sono state aggiunte considerazioni sulle prestazioni di Nitro per una rete avanzata	Questa pagina si concentra su considerazioni di rete per aiutarti a ottimizzare le prestazioni delle istanze Amazon EC2 basate su Nitro.	4 aprile 2024
Nuova policy gestita per le istantanee EBS compatibili con VSS	Amazon EC2 VSS dispone di una nuova policy gestita da IAM che puoi aggiungere al ruolo del profilo dell'istanza per garantire che le tue autorizzazioni rimangano invariate up-to-date e seguano le best practice.	28 marzo 2024
Orologio hardware PTP — Stati Uniti orientali (Virginia settentrionale)	L'orologio hardware PTP è ora disponibile nella regione Stati Uniti orientali (Virginia settentrionale).	26 marzo 2024
Imposta iMDSv2 come account predefinito	Puoi impostare tutti i lanci di nuove istanze EC2 nel tuo account in modo che utilizzino Instance Metadata Service Version 2 (IMDSv2) per impostazione predefinita.	25 marzo 2024
Etichetta le nuove AMI Linux create a partire da un'istantanea	Quando crei un'AMI Linux da un'istantanea, puoi taggare la nuova AMI.	7 marzo 2024

Aggiungi tag a nuove AMI e istantanee durante la copia	Quando copi un AMI, puoi etichettare il nuovo AMI e le nuove istantanee con gli stessi tag oppure puoi etichettarli con tag diversi.	7 marzo 2024
Rimuovere le pagine AWS del Management Pack	Il AWS Management Pack è stato utilizzato principal mente con Windows Server 2012 e versioni precedenti. Queste versioni precedenti della piattaforma del sistema operativo non sono più supportate. Per gestire e risolvere i problemi della tua flotta di server in esecuzion e in locale AWS e in locale, consulta AWS Systems Manager Fleet Manager.	12 febbraio 2024
EC2 Instance Connect preinstallato sulle AMI macOS	EC2 Instance Connect ora è preinstallato su macOS Sonoma 14.2.1 o versioni successive, macOS Ventura 13.6.3 o versioni successive e macOS Monterey 12.7.2 o versioni successive.	26 gennaio 2024
Supporto per CentOS, macOS e RHEL di EC2 Instance Connect	Ora è possibile installare EC2 Instance Connect sulle AMI supportate di CentOS, macOS e RHEL.	6 dicembre 2023
Supporto per l'ibernazione per C7a, C7i, R7a, R7i e R7iz	Iberna le istanze appena avviate in esecuzione sui tipi di istanza C7a, C7i, R7a, R7i e R7iz.	1 dicembre 2023

Selettore del tipo di istanza EC2 di Amazon Q	Il selettore del tipo di istanza EC2 di Amazon Q considera il caso d'uso, il tipo di carico di lavoro e le preferenze del produttore della CPU, nonché il modo in cui dai priorità a prezzo e prestazioni. Utilizza quindi questi dati per fornire indicazioni e suggerimenti per i tipi di istanze Amazon EC2 più adatti ai nuovi carichi di lavoro.	28 novembre 2023
Piano gratuito EC2	Puoi monitorare l'utilizzo del piano gratuito di EC2 dal pannello di controllo di EC2.	26 novembre 2023
Console-to-Code	Console-to-Code può aiutarti a iniziare con il tuo codice di automazione. Console-to-Code registra le operazioni della console, quindi utilizza l'IA generativa per suggerire codice nel formato infrastructure-as code che preferisci. Puoi usare il codice come punto di partenza, personalizzandolo per renderlo pronto per la produzione per il tuo caso d'uso specifico.	26 novembre 2023

Timeout configurabili per il tracciamento delle connessioni inattive	Le connessioni dei gruppi di sicurezza che rimangono inattive possono portare all'esaurimento del tracciamento delle connessioni, impedire il tracciamento delle connessioni ed eliminare i pacchetti. Ora puoi impostare il timeout in secondi per il tracciamento delle connessioni del gruppo di sicurezza su un'interfaccia di rete elastica.	17 novembre 2023
Clock hardware PTP	Le istanze supportate ora dispongono di un clock hardware PTP (Precision Time Protocol). Il clock hardware PTP supporta NTP o una connessione PTP diretta.	16 novembre 2023
Cambio del tipo di istanza per l'istanza abilitata per l'ibernazione	Adesso puoi modificare il tipo di istanza di un'istanza abilitata per l'ibernazione quando si trova nello stato `stopped`.	16 novembre 2023
Topologia delle istanze	Puoi utilizzare l' DescribeInstanceTopology API per rilevare la posizione delle istanze e quindi utilizzare queste informazioni per ottimizzare i processi HPC e ML eseguendoli su istanze fisicamente più vicine tra loro.	13 novembre 2023

Supporto AMI condiviso di EC2 Fast Launch	Ora puoi abilitare EC2 Fast Launch su un'AMI condivisa con te. Quando abiliti EC2 Fast Launch su un'AMI condivisa, le istantanee predisposte per un avvio più rapido vengono create nel tuo account.	6 novembre 2023
Blocchi di capacità per ML	Ora puoi prenotare istanze GPU in date future per supportare i tuoi carichi di lavoro di machine learning (ML) di breve durata.	31 ottobre 2023
Ibernazione di istanze spot	Ora puoi ibernare le tue istanze spot utilizzando la stessa esperienza di ibernazione e le stesse famiglie di istanze attualmente disponibili per le istanze on demand.	24 ottobre 2023
Blocco dell'accesso pubblico per le AMI per impostazione predefinita	Il blocco dell'accesso pubblico per le AMI è ora abilitato per impostazione predefinita per tutti i nuovi account e per gli account esistenti senza AMI pubbliche.	20 ottobre 2023
Amazon EC2 Global View	Amazon EC2 Global View supporta tipi di risorse aggiuntivi e opzioni di visualizzazione personalizzabili.	18 ottobre 2023
Supporto dell'ibernazione per Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Iberna le istanze appena avviate dall'AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish).	16 ottobre 2023

Disabilitazione di un'AMI	È possibile disabilitare un'AMI per impedirne l'utilizzo per gli avvii delle istanze.	12 ottobre 2023
Controlli dello stato dei volumi EBS collegati	È possibile utilizzare i controlli dello stato dei volumi EBS collegati per monitorare se i volumi Amazon EBS collegati a un'istanza sono raggiungibili.	11 ottobre 2023
Supporto di ibernazione per Red Hat Enterprise Linux 9	Ibernazione delle istanze appena avviate da AMI Red Hat Enterprise Linux 9.	2 ottobre 2023
Supporto di ibernazione per Microsoft Windows Server 2022	Ibernazione delle istanze appena avviate da AMI Microsoft Windows Server 2022.	2 ottobre 2023
Supporto per l'ibernazione per AL2023	Ibernazione delle istanze appena avviate da AMI AL2023.	2 ottobre 2023
Avvio dell'interruzione delle istanze spot in una serie di istanze spot	Puoi selezionare una serie di istanze spot nella console di Amazon EC2 e avviare un'interruzione delle istanze spot della serie in modo da poter provare in che modo le applicazioni sulle tue istanze spot gestiscono le interruzioni.	21 settembre 2023
Blocco dell'accesso pubblico sulle AMI	Puoi abilitare il blocco dell'accesso pubblico alle AMI a livello di account per bloccare qualsiasi tentativo di rendere pubbliche le tue AMI.	12 settembre 2023

Supporto di ibernazione per M7i e M7i-flex	Iberna le istanze appena avviate in esecuzione sui tipi di istanza M7i e M7i-flex.	22 agosto 2023
EC2-Classic è stato dichiarato obsoleto	Con EC2-Classic, le istanze vengono eseguite in una singola rete semplice condivisa con altri clienti. Amazon VPC sostituisce EC2-Classic. Con Amazon VPC, le istanze vengono eseguite in un cloud privato virtuale (VPC) isolato a livello logico dall'acco unt AWS .	8 agosto 2023
Host dedicati	È possibile allocare host dedicati su risorse hardware specifiche in un Outpost.	20 giugno 2023
Endpoint EC2 Instance Connect	Ora puoi connetterti a un'istanza tramite SSH o RDP senza richiedere che l'istanza disponga di un indirizzo IPv4 pubblico.	13 giugno 2023
IMDS Package Analyzer	Ora puoi utilizzare IMDS Packet Analyzer per identific are le origini delle chiamate IMDSv1 sulle tue istanze EC2.	1 giugno 2023
Istanze bare metal della Console seriale EC2	La console seriale EC2 ora supporta la connettività alla porta seriale di istanze bare metal selezionate.	11 aprile 2023

Quote per i modelli di avvio	Ora è possibile visualizzare le quote per i modelli di avvio e le versioni dei modelli di avvio nella console Service Quotas e utilizzando la CLI Service Quotas.	3 aprile 2023
Notifiche sull'utilizzo delle prenotazioni di capacità	AWS Health ora invia notifiche quando l'utilizzo della capacità per Capacity Reservations nel tuo account scende al di sotto del 20 percento.	3 aprile 2023
Gruppi Prenotazione della capacità	Ora puoi aggiungere le prenotazioni di capacità condivise con te ai gruppi di prenotazioni di capacità di cui sei proprietario.	30 marzo 2023
Modifica opzioni dei metadati dell'istanza	Ora puoi utilizzare la console Amazon EC2 per modificare le opzioni dei metadati dell'istanza.	20 marzo 2023
Aggiornamenti locali del sistema operativo macOS	Ora puoi eseguire aggiornamenti locali del sistema operativo Apple macOS sulle istanze Mac M1.	14 marzo 2023
UEFI preferred	Ora puoi creare un'unica AMI che supporta sia la modalità di avvio Unified Extensible Firmware Interface (UEFI) che BIOS legacy.	3 marzo 2023

Modifica di un'AMI per IMDSv2	Modifica l'AMI esistente in modo che le istanze avviate dall'AMI richiedano IMDSv2 per impostazione predefinita.	28 febbraio 2023
Sicurezza basata sulla virtualizzazione di Windows - Credential Guard	Puoi abilitare Credential Guard, una funzionalità di sicurezza basata sulla virtualiz zazione (VBS), sulle istanze Amazon EC2 supportate.	31 gennaio 2023
Alias AMI nei modelli di avvio	Puoi specificare un AWS Systems Manager parametro anziché l'ID AMI nei modelli di avvio per evitare di dover aggiornare i modelli ogni volta che l'ID AMI cambia.	19 gennaio 2023
Supporto di ibernazione per C6i, I3en e M6i	Iberna le istanze appena avviate in esecuzione sui tipi di istanza C6i, I3en e M6i.	19 dicembre 2022
Prevenzione delle distorsioni di scrittura	Migliora le prestazioni dei carichi di lavoro dei database relazionali ad alta intensità di I/O e riduci la latenza senza influire negativamente sulla resilienza dei dati con la prevenzione delle distorsioni di scrittura, una funzionalità dell'archiviazione a blocchi.	29 novembre 2022
ENA Express	Aumenta la velocità di trasmissione effettiva e minimizza la latenza di coda del traffico di rete tra le istanze EC2 con ENA Express.	28 novembre 2022

Blocco delle regole di conservazione nel cestino	Puoi bloccare le regole di conservazione per proteggerle da modifiche ed eliminazioni accidentali o dannose.	23 novembre 2022
Copia di tag dell'AMI	Quando copi un'AMI, puoi copiare contemporaneamente i tag dell'AMI definiti dall'utente.	18 novembre 2022
Dimensioni dell'AMI per l'archiviazione e il ripristino	La dimensione di un'AMI (prima della compressione) che può essere archiviata e ripristinata da e verso un bucket Amazon S3 ora può arrivare a 5.000 GB.	16 novembre 2022
priceCapacityOptimizedstrategia di allocazione per le istanze Spot	Un parco istanze Spot che utilizza la strategia di allocazione `priceCapacityOptimized` analizza sia il prezzo sia la capacità per selezionare i pool di istanze spot che hanno meno probabilità di essere interrotti e hanno il prezzo più basso possibile.	10 novembre 2022
price-capacity-optimizedstrategia di allocazione per le istanze Spot	Un parco istanze EC2 che utilizza la strategia di allocazione `price-capacity-optimized` analizza sia il prezzo sia la capacità per selezionare i pool di istanze spot che hanno meno probabilità di essere interrotti e hanno il prezzo più basso possibile.	10 novembre 2022

Annullamento della condivisione di un'AMI con il tuo account	Se un'AMI è stata condivisa con il tuo Account AWS e non desideri più che venga condivisa con il tuo account, puoi rimuovere il tuo account dalle autorizzazioni di avvio dell'AMI.	4 novembre 2022
Trasferimento degli indirizzi IP elastici	Ora puoi trasferire gli indirizzi IP elastici da uno Account AWS all'altro.	31 ottobre 2022
Sostituzione di un volume root	Puoi sostituire il volume Amazon EBS root per un'istanza in esecuzione utilizzando un'AMI.	27 ottobre 2022
Connessione automatica dell'istanza al database	Usa la funzione di connessione automatica per connettere rapidamente una o più istanze EC2 a un database RDS per consentire il traffico tra queste.	10 ottobre 2022
Quote delle AMI	Ora le quote si applicano alla creazione e alla condivisione di AMI.	10 ottobre 2022
Configurazione di un'AMI per IMDSv2	Configura un'AMI in modo che le istanze avviate dall'AMI richiedano IMDSv2 per impostazione predefinita.	3 ottobre 2022

Avvio dell'interruzione di un'istanza spot	Puoi selezionare un'istanza spot nella console di Amazon EC2 e avviare un'interruzione in modo da poter provare in che modo le applicazioni sulle tue istanze spot gestiscono le interruzioni.	26 settembre 2022
Fornitore di AMI verificato	Nella console Amazon EC2, le AMI pubbliche di proprietà di Amazon o di un partner Amazon verificato sono contrassegnate dalla dicitura Verified provider (fornitore verificato).	22 luglio 2022
Gruppi di posizionamento su AWS Outposts	Aggiunta una strategia di diffusione degli host per i gruppi di collocamento su un outpost.	30 giugno 2022
Chiavi di condizione per il Cestino	Puoi utilizzare le chiavi di condizione `rbin:Request/ResourceType` e `rbin:Attribute/ResourceType` per filtrare l'accesso alle richieste del Cestino.	14 giugno 2022
Volumi `io2` Block Express	È possibile modificare le dimensioni e la capacità di IOPS allocata di volumi `io2` Block Express ed è possibile abilitarli per un rapido ripristino delle istantanee.	31 maggio 2022

Host dedicati su AWS Outposts	È possibile allocare host dedicati su AWS Outposts.	31 maggio 2022
Protezione da arresto delle istanze	Se desideri che un'istanza non venga arrestata per errore, puoi abilitare la funzionalità di protezione da arresto per tale istanza.	24 maggio 2022
UEFI Secure Boot	UEFI Secure Boot si basa sul processo di avvio sicuro di lunga data di Amazon EC2 e fornisce funzionalità aggiuntive defense-in-depth che aiutano i clienti a proteggere il software dalle minacce che persistono anche dopo i riavvii.	10 maggio 2022
NitroTPM	Nitro Trusted Platform Module (NitroTPM) è un dispositivo virtuale fornito dal sistema AWS Nitro e conforme alla specifica TPM 2.0.	10 maggio 2022
Eventi di modifica dello stato dell'AMI	Amazon EC2 ora genera un evento quando un'AMI cambia stato. Puoi usare Amazon EventBridge per rilevare e reagire a questi eventi.	9 maggio 2022
Descrizione delle chiavi pubbliche	È possibile eseguire query sulla chiave pubblica e sulla data di creazione di una coppia di chiavi Amazon EC2.	28 aprile 2022

Creazione di coppie di chiavi	È possibile specificare il formato della chiave (PEM o PPK) quando si crea una nuova coppia di chiavi.	28 aprile 2022
Montaggio di file system Amazon FSx all'avvio	Puoi montare un file system Amazon FSx for NetApp ONTAP o Amazon FSx for OpenZFS nuovo o esistente al momento del lancio utilizzando la nuova procedura guidata di avvio.	12 aprile 2022
Nuova procedura guidata di avvio dell'istanza	Un'esperienza di avvio nuova e migliorata nella console Amazon EC2, che offre un modo più rapido e semplice per avviare un'istanza EC2.	5 aprile 2022
Obsolescenza automatica delle AMI pubbliche	Di default, la data di obsolescenza di tutte le AMI pubbliche è impostata a due anni dalla data di creazione dell'AMI.	31 marzo 2022
Categoria di metadati dell'istanza: autoscaling/ target-lifecycle-state	Quando si utilizzano i gruppi di Auto Scaling, è possibile accedere allo stato del ciclo di vita di destinazione di un'istanza dai metadati dell'istanza.	24 marzo 2022
Ultima data e ora di avvio dell'AMI	`lastLaunchedTime` indica la data e l'ora dell'ultimo utilizzo dell'AMI per avviare un'istanza.	28 febbraio 2022
Cestino di riciclaggio per AMI	Il Cestino di riciclaggio consente di ripristinare le AMI eliminate accidentalmente.	3 febbraio 2022

Chiavi ED25519	Le chiavi ED25519 non sono supportate per le istanze di Windows, EC2 Instance Connect e Console seriale EC2.	20 gennaio 2022
Piattaforme RHEL aggiuntive per prenotazioni di capacità	Piattaforme Red Hat Enterprise Linux aggiuntive per prenotazioni di capacità on-demand.	11 gennaio 2022
Configurare le AMI di Windows per avvio più rapido	Configurare le AMI di Windows per avviare istanze fino al 65% più velocemente, utilizzando snapshot pre-provisioning.	10 gennaio 2022
Tag dell'istanza nei metadati dell'istanza	È possibile accedere ai tag di un'istanza dai metadati dell'istanza.	6 gennaio 2022
Le Prenotazioni della capacità in gruppi di collocazione cluster	Le Prenotazioni di capacità possono essere create in gruppi di collocamento cluster.	6 gennaio 2022
Cestino di riciclaggio per gli snapshot Amazon EBS	Il Cestino di riciclaggio per gli snapshot Amazon EBS è una caratteristica di recupero degli snapshot che consente di ripristinare gli snapshot eliminati accidentalmente.	29 novembre 2021
Spot Fleet launch-before-terminate	La serie di istanze spot può terminare le istanze spot che ricevono una notifica di ribilanciamento dopo l'avvio di nuove istanze spot sostitutive.	4 novembre 2021

Parco istanze EC2 launch-before-terminate	EC2 Fleet può terminare le istanze spot che ricevono una notifica di ribilanciamento dopo l'avvio di nuove istanze spot sostitutive.	4 novembre 2021
Confronto tra timestamp	Puoi determinare l'ora reale di un evento confrontando il timestamp della tua istanza Amazon EC2 Linux con. ClockBound	2 novembre 2021
AMI condivise con organizzazioni e unità organizzative	Ora puoi condividere le AMI con le seguenti AWS risorse: organizzazioni e unità organizzative (OU).	29 ottobre 2021
Punteggio di posizionamento spot	Ottieni una raccomandazione per una AWS regione o una zona di disponibilità in base ai tuoi requisiti di capacità Spot.	27 ottobre 2021
Selezione del tipo di istanza basata su attributi per serie di istanze spot	Specificare gli attributi che un'istanza deve avere e Amazon EC2 identificherà tutti i tipi di istanza con tali attributi.	27 ottobre 2021
Selezione del tipo di istanza basata su attributi per EC2 Fleet	Specificare gli attributi che un'istanza deve avere e Amazon EC2 identificherà tutti i tipi di istanza con tali attributi.	27 ottobre 2021
Parco istanze di prenotazione della capacità on demand	Per avviare un gruppo, o parco istanze, di prenotazione della capacità, puoi usare un parco istanze di prenotazione della capacità.	5 ottobre 2021

Supporto all'ibernazione per Ubuntu 20.04 LTS - Focal	Ibernazione delle istanze appena avviate da Ubuntu 20.04 LTS - Focal AMI.	4 ottobre 2021
EC2 Fleet e prenotazioni della capacità on demand obiettivo	EC2 Fleet può avviare istanze on demand nelle prenotazioni della capacità `targeted`.	22 settembre 2021
Istanze T3 su host dedicati	Supporto per istanze T3 su host dedicati Amazon EC2.	14 settembre 2021
Supporto di ibernazione per RHEL, Fedora e CentOS	Iberna le istanze appena avviate da AMI RHEL, Fedora e CentOS.	9 settembre 2021
Amazon EC2 Global View	Amazon EC2 Global View consente di visualizzare VPC, sottoreti, istanze, gruppi di sicurezza e volumi in più AWS regioni in un'unica console.	1 settembre 2021
Supporto per rendere obsolete le AMI per Amazon Data Lifecycle Manager	Le policy delle AMI supportate da Amazon Data Lifecycle Manager EBS possono rendere obsolete le AMI. La policy AWSDataLifecycleManagerServiceRoleForAMIManagement AWS gestita è stata aggiornata per supportare questa funzionalità.	23 agosto 2021
Supporto di ibernazione per C5d, M5d e R5d	Iberna le istanze appena avviate in esecuzione sui tipi di istanza C5d, M5d e R5d.	19 agosto 2021
Coppie di chiavi Amazon EC2	Amazon EC2 ora supporta le chiavi ED25519 su istanze Linux e Mac.	17 agosto 2021

Prefissi per le interfacce di rete	È possibile assegnare un intervallo CIDR IPv4 o IPv6 privato, automaticamente o manualmente, alle interfacce di rete.	22 luglio 2021
Finestre di eventi	Puoi definire finestre di eventi personalizzate con ricorrenza settimanale per eventi pianificati che riavviano, arrestano o terminano le istanze Amazon EC2.	15 luglio 2021
ID risorse e supporto di assegnazione di tag per le regole dei gruppi di sicurezza	Puoi fare riferimento alle regole del gruppo di sicurezza in base all'ID risorsa. Puoi aggiungere i tag anche alle regole di un gruppo di sicurezza.	7 luglio 2021
Dichiarazione di un'AMI come obsoleta	È ora possibile specificare quando un'AMI viene dichiarata obsoleta.	11 giugno 2021
Fatturazione al secondo per Windows	Amazon EC2 addebita per l'utilizzo basato su Windows e SQL Server al secondo, con un addebito minimo di un minuto.	10 giugno 2021
Prenotazioni di capacità su AWS Outposts	È ora possibile utilizzare Prenotazioni di capacità su AWS Outposts.	24 maggio 2021
Condivisione di una Prenotazione della capacità	Ora è possibile condividere Prenotazioni di capacità create in Local Zones e Wavelength.	24 maggio 2021

Sostituzione del volume root	È ora possibile utilizzare le attività di sostituzione del volume root per sostituire il volume EBS root per le istanze in esecuzione.	22 Aprile 2021
Archiviazione e ripristino di un'AMI utilizzando S3	Archiviare le AMI supportate da EBS in S3 e ripristinarle da S3 per abilitare la copia tra partizioni di AMI.	6 Aprile 2021
Console seriale EC2	Risolvere i problemi di avvio e connettività di rete stabilendo una connessione alla porta seriale di un'istanza.	30 marzo 2021
Modalità di avvio	Amazon EC2 ora supporta l'avvio UEFI su istanze EC2 selezionate basate su AMD e Intel.	22 marzo 2021
Creazione di un record DNS inverso	È ora possibile impostare la ricerca DNS inversa per gli indirizzi IP elastici.	3 febbraio 2021
Applicazione di tag ad AMI e snapshot al momento della creazione di un'AMI	Quando si crea un'AMI, è possibile contrassegnare l'AMI e gli snapshot con gli stessi tag, oppure contrassegnarli con tag diversi.	4 dicembre 2020
Usa Amazon EventBridge per monitorare gli eventi della flotta Spot	Crea EventBridge regole che attivano azioni programmatiche in risposta ai cambiamenti di stato e agli errori di Spot Fleet.	20 novembre 2020

Usa Amazon EventBridge per monitorare gli eventi della flotta EC2	Crea EventBridge regole che attivano azioni programmatiche in risposta alle modifiche e agli errori dello stato della flotta EC2.	20 novembre 2020
Eliminazione di parchi istanze instant	Elimina un EC2 Fleet di tipo `instant` e terminare tutte le istanze della flotta in una singola chiamata API.	18 novembre 2020
Supporto di ibernazione per T3 e T3a	Iberna le istanze appena avviate in esecuzione sui tipi di istanza T3 e T3a.	17 Novembre 2020
Creazione rapida di Amazon EFS	Puoi creare e montare un file system Amazon EFS su un'istanza al momento del lancio utilizzando Amazon EFS Quick Create.	9 novembre 2020
Categoria di metadati dell'istanza: events/recommendations/rebalance	Ora approssimativa, in UTC, in cui viene emessa la notifica della raccomandazione di ribilanciamento dell'istanza EC2 per l'istanza.	4 novembre 2020
Raccomandazione di ribilanciamento dell'istanza EC2	Un segnale che ti avvisa quando un'istanza spot è a rischio elevato di interruzione.	4 novembre 2020
Prenotazioni della capacità nelle zone Wavelength	Ora è possibile creare e utilizzare Prenotazioni di capacità in Wavelength.	4 novembre 2020

Ribilanciamento della capacità	Configurare EC2 Fleet o la serie di istanze spot affinché avvii un'istanza spot sostitutiva quando Amazon EC2 emette un suggerimento di ribilanci amento.	4 novembre 2020
Supporto di ibernazione per I3, M5ad e R5ad	Iberna le istanze appena avviate in esecuzione sui tipi di istanze I3, M5ad e R5ad.	21 Ottobre 2020
Limiti di vCPU dell'istanza spot	I limiti dell'istanza spot vengono ora gestiti in termini di numero di vCPU che vengono utilizzate o verranno utilizzate dalle istanze spot in esecuzione in attesa dell'evas ione delle richieste aperte.	1 ottobre 2020
Prenotazioni della capacità in zone locali	Prenotazioni di capacità può ora essere creato e utilizzato in Local Zones.	30 settembre 2020
Supporto di ibernazione per M5a e R5a	Iberna le istanze appena avviate in esecuzione sui tipi di istanza M5a e R5a.	28 agosto 2020
I metadati dell'istanza forniscono informazioni sulla posizione dell'istanza e sul posizionamento	Nuovi campi di metadati dell'istanza nella categoria `placement` : regione, nome gruppo di posizionamento, numero di partizione, ID host e ID zona di disponibilità.	24 agosto 2020

Gruppi Prenotazione della capacità	È possibile utilizzare AWS Resource Groups per creare raccolte logiche di prenotazioni di capacità e quindi avviare l'istanza di destinazione in tali gruppi.	29 luglio 2020
EC2Launch v2	Puoi utilizzare EC2Launch v2 per eseguire attività durante il startup dell'istanza, se un'istanza viene arrestata e avviata successivamente, se un'istanza viene riavviata e se è on demand. EC2Launch v2 supporta tutte le versioni di Windows Server e sostituisce EC2Launch e EC2config.	30 giugno 2020
Utilizzo dei propri indirizzi IPv6	Puoi trasferire parte o tutto l'intervallo di indirizzi IPv6 dalla rete locale al tuo account. AWS	21 maggio 2020
Avvio delle istanze utilizzando un parametro Systems Manager	È possibile specificare un AWS Systems Manager parametro anziché un AMI quando si avvia un'istanza.	5 maggio 2020
Personalizzazione delle notifiche di eventi pianificati	Puoi personalizzare le notifiche di eventi pianificati per includere tag nella notifica e-mail.	4 maggio 2020

Applicazione di patch live del kernel a Amazon Linux 2	Kernel Live Patching per Amazon Linux 2 consente di applicare vulnerabilità di sicurezza e patch di bug critici a un kernel Linux in esecuzione, senza riavvii o interruzioni delle applicazioni in esecuzione.	28 aprile 2020
Windows Server su Host dedicati	È possibile utilizzare le AMI di Windows Server fornite da Amazon per eseguire le versioni più recenti di Windows Server Host dedicati.	7 Aprile 2020
Arrestare e avviare un'istanza spot	Arresta le istanze spot supportate da Amazon EBS e avviale quando desideri, invece di fare affidamento sul comportamento di interruzione.	13 gennaio 2020
Aggiunta di tag alle risorse	È possibile contrassegnare i gateway Internet solo egress, i gateway locali, le tabelle di routing del gateway locale, le interfacce virtuali del gateway locale, i gruppi di interfacce virtuali del gateway locale, le associazioni VPC della tabella di routing del gateway locale e le associazioni di gruppi di interfacce virtuali della tabella di routing del gateway locale.	10 gennaio 2020

Connettersi all'istanza utilizzando Session Manager	Puoi avviare una sessione di Session Manager con un'istanza dalla console Amazon EC2.	18 dicembre 2019
Host dedicati e gruppi di risorse host	Gli Host dedicati ora possono essere utilizzati con gruppi di risorse host.	2 dicembre 2019
Condivisione Host dedicato	Ora puoi condividere i tuoi host dedicati tra più AWS account.	2 dicembre 2019
Specifica crediti di default a livello di account	Puoi impostare le specifiche di credito predefinite per la famiglia di istanze Burstable Performance a livello di account per AWS regione.	25 novembre 2019
Individuazione del tipo di istanza	È possibile trovare un tipo di istanza che soddisfa le proprie esigenze.	22 novembre 2019
Host dedicati	Ora puoi configurare un Host dedicato per supportare più tipi di istanza in una famiglia di istanze.	21 novembre 2019
Servizio di metadati dell'istanza versione 2	Puoi utilizzare Servizio di metadati dell'istanza Versione 2, che è un metodo orientato alla sessione per richiedere metadati dell'istanza.	19 novembre 2019
Elastic Fabric Adapter (EFA)	Elastic Fabric Adapters può ora essere usato con Intel MPI 2019 Update 6.	15 novembre 2019

Supporto di ibernazione per le istanze Windows On demand	Puoi ibernare le istanze Windows On demand.	14 ottobre 2019
Acquisiti in coda di istanze riservate	Puoi accodare l'acquisto di un Istanza riservata fino a un massimo di tre anni in anticipo.	4 ottobre 2019
Interruzione della diagnostica	Puoi inviare un'interruzione della diagnostica a un'istanza Linux non raggiungibile o che non risponde per attivare un kernel panic.	14 agosto 2019
Strategia di allocazione ottimizzata della capacità	Utilizzando EC2 Fleet o una serie di istanze spot, puoi avviare le istanze spot da pool spot con capacità ottimale per il numero di istanze che vengono avviate.	12 agosto 2019
Condivisione Prenotazione della capacità on demand	Ora puoi condividere le tue prenotazioni di capacità tra più AWS account.	29 luglio 2019
Elastic Fabric Adapter (EFA)	EFA ora supporta Open MPI 3.1.4 e Intel MPI 2019 Update 4.	26 luglio 2019
EC2 Instance Connect	Con EC2 Instance Connect, puoi connetterti in modo semplice e sicuro alle istanze tramite Secure Shell (SSH).	27 giugno 2019
Ripristino host	Riavvia automaticamente le istanze su un nuovo host in caso di errore hardware imprevisto su un Host dedicato.	5 giugno 2019

Snapshot coerenti a livello di applicazione VSS	Crea istantanee coerenti con le applicazioni di tutti i volumi Amazon EBS collegati alle istanze Windows utilizzando Run Command. AWS Systems Manager	13 maggio 2019
Assistente alla conversione della piattaforma da Windows a Linux per i database Microsoft SQL Server	Spostare carichi di lavoro di Microsoft SQL Server esistenti da un sistema operativo Windows a un sistema operativo Linux.	8 maggio 2019
Aggiornamento automatico Windows	Esegui aggiornamenti automatici delle istanze EC2 Windows utilizzando. AWS Systems Manager	6 maggio 2019
Elastic Fabric Adapter (EFA)	È possibile collegare un Elastic Fabric Adapter alle istanze per accelerare le applicazioni di tipo High Performance Computing (HPC).	29 aprile 2019

Per informazioni sui tipi di istanza rilasciati per Amazon EC2, consulta la cronologia dei documenti nella Amazon EC2 Instance Types Guide.

Cronologia del 2018 e precedenti

La tabella seguente descrive importanti aggiunte alla Guida per l'utente di Amazon EC2 nel 2018 e negli anni precedenti.

Funzionalità	Versione API	Descrizione	Data di rilascio
Gruppi di collocamento di partizione	15-11-2016	I gruppi di collocamento di partizione distribuiscono le istanze sulle partizioni logiche, garantendo così che le istanze in una partizione non condividano l'hardware sottostante con istanze in altre partizioni. Per ulteriori informazioni, consulta Gruppi di collocamento di partizione.	20 dicembre 2018
Ibernazione delle istanze Linux EC2	15-11-2016	Puoi ibernare un'istanza Linux se è abilitata per l'ibernazione e corrisponde ai prerequisiti di ibernazione. Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.	28 novembre 2018
Acceleratori di Amazon Elastic Inference	15-11-2016	Puoi collegare un acceleratore di Amazon Elastic Inference alle istanze per aggiungere accelerazione basata su GPU per ridurre i costi di esecuzione dell'inferenza di deep learning.	28 novembre 2018
La console Spot raccomanda un parco istanze	15-11-2016	La console Spot raccomanda un parco istanze basato sulla best practice Spot (diversificazione delle istanze) per soddisfare le specifiche minime hardware (vCPU, memoria e archiviazione) per le esigenze dell'applicazione. Per ulteriori informazioni, consulta Creare una richiesta di parco istanze spot.	20 novembre 2018
Nuovo tipo di richiesta EC2 Fleet: instant	15-11-2016	EC2 Fleet ora supporta un nuovo tipo di richiesta, `instant`, che è possibile utilizzare per assegnare la capacità in modo sincrono tra tutti i tipi di istanza e i modelli di acquisto. La richiesta `instant` restituisce le istanze avviate nella risposta API e non esegue ulteriori operazioni, permettendoti di controllare se e	14 novembre 2018

Funzionalità	Versione API	Descrizione	Data di rilascio
		quando le istanze vengono avviate. Per ulteriori informazioni, consulta Tipi di richiesta di EC2 Fleet.	
Informazioni sui risparmi Spot	15-11-2016	Puoi visualizzare i risparmi ottenuti utilizzando le istanze spot per un singolo parco istanze spot o per tutte le istanze spot. Per ulteriori informazioni, consulta Risparmio sull'acquisto di Istanze spot.	5 novembre 2018
Supporto della console per l'ottimizzazione delle opzioni CPU	15-11-2016	Quando avvii un'istanza, è possibile ottimizzare le opzioni della CPU per soddisfare esigenze aziendali o carichi di lavoro specifici utilizzando la console Amazon EC2. Per ulteriori informazioni, consulta Ottimizzazione delle opzioni della CPU.	31 ottobre 2018
Supporto della console per la creazione di un modello di avvio da un'istanza	15-11-2016	È possibile creare un modello di avvio utilizzando un'istanza come base per un nuovo modello di avvio utilizzando la console Amazon EC2. Per ulteriori informazioni, consulta Creazione di un modello di avvio.	30 ottobre 2018
Prenotazione di capacità on demand	15-11-2016	Puoi prenotare la capacità per le istanze Amazon EC2 per qualsiasi durata in una determinata zona di disponibilità. Questo consente di creare e gestire le prenotazioni di capacità indipendentemente rispetto agli sconti di fatturazione offerti dalle istanze riservate (RI). Per ulteriori informazioni, consulta Prenotazione della capacità on demand.	25 ottobre 2018

Funzionalità	Versione API	Descrizione	Data di rilascio
Utilizzare i propri indirizzi IP (BYOIP)	15-11-2016	Puoi trasferire parte o tutto l'intervallo di indirizzi IPv4 pubblici dalla rete locale al tuo account. AWS Dopo aver portato l'intervallo di indirizzi a AWS, questo viene visualizzato nel tuo account come pool di indirizzi. È possibile creare un indirizzo IP elastico dal pool di indirizzi e utilizzarlo con le risorse AWS . Per ulteriori informazioni, consulta Utilizzare gli indirizzi IP personali (BYOIP) in Amazon EC2.	23 ottobre 2018
Inserisci un tag Host dedicato al momento della creazione e supporto per la console	15-11-2016	È possibile applicare tag ai Host dedicati al momento della creazione, ed è possibile gestire i tag Host dedicato utilizzando la console Amazon EC2. Per ulteriori informazioni, consulta Assegna un host dedicato Amazon EC2 da utilizzare nel tuo account.	08 ottobre 2018
Supporto della console per il dimensionamento pianificato per serie di istanze spot	15-11-2016	Aumenta o riduce la capacità corrente del parco istanze in base alla data e all'ora. Per ulteriori informazioni, consulta Dimensionare il parco istanze spot utilizzando il dimensionamento pianificato.	20 settembre 2018
Strategia di allocazione per parchi istanze EC2	15-11-2016	Puoi specificare se la capacità on demand viene soddisfatta in base al prezzo (il prezzo più basso per primo) o alla priorità (la priorità più alta per prima). Puoi specificare il numero di pool Spot in cui allocare la capacità spot di destinazione. Per ulteriori informazioni, consulta Strategie di allocazione per istanze spot.	26 luglio 2018

Funzionalità	Versione API	Descrizione	Data di rilascio
Strategia di allocazione per Parchi istanze spot	15-11-2016	Puoi specificare se la capacità on demand viene soddisfatta in base al prezzo (il prezzo più basso per primo) o alla priorità (la priorità più alta per prima). Puoi specificare il numero di pool Spot in cui allocare la capacità spot di destinazione. Per ulteriori informazioni, consulta Strategie di allocazione per istanze spot.	26 luglio 2018
Automazione del ciclo di vita degli snapshot	15-11-2016	È possibile utilizzare Amazon Data Lifecycle Manager per automatizzare la creazione e l'eliminazione di snapshot per i volumi EBS. Per ulteriori informazioni, consulta Amazon Data Lifecycle Manager.	12 luglio 2018
Opzioni CPU del modello di avvio	15-11-2016	Quando si crea un modello di avvio tramite gli strumenti a riga di comando, è possibile ottimizzare le opzioni della CPU per soddisfare esigenze aziendali o carichi di lavoro specifici. Per ulteriori informazioni, consulta Creazione di un modello di avvio.	11 luglio 2018
Tagging di Host dedicati	15-11-2016	È possibile contrassegnare con dei tag gli Host dedicati.	3 luglio 2018
Output della console più recente	15-11-2016	Puoi recuperare l'ultimo output della console per alcuni tipi di istanze quando usi il comando. get-console-output AWS CLI	9 maggio 2018
Ottimizzazione delle opzioni della CPU	15-11-2016	Quando avvii un'istanza, è possibile ottimizzare le opzioni della CPU per soddisfare esigenze aziendali o carichi di lavoro specifici. Per ulteriori informazioni, consulta Ottimizzazione delle opzioni della CPU.	8 maggio 2018

Funzionalità	Versione API	Descrizione	Data di rilascio
EC2 Fleet	15-11-2016	È possibile utilizzare EC2 Fleet per avviare un gruppo di istanze tra tipi di istanza EC2 e zone di disponibilità diversi e tra modelli di acquisto di istanza on demand, istanza riservata e istanza spot. Per ulteriori informazioni, consulta EC2 Fleet.	2 maggio 2018
Istanze on demand in Parchi istanze spot	15-11-2016	È possibile includere una richiesta di capacità on demand nella richiesta di serie di istanze spot per assicurarti di avere sempre capacità di istanza. Per ulteriori informazioni, consulta parco istanze spot.	2 maggio 2018
Tag di snapshot EBS alla creazione	15-11-2016	È possibile contrassegnare con tag gli snapshot durante la creazione.	2 aprile 2018
Modifica dei gruppi di collocamento	15-11-2016	È possibile spostare un'istanza all'interno o all'esterno di un gruppo di collocamento o modificarne il gruppo di collocamento. Per ulteriori informazioni, consulta Modifica del gruppo di collocamento per un'istanza.	1 marzo 2018
ID più lunghi per le risorse	15-11-2016	È possibile abilitare il formato ID più lungo per più tipi di risorse. Per ulteriori informazioni, consulta ID risorsa.	9 febbraio 2018
Miglioramenti in termini di prestazioni di rete	15-11-2016	Le istanze al di fuori di un gruppo di collocazi one cluster possono ora usufruire di una maggiore larghezza di banda durante l'invio o la ricezione del traffico di rete tra altre istanze o Amazon S3.	24 gennaio 2018
Tag di indirizzi IP elastici	15-11-2016	È possibile contrassegnare con tag gli indirizzi IP elastici. Per ulteriori informazioni, consulta Applicazione di tag a un indirizzo IP elastico.	21 dicembre 2017

Funzionalità	Versione API	Descrizione	Data di rilascio
Amazon Time Sync Service	15-11-2016	È possibile utilizzare il servizio Amazon Time Sync per mantenere l'orario preciso nell'istanza. Per ulteriori informazioni, consulta Sincronizzazione precisa dell'orologio e dell'ora sulla tua istanza EC2.	29 novembre 2017
T2 Unlimited	15-11-2016	Le istanze T2 in modalità illimitata possono superare la baseline per tutto il periodo necessario. Per ulteriori informazioni, consulta Istanze a prestazioni espandibili.	29 novembre 2017
Modelli di lancio	15-11-2016	Un modello di avvio può contenere tutti o alcuni parametri per avviare un'istanza, così da non doverli specificare ogni volta che avvii un'istanza. Per ulteriori informazioni, consulta Avvio di un'istanza da un modello di avvio.	29 novembre 2017
Collocazione sparsa	15-11-2016	I gruppi di collocamento sparsa sono consigliati per le applicazioni con un numero ridotto di istanze critiche che è necessario tenere separate. Per ulteriori informazioni, consulta Gruppi di collocamento sparsi.	29 novembre 2017
Ibernazione di istanza spot	15-11-2016	Il servizio Spot può ibernare le istanze spot in caso di interruzione. Per ulteriori informazioni, consulta Ibernare le Istanze spot interrotte.	28 novembre 2017
Monitoraggio degli obiettivi del parco istanze spot	15-11-2016	È possibile configurare policy di dimensionamento con monitoraggio degli obiettivi per il parco istanze spot. Per ulteriori informazioni, consulta Dimensionare il parco istanze spot utilizzando una policy di monitoraggio degli obiettivi.	17 novembre 2017

Funzionalità	Versione API	Descrizione	Data di rilascio
La serie di istanze spot si integra con Elastic Load Balancing	15-11-2016	È possibile collegare uno o più load balancer a una serie di istanze Spot.	10 novembre 2017
Unione e divisione di Istanze riservate modificabili	15-11-2016	È possibile scambiare (unire) due o più Istanze riservate modificabili per ottenere una nuova Istanza riservata modificabile. Inoltre è possibile utilizzare il processo di modifica per suddividere una Istanza riservata modificabile in prenotazioni più piccole. Per ulteriori informazioni, consulta Scambiare le Istanze riservate modificabili.	6 novembre 2017
Modifica della tenancy di un VPC	15-11-2016	È possibile modificare l'attributo della tenancy delle istanze di un VPC da `dedicated` a `default`. Per ulteriori informazioni, consulta Modifica la locazione di un Amazon VPC.	16 ottobre 2017
Fatturazione per secondo	15-11-2016	Amazon EC2 addebita per l'utilizzo basato su Linux entro il secondo, con un addebito minimo di un minuto.	2 ottobre 2017
Arresto in caso di interruzione	15-11-2016	È possibile specificare se Amazon EC2 deve arrestare o terminare le Istanze spot quando vengono interrotte. Per ulteriori informazioni, consulta Comportamento delle interruzioni delle istanze Spot.	18 settembre 2017
Tag di gateway NAT	15-11-2016	È possibile contrassegnare con dei tag il gateway NAT. Per ulteriori informazioni, consulta Assegnazione di tag alle risorse.	7 settembre 2017

Funzionalità	Versione API	Descrizione	Data di rilascio
Descrizione della regola di gruppo di sicurezza	15-11-2016	È possibile aggiungere descrizioni alle regole di un gruppo di sicurezza. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza.	31 agosto 2017
Elastic Graphics	15-11-2016	Collegare gli acceleratori Grafica elastica alle istanze per accelerare le prestazioni grafiche delle applicazioni.	29 agosto 2017
Ripristino degli indirizzi IP elastici	15-11-2016	Se rilasci un indirizzo IP elastico per l'uso in un VPC, è possibile recuperarlo. Per ulteriori informazioni, consulta Recupero di un indirizzo IP elastico.	11 agosto 2017
Tag serie di istanze spot	15-11-2016	È possibile configurare il Parco istanze spot in modo che contrassegni automaticamente con tag le istanze che avvia.	24 luglio 2017
Assegnazione di tag alle risorse al momento della creazione	15-11-2016	È possibile contrassegnare con tag le istanze e i volumi durante la creazione. Per ulteriori informazioni, consulta Assegnazione di tag alle risorse. Inoltre, è possibile utilizzare le autorizzazioni a livello di risorsa basate su tag per controllare i tag applicati. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.	28 marzo 2017
Esecuzione di modifiche sui volumi EBS collegati	15-11-2016	Con la maggior parte dei volumi EBS collegata alla maggior parte delle istanze EC2, è possibile modificare le dimensioni, il tipo e IOPS del volume senza scollegare il volume o arrestare l'istanza.	13 febbraio 2017

Funzionalità	Versione API	Descrizione	Data di rilascio
Collegamento di un ruolo IAM	15-11-2016	Inoltre, è possibile collegare, distaccare o sostituire un ruolo IAM per un'istanza esistente . Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.	9 febbraio 2017
Istanze spot dedicate	15-11-2016	È possibile eseguire Istanze spot su hardware con tenant singolo in un virtual private cloud (VPC). Per ulteriori informazioni, consulta Specificare una tenancy per le Istanze spot.	19 gennaio 2017
Supporto IPv6	15-11-2016	È possibile associare un CIDR IPv6 al VPC e alle sottoreti e assegnare gli indirizzi IPv6 alle istanze nel VPC. Per ulteriori informazioni, consulta Indirizzamento IP per le istanze Amazon EC2.	1 dicembre 2016
Scalabilità automatica per il Parco istanze spot		Ora è possibile configurare policy di dimensionamento per il Parco istanze spot. Per ulteriori informazioni, consulta Scalabilità automatica per il parco istanze spot.	1 settembre 2016
Elastic Network Adapter (ENA)	01/04/2016	Ora, è possibile utilizzare ENA per reti avanzate. Per ulteriori informazioni, consulta Supporto di reti avanzate.	28 giugno 2016
Supporto avanzato per la visualizzazione e la modifica di ID più lunghi	01/04/2016	Ora è possibile visualizzare e modificare le impostazioni degli ID più lunghi per altri utenti IAM, ruoli IAM o per l'utente root. Per ulteriori informazioni, consulta ID risorsa.	23 giugno 2016
Copia istantanee crittografate di Amazon EBS tra account AWS	01/04/2016	Ora puoi copiare istantanee EBS crittografate tra account. AWS	21 giugno 2016

Funzionalità	Versione API	Descrizione	Data di rilascio
Acquisizione di uno screenshot di una console di istanze	01/10/2015	Ora, è possibile ottenere ulteriori informazioni durante il debug di istanze irraggiungibili. Per ulteriori informazioni, consulta Acquisizione di uno screenshot di un'istanza irraggiungibile.	24 maggio 2016
Due nuovi tipi di volume EBS	01/10/2015	Ora, è possibile creare volumi Throughput Optimized HDD (st1) e Cold HDD (sc1).	19 aprile 2016
Aggiunti nuovi parametri NetworkPacketsIn e NetworkPacketsOut parametri per Amazon EC2		Aggiunti nuovi parametri NetworkPacketsIn e NetworkPacketsOut parametri per Amazon EC2. Per ulteriori informazioni, consulta Parametri dell'istanza.	23 marzo 2016
CloudWatch metriche per Spot Fleet		Ora puoi ottenere le CloudWatch metriche per la tua flotta Spot. Per ulteriori informazioni, consulta CloudWatch metriche per Spot Fleet.	21 marzo 2016
Istanze pianificate	01/10/2015	Le istanze riservate pianificate (istanze pianificate) ti permettono di acquistare prenotazioni di capacità giornaliere, settimanali o mensili con una data di inizio e una durata specifici.	13 gennaio 2016
ID più lunghi per le risorse	01/10/2015	Stiamo introducendo gradualmente ID di lunghezza maggiore per alcuni tipi di risorse Amazon EC2 ed Amazon EBS. Durante il periodo di accettazione, è possibile abilitare il formato ID più lungo per i tipi di risorsa supportati. Per ulteriori informazioni, consulta ID risorsa.	13 gennaio 2016

Funzionalità	Versione API	Descrizione	Data di rilascio
ClassicLink Supporto DNS	01/10/2015	Puoi abilitare il supporto ClassicLink DNS per il tuo VPC in modo che i nomi host DNS indirizzati tra istanze EC2-Classic collegate e istanze nel VPC si risolvano in indirizzi IP privati e non indirizzi IP pubblici.	11 gennaio 2016
Host dedicati	01/10/2015	Un host dedicato di Amazon EC2 è un server fisico con capacità di istanze dedicata al tuo uso. Per ulteriori informazioni, consulta Host dedicati di Amazon EC2.	23 novembre 2015
Durata dell'istanza spot	01/10/2015	Ora, è possibile specificare una durata per le Istanze spot. I blocchi di istanze Spot non sono supportati (gennaio 2023).	6 ottobre 2015
Richiesta di modificare di un Parco istanze spot	01/10/2015	Ora è possibile modificare la capacità obiettivo della richiesta del parco istanze spot. Per ulteriori informazioni, consulta Modificare una richiesta di parco istanze spot.	29 settembre 2015
Strategia di allocazione diversificata del Parco istanze spot	15/04/2015	Ora è possibile allocare le istanze spot in più pool Spot utilizzando una sola richiesta di Parco istanze spot. Per ulteriori informazioni, consulta Strategie di allocazione per istanze spot.	15 settembre 2015
Ponderazione delle istanze del Parco istanze spot	15/04/2015	Ora, è possibile definire le unità di capacità con cui ogni tipo di istanza contribuisce alle prestazioni dell'applicazione e regolare di conseguenza il prezzo di offerta per le Istanze spot di ciascun pool di Spot. Per ulteriori informazioni, consulta Ponderazione delle istanze del parco istanze spot.	31 agosto 2015

Funzionalità	Versione API	Descrizione	Data di rilascio
Nuova operazione di allarme di riavvio e nuovo ruolo IAM per l'uso con operazioni di allarme		Sono stati aggiunti l'operazione di allarme di riavvio e un nuovo ruolo IAM per l'uso con operazioni di allarme. Per ulteriori informazioni, consulta Creazione di allarmi che arrestano, terminano, riavviano o recuperano un'istanza.	23 luglio 2015
Spot Fleets	15/04/2015	È possibile gestire una raccolta o un parco di istanze anziché gestire richieste di Parco istanze spot separate. Per ulteriori informazioni, consulta parco istanze spot.	18 maggio 2015
Migrazione degli indirizzi IP elastici a EC2-Classic	15/04/2015	Non è possibile eseguire la migrazione di un indirizzo IP elastico allocato per l'uso in EC2-Classic in modo da poterlo utilizzare in un VPC.	15 maggio 2015
Importazione di VMs con più dischi come AMI	01/03/2015	Ora, il processo VM Import supporta l'importazione di VM con più dischi come AMI. Per ulteriori informazioni, consulta l'articolo relativo all'importazione di una VM come immagine tramite VM Import/Export nella Guida per l'utente di VM Import/Export .	23 aprile 2015
Systems Manager		Systems Manager consente di configurare e gestire le istanze EC2.	17 febbraio 2015
Systems Manager per Microsoft SCVMM 1.5		Ora, puoi utilizzare Systems Manager per Microsoft SCVMM per avviare un'istanza e importare una VM da SCVMM in Amazon EC2.	21 gennaio 2015

Funzionalità	Versione API	Descrizione	Data di rilascio
Ripristino automatico di istanze EC2		Puoi creare un CloudWatch allarme Amazon che monitora un'istanza Amazon EC2 e ripristina automaticamente l'istanza se viene danneggiata a causa di un guasto hardware sottostante o di un problema che AWS richiede la riparazione. Un'istanza ripristinata è identica all'istanza originale, incluso l'ID dell'istanza, gli indirizzi IP e tutti i metadati dell'istanza. Per ulteriori informazioni, consulta Resilienza delle istanze.	12 gennaio 2015
ClassicLink	01/10/2014	ClassicLink ti consente di collegare la tua istanza EC2-Classic a un VPC nel tuo account. È possibile associare i gruppi di sicurezza VPC all'istanza EC2-Classic e consentire la comunicazione tra l'istanza EC2-Classic e le istanze del VPC tramite indirizzi IP privati.	7 gennaio 2015
Avvisi di interruzione delle istanze spot		Il modo migliore per prevenire l'interruzione dell'istanza spot è quello di progettare l'applicazione in modo che sia tollerante ai guasti. Inoltre, è possibile usufruire degli avvisi di interruzione delle istanze spot, che avvisano l'utente due minuti prima che Amazon EC2 termini il Parco istanze spot. Per ulteriori informazioni, consulta Avvisi di interruzione dell'istanza spot.	5 gennaio 2015
Systems Manager per Microsoft SCVMM		Systems Manager for Microsoft SCVMM fornisce un' easy-to-useinterfaccia semplice per la gestione AWS delle risorse, come le istanze EC2, di Microsoft SCVMM.	29 ottobre 2014

Funzionalità	Versione API	Descrizione	Data di rilascio
Supporto della paginazione di `DescribeVolumes`	01/03/2014	Ora, la chiamata API `DescribeVolumes` supporta la paginazione dei risultati con i parametri `MaxResults` e `NextToken` . Per ulteriori informazioni, DescribeVolumesconsulta Amazon EC2 API Reference.	23 ottobre 2014
Aggiunto il supporto per Amazon CloudWatch Logs		Puoi utilizzare Amazon CloudWatch Logs per monitorare, archiviare e accedere al sistema, all'applicazione e ai file di registro personalizzati dalle tue istanze o da altre fonti. Puoi quindi recuperare i dati di log associati da CloudWatch Logs utilizzando la CloudWatch console Amazon, i comandi CloudWatch Logs nella AWS CLI o l'SDK Logs. CloudWatch	10 luglio 2014
Nuova pagina EC2 Service Limits (Restrizioni dei servizi EC2)		Utilizzare la pagina EC2 Service Limits (Restrizioni dei servizi EC2) nella console Amazon EC2 per visualizzare i limiti attuali per le risorse fornite da Amazon EC2 e Amazon VPC, in base alla regione.	19 giugno 2014
Volumi Amazon EBS General Purpose SSD	01/05/2014	I volumi General Purpose SSD offrono archiviazione conveniente ideale per un'ampia gamma di carichi di lavoro. Questi volumi forniscono latenze di millisecondi a una cifra, la possibilità di aumentare le prestazioni fino a 3.000 IOPS per lunghi periodi di tempo e prestazioni di base pari a 3 IOPS/GiB. La dimensione di un volume SSD per scopo generico può essere compresa tra 1 GiB e 1 TiB.	16 giugno 2014

Funzionalità	Versione API	Descrizione	Data di rilascio
AWS Management Pack		AWS Management Pack ora supporta System Center Operations Manager 2012 R2.	22 maggio 2014
Amazon EBS encryption	01/05/2014	Crittografia Amazon EBS offre una soluzione di crittografia semplice per gli snapshot e i volumi di dati EBS senza la necessità di creare e mantenere un'infrastruttura di gestione delle chiavi sicura. La crittografia EBS consente la sicurezza dei dati inattivi tramite la crittografia dei dati utilizzando Chiavi gestite da AWS. La crittografia viene implementata a livello del server che ospita le istanze EC2, perciò viene applicata anche ai dati in trasferimento tra le istanze EC2 e l'archiviazione EBS.	21 maggio 2014
Report di utilizzo di Amazon EC2		I report di utilizzo di Amazon EC2 sono un insieme di report che mostrano dati su costi e uso relativi all'utilizzo di EC2.	28 gennaio 2014
Importazione della macchina virtuale Linux	15/10/2013	Ora, il processo VM Import supporta l'importazione di istanze Linux. Per ulteriori informazioni, consulta la Guida per l'utente di VM Import/Export.	16 dicembre 2013
Autorizzazioni a livello di risorsa per RunInstances	15/10/2013	Ora puoi creare policy AWS Identity and Access Management per controllare le autorizzazioni a livello di risorsa per l'azione dell'API Amazon EC2. RunInstances Per ulteriori informazioni e policy di esempio, consulta Identity and Access Management per Amazon EC2.	20 novembre 2013

Funzionalità	Versione API	Descrizione	Data di rilascio
Avvio di un'istanza da Marketplace AWS		Ora puoi avviare un'istanza Marketplace AWS utilizzando la procedura guidata di avvio di Amazon EC2. Per ulteriori informazioni, consulta Avvia un' Marketplace AWS istanza.	11 novembre 2013
Nuova procedura guidata di avvio		È disponibile una procedura guidata di avvio nuova e riprogettata di EC2. Per ulteriori informazioni, consulta Avvio di un'istanza tramite la vecchia procedura guidata di avvio.	10 ottobre 2013
Modifica dei tipi di istanze delle istanze riservate	01/10/2013	È ora possibile modificare il tipo di istanza di istanze riservate Linux all'interno della stessa famiglia (ad esempio, M1, M2, M3, C1). Per ulteriori informazioni, consulta Modificare le Istanze riservate.	09 ottobre 2013
Modifica delle istanze riservate Amazon EC2	15/08/2013	Ora, è possibile modificare le istanze riservate in una regione. Per ulteriori informazioni, consulta Modificare le Istanze riservate.	11 settembre 2013
Assegnazione di un indirizzo IP pubblico	15/07/2013	Ora, è possibile assegnare un indirizzo IP pubblico quando si avvia un'istanza in un VPC. Per ulteriori informazioni, consulta Assegnare un indirizzo IPv4 pubblico durante l'avvio dell'istanza.	20 agosto 2013
Concessione delle autorizzazioni a livello di risorsa	15/06/2013	Amazon EC2 supporta nuovi nomi della risorsa Amazon (ARN) e chiavi di condizione. Per ulteriori informazioni, consulta Policy IAM per Amazon EC2.	8 luglio 2013
Copie di snapshot incrementali	01/02/2013	Ora, è possibile eseguire copie di snapshot incrementali.	11 giugno 2013

Funzionalità	Versione API	Descrizione	Data di rilascio
AWS Management Pack		Il AWS Management Pack collega le istanze Amazon EC2 e i sistemi operativi Windows o Linux in esecuzione al loro interno. Il AWS Management Pack è un'estensione di Microsoft System Center Operations Manager.	8 maggio 2013
Nuova pagina Tags (Tag)		È disponibile una nuova pagina Tags (Tag) nella console Amazon EC2. Per ulteriori informazioni, consulta Tagging delle risorse Amazon EC2..	04 aprile 2013
Copia di un'AMI da una regione a un'altra	01/02/2013	Puoi copiare un'AMI da una regione all'altra, in modo da avviare istanze coerenti in più di una AWS regione in modo rapido e semplice. Per ulteriori informazioni, consulta Copiare un'AMI.	11 marzo 2013
Avvio di istanze in un VPC predefinito	01/02/2013	Il tuo AWS account è in grado di avviare istanze in EC2-Classic o in un VPC, oppure solo in un VPC, su base individuale. region-by-region Se è possibile avviare istanze solo in un VPC, viene creato automaticamente un VPC di default. Quando avvii un'istanza, essa viene avviata nel VPC predefinito, a meno che tu non abbia creato un VPC non predefinito e lo abbia specificato all'avvio dell'istanza.	11 marzo 2013
Copia snapshot EBS	01/12/2012	È possibile utilizzare copie snapshot per creare backup di dati, creare nuovi volumi Amazon EBS o creare Amazon Machine Image (AMI).	17 dicembre 2012

Funzionalità	Versione API	Descrizione	Data di rilascio
Controlli dello stato e parametri EBS aggiornati per volumi SSD con capacità di IOPS allocata	01/10/2012	I parametri di EBS sono stati aggiornati in modo da includere due nuovi parametri per i volumi SSD con capacità di IOPS allocata. Inoltre, sono stati aggiunti nuovi controlli dello stato per i volumi SSD con capacità di IOPS allocata.	20 novembre 2012
Stato della richiesta di istanza spot	01/10/2012	Lo stato della richiesta di istanza spot facilita la determinazione dello stato delle richieste Spot.	14 ottobre 2012
Marketplace di istanze riservate Amazon EC2	15/08/2012	Il Marketplace delle istanze riservate mette in comunicazione i venditori che dispongono di istanze riservate Amazon EC2 non più necessarie e gli acquirenti che desiderano acquistare capacità aggiuntiva. Le istanze riservate acquistate e vendute attraverso il Marketplace delle istanze riservate funzionano come qualsiasi altra istanza riservata, tranne che possono avere meno di un periodo di validità standard completo rimanente e possono essere vendute a prezzi diversi.	11 settembre 2012
SSD con capacità di IOPS allocata per Amazon EBS	20/07/2012	I volumi SSD con capacità di IOPS allocata offrono elevate prestazioni prevedibili per carichi di lavoro I/O intensi, come le applicazioni di database, che si basano su tempi di risposta costanti e rapidi.	31 luglio 2012

Funzionalità	Versione API	Descrizione	Data di rilascio
Ruoli IAM per istanze Amazon EC2	01/06/2012	I ruoli IAM per Amazon EC2 forniscono: • AWS chiavi di accesso per le applicazioni in esecuzione su istanze Amazon EC2. • Rotazione automatica delle chiavi di AWS accesso sull'istanza Amazon EC2. • Autorizzazioni granulari per le applicazioni in esecuzione su istanze Amazon EC2 che effettuano richieste ai tuoi servizi. AWS	11 giugno 2012
Caratteristiche delle istanze spot che semplificano l'avvio e gestiscono il potenziale di interruzione.		Ora, è possibile gestire le Istanze spot come segue: • Specificare la quantità che si è disposti a offrire per Istanze spot tramite le configurazioni di avvio di Auto Scaling e pianificare la quantità che sei disposto a offrire per Istanze spot. Per maggiori informazioni, consulta l'articolo relativo al lancio delle Istanze spot nel gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling. • Ricevi notifiche quando le istanze vengono avviate o terminate. • Utilizza i AWS CloudFormation modelli per avviare le istanze Spot in una pila di risorse. AWS	7 giugno 2012

Funzionalità	Versione API	Descrizione	Data di rilascio
Esportazione dell'istanza EC2 e time stamp per i controlli dello stato per Amazon EC2	01/05/2012	È stato aggiunto supporto per l'esportazione dell'istanza di Windows Server originariamente importate in EC2. È stato aggiunto supporto per time stamp sullo stato dell'istanza e sullo stato del sistema per indicare la data e l'ora in cui un controllo dello stato non è riuscito.	25 maggio 2012
Esportazione dell'istanza EC2 e time stamp in istanza e controlli dello stato del sistema per Amazon VPC	01/05/2012	È stato aggiunto supporto per l'esportazione dell'istanza EC2 su Citrix Xen, Microsoft Hyper-V e VMware vSphere. È stato aggiunto supporto per time stamp in istanza e controlli dello stato del sistema.	25 maggio 2012
Marketplace AWS AMI	01/04/2012	È stato aggiunto il supporto per le Marketplace AWS AMI.	19 aprile 2012
Livelli di prezzi delle istanze riservate	15/12/2011	È stata aggiunta una nuova sezione in cui viene indicato come usufruire del prezzo scontato integrato nei livelli di prezzi delle istanze riservate.	5 marzo 2012
Interfacce di rete elastiche per istanze EC2 in Amazon Virtual Private Cloud	01/12/2011	È stata aggiunta una nuova sezione relativa alle interfacce di rete elastiche per le istanze EC2 in un VPC. Per ulteriori informazioni, consulta Interfacce di rete elastiche.	21 dicembre 2011
Nuovi tipi di offerta per le istanze riservate Amazon EC2	01/11/2011	È possibile scegliere tra una varietà di offerte di istanze riservate che riguardano l'utilizzo previsto dell'istanza.	01 dicembre 2011

Funzionalità	Versione API	Descrizione	Data di rilascio
Stato dell'istanza Amazon EC2	01/11/2011	Puoi visualizzare ulteriori dettagli sullo stato delle tue istanze, inclusi gli eventi pianificati AWS che potrebbero avere un impatto sulle tue istanze. Queste attività operative includono i riavvii delle istanze necessari per applicare gli aggiornamenti software o le patch di sicurezza oppure i requisiti necessari per il ritiro delle istanze in caso di problemi hardware. Per ulteriori informazioni, consulta Monitoraggio dello stato delle istanze.	16 novembre 2011
Istanze spot in Amazon VPC	15/07/2011	Sono state aggiunte informazioni sul supporto per le Amazon VPC in Istanze spot. Con questo aggiornamento, gli utenti possono avviare Istanze spot in un virtual private cloud (VPC). Avviando Istanze spot in un VPC, gli utenti delle Istanze spot possono sfruttare i vantaggi di Amazon VPC.	11 ottobre 2011
Processo di VM import semplificato per gli utenti degli strumenti CLI	15/07/2011	Il processo VM Import viene semplificato con la funzionalità avanzata di `ImportInstance` e `ImportVolume`, che ora eseguirà il caricamento delle immagini in Amazon EC2 dopo aver creato l'attività di importazione. Inoltre, con l'introduzione di `ResumeImport`, gli utenti possono riavviare un caricamento incompleto nel punto in cui l'attività è stata interrotta.	15 settembre 2011

Funzionalità	Versione API	Descrizione	Data di rilascio
Supporto per l'importazione in formato file VHD		Ora, VM Import può importare file di immagini di macchine virtuali in formato VHD. Il formato file VHD è compatibile con le piattaforme di virtualizzazione Citrix Xen e Microsoft Hyper-V. Con questa versione, VM Import ora supporta i formati di immagini RAW, VHD e VMDK (compatibili con VMware ESX). Per ulteriori informazioni, consulta la Guida per l'utente di VM Import/Export.	24 agosto 2011
Aggiorna al connettore di importazione VM di Amazon EC2 per VMware vCenter		Sono state aggiunte informazioni sulla versione 1.1 del connettore di importazione VM di Amazon EC2 per l'appliance virtuale VMware vCenter (Connector). Questo aggiornamento include il supporto proxy per l'accesso a Internet, una migliore gestione degli errori, una maggiore accuratezza della barra di avanzamento delle attività e diverse correzioni di bug.	27 giugno 2011
Modifiche dei prezzi della zona di disponibilità delle Istanze spot	15/05/2011	Sono state aggiunte informazioni sulla funzione dei prezzi della zona di disponibilità delle Istanze spot. In questa versione, abbiamo aggiunto nuove opzioni di prezzi della zona di disponibilità come parte delle informazioni restituite quando viene eseguita una query per le richieste di istanze spot e la cronologia dei prezzi Spot. Queste aggiunte semplificano la determinazione del prezzo richiesto per avviare un'istanza spot in una particolare zona di disponibilità.	26 maggio 2011

Funzionalità	Versione API	Descrizione	Data di rilascio
AWS Identity and Access Management		Sono state aggiunte informazioni su AWS Identity and Access Management (IAM), che consentono agli utenti di specificare quali azioni di Amazon EC2 un utente può utilizzare con le risorse Amazon EC2 in generale. Per ulteriori informazioni, consulta Identity and Access Management per Amazon EC2.	26 aprile 2011
Istanze dedicate		Avviate all'interno dell'Amazon Virtual Private Cloud (Amazon VPC), le istanze dedicate sono istanze fisicamente isolate a livello di hardware host. Le istanze dedicate ti consentono di sfruttare Amazon VPC e AWS il cloud, con vantaggi tra cui il provisioning elastico su richiesta e il pagamento solo per ciò che usi, isolando al contempo le istanze di calcolo Amazon EC2 a livello hardware. Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.	27 marzo 2011
AWS Aggiornamenti delle istanze riservate alla console di gestione		Gli aggiornamenti alla console di AWS gestione semplificano la visualizzazione delle istanze riservate da parte degli utenti e l'acquisto di istanze riservate aggiuntive, incluse le istanze riservate dedicate.	27 marzo 2011
Informazioni sui metadati	01-01-2011	Sono state aggiunte informazioni sui metadati per riflettere le modifiche nella versione 01/01/2011. Per ulteriori informazioni, consulta Utilizzo dei metadati delle istanze e Categorie di metadati dell'istanza.	11 marzo 2011

Funzionalità	Versione API	Descrizione	Data di rilascio
Amazon EC2 VM Import Connector per VMware vCenter		Sono state aggiunte informazioni sul connettore di importazione VM di Amazon EC2 per l'appliance virtuale VMware vCenter (Connector). Il Connector è un plug-in per VMware vCenter che si integra con il client VMware vSphere e fornisce un'interfaccia utente grafica che è possibile utilizzare per importare le macchine virtuali VMware in Amazon EC2.	3 marzo 2011
Forzatura del distacco del volume		Ora puoi usare il AWS Management Console per forzare il distacco di un volume Amazon EBS da un'istanza.	23 febbraio 2011
Protezione per la cessazione dell'istanza		Ora puoi utilizzare la console di AWS gestione per impedire la chiusura di un'istanza. Per ulteriori informazioni, consulta Abilitare la protezione da cessazione.	23 febbraio 2011
VM Import	15/11/2011	Sono state aggiunte informazioni su VM Import, cosa che consente l'importazione di una macchina virtuale o un volume in Amazon EC2. Per ulteriori informazioni, consulta la Guida per l'utente di VM Import/Export.	15 dicembre 2010
Monitoraggio base per istanze	31/08/2010	Sono state aggiunte informazioni sul monitoraggio base per le istanze EC2.	12 dicembre 2010
Filtri e tag	31/08/2010	Sono state aggiunte informazioni sull'elenco, il filtraggio e il tagging delle risorse. Per ulteriori informazioni, consulta Elencare e filtrare le risorse e Tagging delle risorse Amazon EC2..	19 settembre 2010

Funzionalità	Versione API	Descrizione	Data di rilascio
Avvio di istanze idempotenti	31/08/2010	Sono state aggiunte informazioni sull'assi curazione dell'idempotenza durante l'esecuzi one delle istanze.	19 settembre 2010
AWS Identity and Access Management per Amazon EC2		Amazon EC2 ora si integra con AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Identity and Access Management per Amazon EC2.	2 settembre 2010
Designazione di indirizzi IP di Amazon VPC	15/06/2010	Ora, gli utenti Amazon VPC possono specifica re l'indirizzo IP pubblico per assegnare un'istanza avviata in un VPC.	12 luglio 2010
CloudWatch Monitoraggio Amazon per Amazon EBS Volumes		Il CloudWatch monitoraggio di Amazon è ora disponibile automaticamente per i volumi Amazon EBS.	14 giugno 2010
Istanze riservate con Windows		Ora, Amazon EC2 supporta le istanze riservate con Windows.	22 febbraio 2010

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.