User Guide

AWS Cost Management

AWS Cost Management: User Guide

Table of Contents

What is AWS Billing and Cost Management? 1
Features of AWS Billing and Cost Management 1
Billing and payments 1
Cost analysis 2
Cost organization 2
Budgeting and planning 3
Savings and commitments 3
Related services 3
AWS Billing Conductor 3
IAM 4
AWS Organizations 4
AWS Pricing Calculator 5
Getting started 6
Sign up for an AWS account 6
Create a user with administrative access 7
Attach the required IAM policy to an IAM identity 8
Review your bills and usage 8
Set up your AWS Cost Management features 9
What do I do next? 9
Using the Billing and Cost Management API 9
Learn more 9
Getting help 9
Using the AWS Billing and Cost Management home page 12
Managing Billing and Cost Management widgets 12
Cost summary 13
Cost monitor 14
Cost breakdown 15
Recommended actions 15
Related resources 17
Cost allocation coverage 17
Savings opportunities 19
Understanding the differences between AWS Billing data and AWS Cost Explorer data 19
Billing data 19
Cost Explorer data 20

Amortized costs ... 20
AWS service grouping ... 20
Estimated charges for the current month ... 21
Rounding ... 21
Presentation of discounts, credits, refunds, and taxes ... 21
AWS Cost Explorer ... 22
Enabling Cost Explorer ... 23
Controlling access to Cost Explorer ... 24
Getting started with Cost Explorer ... 27
Starting Cost Explorer ... 28
Exploring your data using Cost Explorer ... 28
Navigating Cost Explorer ... 29
Your Cost Explorer costs ... 29
Your Cost Explorer trends ... 29
Your daily unblended costs ... 30
Your monthly unblended costs ... 30
Your net unblended costs ... 31
Your recent Cost Explorer reports ... 31
Your amortized costs ... 31
Your net amortized costs ... 31
Using the Cost Explorer chart ... 32
Exploring more data for advanced cost analysis ... 53
Multi-year data at monthly granularity ... 53
Granular data ... 54
Understanding your estimated monthly usage summary ... 56
Configuring multi-year and granular data ... 58
Using the AWS Cost Explorer API ... 60
Service endpoint ... 61
Granting IAM permissions to use the AWS Cost Explorer API ... 61
Best practices for the AWS Cost Explorer API ... 61
Analyzing your cost data with Amazon Q (preview) ... 62
Overview ... 63
Security ... 66
Reports ... 68
Using the default Cost Explorer reports ... 68
Cost and usage reports ... 68

Reserved Instance reports ... 69
Saving reports and results ... 76
Saving your configuration ... 76
Downloading the cost data CSV file ... 77
Managing your saved Cost Explorer reports ... 77
AWS Budgets ... 80
Best practices for AWS Budgets ... 82
Best practices for controlling access to AWS Budgets ... 82
Best practices for budget actions ... 83
Best practices for setting budgets ... 84
Best practices for using the advanced options when setting cost budgets ... 84
Understanding the AWS Budgets update frequency ... 84
Best practices for setting budget alerts ... 84
Best practices for setting budget alerts using Amazon SNS topics ... 85
Best practices for tagging budgets ... 85
Creating a budget ... 86
Using a budget template (simplified) ... 87
Customizing a budget (advanced) ... 88
Budget methods ... 99
Budget filters ... 101
Viewing your budgets ... 104
Reading your budgets ... 105
Editing a budget ... 106
Downloading a budget ... 107
Copying a budget ... 107
Deleting a budget ... 108
Configuring AWS Budgets actions ... 108
Setting up a role for AWS Budgets to run budget actions ... 109
Configuring a budget action ... 110
Reviewing and approving your budget action ... 112
Creating an Amazon SNS topic for budget notifications ... 113
Troubleshooting ... 115
Checking or resending notification confirmation emails ... 115
Protecting your Amazon SNS budget alerts data with SSE and AWS KMS ... 116
Receiving budget alerts in Amazon Chime and Slack ... 118
AWS Budgets Reports ... 120

Creating an AWS Budgets report ... 120
Editing an AWS Budgets report ... 121
Copying an AWS Budgets report ... 122
Deleting an AWS Budgets report ... 122
AWS Cost Anomaly Detection ... 123
Setting up ... 124
Enabling Cost Explorer ... 124
Controlling access using IAM ... 124
Accessing the console ... 125
Quotas ... 125
Access control and examples ... 125
Controlling access using resource-level policies ... 126
Controlling access using tags (ABAC) ... 127
Getting started ... 128
Creating your cost monitors and alert subscriptions ... 129
Detection history values ... 133
Viewing your anomalies ... 135
Monitor types ... 137
Editing your alerts ... 138
Creating an Amazon SNS topic for anomaly notifications ... 139
Checking or resending notification confirmation email messages ... 141
Protecting your Amazon SNS anomaly detection alerts data with SSE and AWS KMS ... 116
Receiving anomaly alerts in Amazon Chime and Slack ... 144
Opting out ... 146
Cost Optimization Hub ... 148
Getting started with Cost Optimization Hub ... 149
Accounts supported by Cost Optimization Hub ... 149
Policy to opt in to Cost Optimization Hub ... 150
Enabling Cost Optimization Hub ... 151
Opting in to Compute Optimizer ... 152
Accessing the console ... 152
Opting out of Cost Optimization Hub ... 152
AWS Organizations trusted access ... 153
Delegate an administrator account ... 155
Viewing your cost optimization opportunities ... 157
Viewing the dashboard ... 157

- Prioritizing your cost optimization opportunities ... 159
- Understanding cost optimization strategies ... 159
- Viewing your savings opportunities ... 163
  - Viewing recommended actions and estimated savings ... 164
  - Grouping related recommendations ... 165
- Understanding savings estimation and aggregation ... 165
  - Savings estimation mode ... 165
  - Estimated monthly savings ... 166
  - Aggregating estimated savings ... 166
- Supported resources ... 167

Rightsizing Recommendations ... 169

- Getting started with rightsizing recommendations ... 169
- Using your rightsizing recommendations ... 170
  - Enhancing your recommendations using CloudWatch metrics ... 172
- CSV details ... 172
- Understanding your rightsizing recommendations calculations ... 174
  - Consolidated billing family ... 174
  - Determining if an instance is idle, underutilized, or neither ... 174
  - Generating modification recommendations ... 174
  - Savings calculation ... 175
- Understanding your reservations with Cost Explorer ... 176
  - Using your RI reports ... 176
  - Managing your reservation expiration alerts ... 176
- RI Recommendations ... 177
  - RI Recommendations for Size-Flexible RIs ... 178
  - Viewing the Cost Explorer Reservation Recommendations ... 179
  - Reading the Cost Explorer RI Recommendations ... 179
  - Modifying Your RI Recommendations ... 181
  - Saving Your RI Recommendations ... 182
  - Using Your RI Recommendations ... 187

Savings Plans ... 189

Security ... 190

- Data protection ... 191
- Identity and Access Management ... 191
  - User types and billing permissions ... 192
  - Audience ... 192

Authenticating with identities ... 195
Managing access using policies ... 198
Overview of managing access ... 201
How AWS Cost Management works with IAM ... 203
Identity-based policy examples ... 210
Using IAM policies for AWS Cost Management ... 213
AWS Cost Management policy examples ... 232
Migrating access control ... 248
Cross-service confused deputy prevention ... 263
Troubleshooting ... 264
Service-linked roles ... 267
Using service-linked roles ... 267
Logging and monitoring ... 275
AWS Cost and Usage Reports ... 275
AWS Cost Explorer ... 275
AWS Budgets ... 276
AWS CloudTrail ... 276
Logging AWS Cost Management API calls with AWS CloudTrail ... 276
Compliance validation ... 288
Resilience ... 289
Infrastructure security ... 289
Quotas and restrictions ... 291
Budgets ... 291
Budget reports ... 292
Cost Explorer ... 292
AWS Cost Anomaly Detection ... 292
Savings Plans ... 293
Document history ... 294
AWS Glossary ... 305

What is AWS Billing and Cost Management?

Welcome to the AWS Cost Management User Guide.

AWS Billing and Cost Management provides a suite of features to help you set up your billing, retrieve and pay invoices, and analyze, organize, plan, and optimize your costs.

To get started, set up your billing to match your requirements. For individuals or small organizations, AWS will automatically charge the credit card provided.

For larger organizations, you can use AWS Organizations to consolidate your charges across multiple AWS accounts. You can then configure invoicing, tax, purchase order, and payment methods to match your organization’s procurement processes.

You can allocate your costs to teams, applications, or environments by using cost categories or cost allocation tags, or using AWS Cost Explorer. You can also export data to your preferred data warehouse or business intelligence tool.

See the following overview of features to help you manage your cloud finances.

Features of AWS Billing and Cost Management

Topics

- Billing and payments
- Cost analysis
- Cost organization
- Budgeting and planning
- Savings and commitments

Billing and payments

Understand your monthly charges, view and pay invoices, and manage preferences for billing, invoices, tax, and payments.

- **Bills page –** Download invoices and view detailed monthly billing data to understand how your charges were calculated.

- **Purchase orders –** Create and manage your purchase orders to comply with your organization's unique procurement processes.
- **Payments –** Understand your outstanding or past-due payment balance and payment history.
- **Payment profiles –** Set up multiple payment methods for different AWS service providers or parts of your organization.
- **Credits –** Review credit balances and choose where credits should be applied.
- **Billing preferences –** Enable invoice delivery by email and your preferences for credit sharing, alerts, and discount sharing.

Cost analysis

Analyze your costs, export detailed cost and usage data, and forecast your spending.

- **AWS Cost Explorer –** Analyze your cost and usage data with visuals, filtering, and grouping. You can forecast your costs and create custom reports.
- **Data exports –** Create custom data exports from Billing and Cost Management datasets.
- **Cost Anomaly Detection –** Set up automated alerts when AWS detects a cost anomaly to reduce unexpected costs.
- **AWS Free Tier –** Monitor current and forecasted usage of free tier services to avoid unexpected costs.
- **Split cost allocation data –** Enable detailed cost and usage data for shared Amazon Elastic Container Service (Amazon ECS) resources.
- **Cost Management preferences –** Manage what data that member accounts can view, change account data granularity, and configure cost optimization preferences.

Cost organization

Organize your costs across teams, applications, or end customers.

- **Cost categories –** Map costs to teams, applications, or environments, and then view costs along these dimensions in Cost Explorer and data exports. Define split charge rules to allocate shared costs.
- **Cost allocation tags –** Use resource tags to organize, and then view costs by cost allocation tag in Cost Explorer and data exports.

Budgeting and planning

Estimate the cost of a planned workload, and create budgets to track and control costs.

Budgets – Set custom budgets for cost and usage to govern costs across your organization and receive alerts when costs exceed your defined thresholds.

Savings and commitments

Optimize resource usage and use flexible pricing models to lower your bill.

- **AWS Cost Optimization Hub –** Identify savings opportunities with tailored recommendations including deleting unused resources, rightsizing, Savings Plans, and reservations.
- **Savings Plans –** Reduce your bill compared to on-demand prices with flexible pricing models. Manage your Savings Plans inventory, review purchase recommendations, and analyze Savings Plan utilization and coverage.
- **Reservations –** Reserve capacity at discounted rates for Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon DynamoDB, and more.

Related services

AWS Billing Conductor

Billing Conductor is a custom billing service that supports the showback and chargeback workflows of AWS Solution Providers and AWS Enterprise customers. You can customize a second, alternative version of your monthly billing data. The service models the billing relationship between you and your customers or business units.

Billing Conductor doesn't change the way that you're billed by AWS each month. Instead, you can use the service to configure, generate, and display rates to specific customers over a given billing period. You can also use it to analyze the difference between the rates that you apply to your groupings relative to the actual rates for those same accounts from AWS.

As a result of your Billing Conductor configuration, the payer account (management account) can also see the custom rate that's applied on the billing details page of the AWS Billing and Cost Management console. The payer account can also configure AWS Cost and Usage Reports per billing group.

For more information about Billing Conductor, see the AWS Billing Conductor User Guide.

IAM

You can use AWS Identity and Access Management (IAM) to control who in your account or organization has access to specific pages on the Billing and Cost Management console. For example, you can control access to invoices and detailed information about charges and account activity, budgets, payment methods, and credits. IAM is a feature of your AWS account. You don't need to do anything else to sign up for IAM and there's no charge to use it.

When you create an account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform.

For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

By default, IAM users and roles in your account can't access the Billing and Cost Management console. To grant access, enable the **Activate IAM Access** setting. For more information, see About IAM Access.

If you have multiple AWS accounts in your organization, you can manage linked account access to Cost Explorer data by using the **Cost Management preferences** page. For more information, see Controlling access to Cost Explorer.

For more information about IAM, see the IAM User Guide.

AWS Organizations

You can use the consolidated billing feature in Organizations to consolidate billing and payment for multiple AWS accounts. Every organization has a *management account* that pays the charges of all the *member accounts*.

Consolidated billing has the following benefits:

- **One bill** – Get one bill for multiple accounts.
- **Easy tracking** – Track charges across multiple accounts and download the combined cost and usage data.

- **Combined usage –** Combine the usage across all accounts in the organization to share the volume pricing discounts, Reserved Instances discounts, and Savings Plans. This can result in a lower charge for your project, department, or company than with individual standalone accounts. For more information, see Volume discounts.
- **No extra fee –** Consolidated billing is offered at no additional cost.

For more information about Organizations, see the AWS Organizations User Guide.

AWS Pricing Calculator

AWS Pricing Calculator is a web-based planning tool to create estimates for your AWS use cases. Use it to model your solutions before building them, explore the AWS service price points, and review the calculations behind your estimates. Use AWS Pricing Calculator to help plan how you spend, find cost saving opportunities, and make informed decisions when using AWS. AWS Pricing Calculator is useful if you're new to AWS and for those who want to reorganize or expand their AWS usage.

For more information, see https://calculator.aws/#/ and the AWS Pricing Calculator User Guide.

Getting started

This section provides information that you need to get started with using the AWS Cost Management console.

Topics

- Sign up for an AWS account
- Create a user with administrative access
- Attach the required IAM policy to an IAM identity
- Review your bills and usage
- Set up your AWS Cost Management features
- What do I do next?

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

Create a user with administrative access

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

   For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide*.

2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups in the *AWS IAM Identity Center User Guide*.

Attach the required IAM policy to an IAM identity

AWS account owners can provide permissions to specific users who need to view or manage the Billing and Cost Management data for an AWS account. To start activating access to the Billing and Cost Management console, see IAM tutorial: Delegate access to the billing console in the *IAM User Guide*.

For more information about IAM policies specific to Billing and Cost Management, see Using identity-based policies (IAM policies) for Billing and Cost Management.

For a list of Billing and Cost Management policy examples, see Billing and Cost Management policy examples.

Review your bills and usage

Use features in the Billing console to view your current AWS charges and AWS usage.

To open the Billing console and view your usage and charges

1. Sign into the AWS Management Console and open the Billing and Cost Management console at https://console.aws.amazon.com/billing/.
2. Choose **Bills** to see the details for your current charges.

   Choose **Payments** to see your historical payment transactions.

   Choose **AWS Cost and Usage Reports** to see reports that break down your costs.

For information about Billing console features, see the Billing User Guide.

For more information about setting up and using AWS Cost and Usage Reports, see the AWS Cost and Usage Reports User Guide.

Set up your AWS Cost Management features

Review the process that's needed to activate your AWS Cost Management features.

- **AWS Cost Explorer**: Enabling Cost Explorer
- **AWS Budgets**: Best practices for AWS Budgets
- **AWS Budgets reports**: Reporting your budget metrics with budget reports
- **AWS Cost Anomaly Detection**: Setting up your anomaly detection
- **Savings Plans**: Getting started with Savings Plans in the *Savings Plans User Guide*

What do I do next?

Now that you have AWS Cost Management set up, you're ready to use the features available to you. The rest of this guide helps you navigate your journey using the console.

Using the Billing and Cost Management API

Use the AWS Billing and Cost Management API Reference to programmatically use some AWS Cost Management features.

Learn more

You can find more information about AWS Cost Management features including presentations, virtual workshops, and blog posts on the Cloud Financial Management with AWS page.

You can find virtual workshops by choosing the **Services** drop-down and selecting your feature.

Getting help

There are several resources that you can use if you want to learn more about or need help with any of the AWS Cost Management features.

AWS Knowledge Center

All AWS account owners have access to account and billing support free of charge. You can find answers to your questions quickly by visiting the AWS Knowledge Center.

To find your question or request

1. Open AWS Knowledge Center.
2. Choose **Billing Management**.
3. Scan the list of topics to locate a question that is similar to yours.

Contacting AWS Support

Contacting AWS Support is the fastest and most direct method for communicating with an AWS associate about your questions. AWS Support doesn't publish a direct phone number for reaching a support representative. You can use the following process to have an associate reach out to you by email or phone instead.

Only personalized technical support requires a support plan. For more information, visit AWS Support.

To open an AWS Support case where you specify *Regarding: Account and Billing Support*, you must either be signed into AWS as the root account owner, or have IAM permissions to open a support case. For more information, see Accessing AWS Support in the *AWS Support User Guide*.

If you closed your AWS account, you can still sign in to AWS Support and view past bills.

To contact AWS Support

1. Sign in and navigate to the AWS Support Center.
2. Choose **Create case**.
3. On the **Create case** page, choose **Account and billing** and fill in the required fields on the form.
4. After you complete the form, under **Contact options**, choose either **Web** for an email response or **Phone** to request a telephone call from an AWS Support representative. Instant messaging support isn't available for billing inquiries.

To contact AWS Support when you can't sign in to AWS

1. Recover your password or submit a form at AWS account support.
2. Choose an inquiry type in the **Request information** section.
3. Fill out the **How can we help you?** section.

4. Choose **Submit**.

Using the AWS Billing and Cost Management home page

Use the Billing and Cost Management home page for an overview of your AWS cloud financial management data and to help you make faster and more informed decisions. Understand high-level cost trends and drivers, quickly identify anomalies or budget overruns which require your attention, review recommended actions, understand cost allocation coverage, and identify savings opportunities.

The data on this page comes from AWS Cost Explorer. If you haven't used Cost Explorer before, it's *automatically* enabled for you once you visit this page. It can take up to 24 hours for your data to appear on this page. When available, your data will be refreshed at least once every 24 hours. The Cost Explorer data on the home page is tailored for analytical purposes. This means the data can differ from your invoices and the **Bills** page due to differences in how data is grouped into AWS services; how discounts, credits, refunds, and taxes are displayed; differences in timing for the current month's estimated charges; and rounding.

For more information, see Understanding the differences between AWS Billing data and AWS Cost Explorer data.

For more information about AWS Cloud Financial Management, see the Getting started page in the AWS Billing and Cost Management console. You can choose a topic and then follow the links to that specific console page or the documentation.

Managing Billing and Cost Management widgets

You can customize how the widgets appear by moving or resizing the widgets.

To manage the Billing and Cost Management widgets

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement.
2. (Optional) To customize the Billing and Cost Management home page, drag and drop a widget to move it, or change the widget size.
3. To take action on each recommendation or to learn more, review the data in the widget and then follow the links in the widget.
4. To reset the layout, choose **Reset layout** and then choose **Reset**.

You can use the following widgets:

- Cost summary
- Cost monitor
- Cost breakdown
- Recommended actions
- Savings opportunities

Cost summary

The cost summary widget provides a quick view of your current cost trends compared to your spending in the last month.

To view your month-to-date estimated charges on the **Bills** page, choose **View bill**.

All metrics shown in the cost summary widget exclude credits and refunds. This means you might see different numbers on the home page compared to the **Bills** page or your invoices. The widget shows the following metrics that you can choose to view in Cost Explorer:

- **Month-to-date cost** – Your estimated costs for the current month. The trend indicator compares the current month's costs to last month's cost for the same time period.
- **Last month's cost for same time period** – Your costs for last month, for the same time period. For example, if today is February 15, the widget also shows last month's cost for January 1–15.

> **Note**
>
> Trend calculations might be influenced by the number of days in each month. For example, on July 31, the trend indicator will look at costs from July 1–31 and compare it to costs for June 1–30.

- **Total forecasted cost for current month** – A forecast of your estimated total costs for the current month.
- **Last month's total cost** – The total costs for last month. For more information, choose each metric to view the costs in Cost Explorer, or choose **View bill** to view your month-to-date estimated charges on the **Bills** page.

> **Note**
>
> The metrics in this widget exclude credits and refunds. The costs here might differ from the costs on the **Bills** page or your invoices.

For more information about Cost Explorer, see Forecasting with Cost Explorer.

Cost monitor

This widget provides a quick view of your cost and usage budgets and any cost anomalies that AWS detected, so that you can fix it.

- **Budgets status –** Alerts you if any of your cost and usage budgets were exceeded.

  The status can be the following:
- **OK –** Cost and usage budgets haven't been exceeded.
- **Over budget –** A cost and usage budget has been exceeded. Your actual cost is greater than 100%. The number of exceeded budgets and a warning icon will appear.
- **Setup required –** You haven't created any cost and usage budgets.

Choose the status indicator to go to the **Budgets** page to review details of each budget or to create one. The budgets status indicator only shows information about cost and usage budgets. Budgets that you created to track the coverage or utilization of your Savings Plans or reservations won't appear in this widget. Cost anomalies status alerts you if AWS detected any anomalies with your costs since the first day of the current month. The status can be the following:

- **OK –** Cost anomalies haven't been detected in the current month.
- **Anomalies detected –** A cost anomaly has been detected. The number of anomalies detected and a warning icon will appear.
- **Setup required –** You haven't created any anomaly detection monitors.

Choose the status indicator to go to the **Cost Anomaly Detection** page to review details of each anomaly detected, or to create an anomaly detection monitor. The cost anomalies status indicator only displays information about cost anomalies detected in the current month. To view your full anomaly history, go to the **Cost Anomaly Detection** page.

For more information about budgets, see Managing your costs with AWS Budgets.

For more information about anomaly detection monitors, see Detecting unusual spend with AWS Cost Anomaly Detection.

Cost breakdown

This widget provides a breakdown of your costs for the last six months, so you can understand cost trends and drivers. To break down your costs, choose an option from the dropdown list:

- Service
- AWS Region
- Member account (for AWS Organizations management accounts)
- Cost allocation tag
- Cost category

If you choose cost category or cost allocation tag key, hover over the chart to see the values.

To dive deeper into your cost and usage, choose **Analyze your costs in Cost Explorer**. Use Cost Explorer to visualize, group, and filter your costs and usage, with additional dimensions, such as Availability Zone, instance type, and database engine.

For more information about Cost Explorer, see Exploring your data using Cost Explorer.

Recommended actions

This widget helps you implement AWS cloud financial management best practices and optimize your costs.

To use the recommended actions widget

1. For each recommendation, follow the link to take action on your account. By default, the widget shows up to seven recommended actions.
2. To load additional recommended actions, choose **Load more actions**.
3. To dismiss a specific recommendation, choose the **X** icon on the top right corner.

> **Note**
>
> If you don’t have permission to access the AWS service that shows each recommendation, you will see an access denied error. For example, if you have access to all Billing and Cost Management actions *except* `budgets:DescribeBudgets`, you can view all recommendations on the page except for budgets. See the error message about adding the missing IAM action to your policy.

This widget provides the following recommendations:

Budgets

This widget shows recommendations if any budgets require your attention, such as the following examples:

- Cost and usage budgets have been exceeded or are forecasted to be exceeded
- Savings Plan, reservation coverage, or utilization has dropped below the defined budget thresholds
- Your custom budget alert thresholds have been exceeded

Unlike the cost monitor widget, this widget shows information related to:

- Budgets that are forecasted to be exceeded but haven’t yet
- Budgets that are in alarm but haven't been exceeded
- Utilization and coverage budgets for your Savings Plans or reservations

Cost anomaly detection

This widget shows recommendations if any anomalies have been detected that require your attention. Unlike the cost monitor widget, this widget shows cost anomalies that were detected in the last 90 days with a total cost impact greater than $100 and an impact percentage greater than 40%.

Cost optimization

This widget shows recommendations for the following reasons:

- To help you improve cost efficiency and lower your AWS bill. You will see recommendations from AWS Cost Optimization Hub when the total estimated savings amount is at least 5% of last month’s costs.
- To review under-utilized Savings Plans or reservations
- To renew any Savings Plans or reservations that will expire within the next 30 days

AWS Free Tier

This widget shows recommendations if your usage exceeded 85% of any service's free tier usage limits.

Getting started

This widget shows recommendations to implement AWS cloud financial management best practices, such as:

- Create budgets to track and govern spending
- You have active Savings Plans but haven't created a Savings Plan budget
- You have Reserved Instance commitments but haven't created a Reserved Instance budget
- Add an alternate billing contact so that the correct people receive communications from AWS
- You haven't set up a cost anomaly monitor

Related resources

For more information, see the following topics:

- Managing your costs with AWS Budgets
- Detecting unusual spend with AWS Cost Anomaly Detection
- Cost Optimization Hub
- Using the AWS Free Tier
- Adding additional billing contact email addresses

Cost allocation coverage

To create cost visibility and accountability in your organization, it's important to allocate costs to teams, applications, environments, or other dimensions. This widget shows unallocated costs for your cost categories and cost allocation tags, so that you can identify where to take action to organize your costs.

Cost allocation coverage is defined as the percentage of your costs that don't have a value assigned to the cost category or cost allocation tag keys that you've created.

Example Example

- Your month-to-date spend is $100, and you created a cost category (named *Teams*) to organize costs by individual teams.
- You have $40 in the *Team A* cost category value, $35 in the *Team B* cost category value, and $25 that are unallocated.
- In this case, your cost allocation coverage is 25/100 = 25%.

A lower unallocated cost metric means that your costs are properly allocated along the dimensions important to your organization. For more information, see Building a cost allocation strategy in the *Best Practices for Tagging AWS Resources* whitepaper.

This widget compares the month-to-date unallocated cost percentage to all of last month's unallocated cost percentage. The widget shows up to five cost allocation tag keys or five cost categories. If you have more than five of either cost allocation tag keys or cost categories, use the widget preferences to specify the ones that you want.

To analyze your unallocated costs in more detail by using Cost Explorer, choose the cost category or cost allocation name.

To improve cost allocation coverage for your cost categories or cost allocation tags, you can edit your cost category rules or improve resource tagging by using AWS Tag Editor.

For more information, see the following topics:

- Managing your costs with AWS cost categories
- Using AWS cost allocation tags
- Using Tag Editor

Savings opportunities

This widget shows recommendations from Cost Optimization Hub to help you save money and lower your AWS bill. This can include:

- Deleting unused resources
- Rightsizing over-provisioned resources
- Purchasing Savings Plans or reservations

For each savings opportunity, the widget shows your estimated monthly savings. Your estimated savings are *de-duplicated* and *automatically* adjusted for each recommended savings opportunity.

Example Example

- Let's say that you have two Amazon EC2 instances, *`InstanceA`* and *`InstanceB`*.
- If you purchased a Savings Plan, you could reduce the cost for *`InstanceA`* by $20 and the cost of *`InstanceB`* by $10, for a total of $30 savings.
- However, if *`InstanceB`* is idle, the widget might recommend that you terminate it instead of purchasing a Savings Plan. The savings opportunity would tell you how much you could save by terminating the idle *`InstanceB`*.

To view the savings opportunities in this widget, you can opt in by visiting the Cost Optimization Hub page or using the Cost Management preferences page.

Understanding the differences between AWS Billing data and AWS Cost Explorer data

Billing data

Your billing data appears on the **Bills** and **Payments** pages of the AWS Billing and Cost Management console, and in the invoice that AWS issues to you. Billing data helps you understand the actual invoiced charges for previous billing periods, and the estimated charges that you've accrued for the current billing period, based on your month-to-date service usage. Your invoice represents the amount that you owe to AWS.

Cost Explorer data

Your Cost Explorer data appears in the following places:

- The Billing and Cost Management home page
- The pages for Cost Explorer, Budgets, and Cost Anomaly Detection
- Your reports for coverage and usage

Cost Explorer supports deep-dive analysis so that you can identify savings opportunities. Cost Explorer data provides more granular dimensions (such as Availability Zone or operating system) and includes features that might show differences when compared to billing data. On the **Cost Management** preferences page, you can manage your preferences for Cost Explorer data, including linked account access and historical and granular data settings. For more information, see Controlling access to Cost Explorer.

Amortized costs

Billing data is always presented on a *cash* basis. It represents the amount that AWS charges you each month. For example, if you purchase a one-year, all-upfront Savings Plan in September, AWS will charge you the full cost for that Savings Plan in the September billing period. Your billing data will then include the full cost of that Savings Plan in September. This helps you understand, validate, and pay your AWS invoices on time.

In contrast, you can use Cost Explorer data to view amortized costs. When costs are amortized, an upfront charge is spread, or *amortized* over the life of that agreement. In the previous example, you can use Cost Explorer for an amortized view of your Savings Plan. A one-year, all-upfront Savings Plan purchase will be spread evenly across the 12 months of the commitment term. Use amortized costs to gain insight into the effective daily costs associated with your portfolio of reservations or Savings Plans.

AWS service grouping

With billing data, your AWS charges are grouped into AWS services on your invoice. To help with deep-dive analysis, Cost Explorer will group some costs differently.

For example, let's say that you want to understand compute costs for Amazon Elastic Compute Cloud compared to ancillary cost, such as Amazon Elastic Block Store volumes or NAT gateways.

Instead of a single group for Amazon EC2 costs, Cost Explorer will group costs into **EC2 - Instances** and **EC2 - Other**.

In another example, to help analyze data transfer costs, Cost Explorer groups your transfer costs by service. In billing data, data transfer costs are grouped into a single service named **Data Transfer**.

Estimated charges for the current month

Your billing data and Cost Explorer data are refreshed at least once per day. The cadence when they're refreshed might differ. This can result in differences for your month-to-date estimated charges.

Rounding

Your billing data and Cost Explorer data are processed at different granularities. For example, Cost Explorer data is available with hourly and resource-level granularity. Billing data is monthly and doesn't offer resource-level details. As a result, your billing data and Cost Explorer data might vary due to rounding. When these data sources are different, the amount on your invoice is the final amount that you owe to AWS.

Presentation of discounts, credits, refunds, and taxes

The billing data on the **Bills** page (for example, in the **Charges by service** tab) excludes refunds, while Cost Explorer data includes refunds. When a refund is issued, this might cause differences in other charge types.

For example, let's say that a portion of your taxes was refunded. On the **Bills** page, the **Taxes by service** tab will continue to show the full tax amount. The Cost Explorer data will show the post-refund tax amount.

Analyzing your costs with AWS Cost Explorer

AWS Cost Explorer is a tool that enables you to view and analyze your costs and usage. You can explore your usage and costs using the main graph, the Cost Explorer cost and usage reports, or the Cost Explorer RI reports. You can view data for up to the last 13 months, forecast how much you're likely to spend for the next 12 months, and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to identify areas that need further inquiry and see trends that you can use to understand your costs.

You can view your costs and usage using the Cost Explorer user interface free of charge. You can also access your data programmatically using the Cost Explorer API. Each paginated API request incurs a charge of $0.01. You can't disable Cost Explorer after you enable it.

In addition, Cost Explorer provides preconfigured views that display at-a-glance information about your cost trends and give you a head start on customizing views that suit your needs.

When you first sign up for Cost Explorer, AWS prepares the data about your costs for the current month and the last 13 months, and then calculates the forecast for the next 12 months. The current month's data is available for viewing in about 24 hours. The rest of your data takes a few days longer. Cost Explorer refreshes your cost data at least once every 24 hours. However, this depends on your upstream data from your billing applications, and some data might be updated later than 24 hours. After you sign up, Cost Explorer by default can display up to 13 months of historical data (if you have that much), the current month, and the forecasted costs for the next 12 months. The first time that you use Cost Explorer, Cost Explorer walks you through the main parts of the console with an explanation for each section.

Cost Explorer uses the same dataset that is used to generate the AWS Cost and Usage Reports and the detailed billing reports. For a comprehensive review of the data, you can download it into a comma-separated value (CSV) file.

Topics

- Enabling Cost Explorer
- Getting started with Cost Explorer
- Exploring your data using Cost Explorer
- Exploring more data for advanced cost analysis
- Using the AWS Cost Explorer API

- Analyzing your Cost Explorer data with Amazon Q (preview)

Enabling Cost Explorer

You can enable Cost Explorer for your account by opening Cost Explorer for the first time in the AWS Cost Management console. You can't enable Cost Explorer using the API. After you enable Cost Explorer, AWS prepares the data about your costs for the current month and the previous 13 months, and then calculates the forecast for the next 12 months. The current month's data is available for viewing in about 24 hours. The rest of your data takes a few days longer. Cost Explorer updates your cost data at least once every 24 hours.

As part of the process of enabling Cost Explorer, AWS automatically configures Cost Anomaly Detection for your account. Cost Anomaly Detection is an AWS Cost Management feature. This feature uses machine learning models to detect and alert on anomalous spend patterns in your deployed AWS services. To get you started with Cost Anomaly Detection, AWS sets up an AWS services monitor and a daily summary alert subscription. You're alerted about any anomalous spend that exceeds $100 and 40% of your expected spend across the majority of your AWS services in your accounts. For more information, see limitations and Detecting unusual spend with AWS Cost Anomaly Detection.

Note

You can opt out of Cost Anomaly Detection at any time. For more information, see Opting out of Cost Anomaly Detection.

You can launch Cost Explorer if your account is a member account in an organization where the management account enabled Cost Explorer. Know that your organization's management account can also deny your account access. For more information, see Consolidated billing for AWS Organizations.

Note

An account’s status within an organization determines what cost and usage data are visible:

- A standalone account joins an organization. After this, the account can no longer access cost and usage data from when the account was a standalone account.

- A member account leaves an organization to become a standalone account. After this, the account can no longer access cost and usage data from when the account was a member of the organization. The account can access only the data that's generated as a standalone account.
- A member account leaves organization A to join organization B. After this, the account can no longer access cost and usage data from when the account was a member of organization A. The account can access only the data that's generated as a member of organization B.
- An account rejoins an organization that the account previously belonged to. After this, the account regains access to its historical cost and usage data.

Signing up to receive the AWS Cost and Usage Reports or the Detailed Billing Report doesn't automatically enable Cost Explorer. To do so, follow this procedure.

To sign up for Cost Explorer

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Cost Explorer**.
3. On the **Welcome to Cost Explorer** page, choose **Launch Cost Explorer**.

For more information about controlling access to Cost Explorer, see Controlling access to Cost Explorer.

Controlling access to Cost Explorer

You can manage access to your Cost Explorer in the following ways:

- Using the management account, you can enable Cost Explorer as a root user, automatically enabling all member accounts.
- After member accounts are enabled, you can change Cost Explorer settings from within the management account. You can control the information that can be accessed in Cost Explorer. This includes costs, refunds or credits, discounts, and Reserved Instance (RI) recommendations.
- After you enable Cost Explorer at the management account level, you can manage user IAM policies. For example, you can grant users full access or deny users access to Cost Explorer.

This topic provides information about how to control access in Cost Explorer.

For information about managing access to Billing and Cost Management pages, see Overview of managing access permissions.

To reference Cost Explorer IAM policies, see Using identity-based policies (IAM policies) for AWS Cost Management.

For more information about consolidated billing, see Consolidated billing for AWS Organizations.

Topics

- Granting Cost Explorer access
- Controlling access using Cost Explorer preferences
- Managing Cost Explorer access for users

Granting Cost Explorer access

If you're signed into the management account with your root account credentials, you can enable Cost Explorer access. Your root account credentials are through the Billing and Cost Management console. Enabling Cost Explorer at the management account level enables Cost Explorer for all of your organization accounts. All accounts in the organization are granted access, and you can't grant or deny access individually.

Controlling access using Cost Explorer preferences

A management account can grant access to Cost Explorer for all or none of the member accounts. Access isn’t customizable for each individual member account.

The management account in AWS Organizations has full access to all Billing and Cost Management information for costs incurred by both the management account and member accounts. Member accounts only have access to their own cost and usage data in Cost Explorer.

By default, the management account in AWS Organizations sees all costs at the chargeable rate. If an organization is onboarded to Billing Conductor, the management account also sees costs at the proforma rate. The Cost Explorer view for member accounts depends on the configuration in Billing Conductor.

The owner of a management account can do the following:

- View all costs in Cost Explorer.
- Grant all member accounts the permission to see the costs for their own member account, refunds, credits, and RI recommendations.

Member account owners can't see costs, refunds, and RI recommendations for other accounts in the Organizations. For more information about consolidated billing, see Consolidated billing for AWS Organizations.

If you're an AWS account owner and not using consolidated billing, you have full access to all Billing and Cost Management information including Cost Explorer.

If you're onboarded to Billing Conductor, the Cost Explorer view for member accounts depends on whether a member account is part of a billing group.

If a member account is part of a billing group:

- The member account sees all costs at the proforma rate.
- Cost Explorer preferences, such as **Linked Account Access**, **Linked Account Refunds and Credits**, **Linked Account Discounts**, **Hourly and Resource Level Data**, and **Split cost allocation data** are not applicable to the member account.

If a member account is not part of a billing group:

- The member account see costs at the chargeable rate.
- Cost Explorer preferences apply to the member account.

For more information about Billing Conductor, see the Billing Conductor User Guide.

Organizations account status use cases

An account’s status within an organization determines what cost and usage data are visible in the following ways:

- A standalone account joins an organization. After this, the account can no longer access cost and usage data from when the account was a standalone account.
- A member account leaves an organization to become a standalone account. After this, the account can no longer access cost and usage data from when the account was a member of their

previous organization. The account can only access the data that's generated as a standalone account.

- A member account leaves organization A to join organization B. After this, the account can no longer access cost and usage data from organization A. The account can access only the data that's generated as a member of organization B.
- An account rejoins an organization that it previously belonged to. After this, the account regains access to its historical cost and usage data.

Controlling member accounts’ access using Cost Explorer preferences

You can grant or restrict the access to all member accounts in your Organizations. When you enable your account at the management account level, all member accounts are granted access to their cost and usage data by default.

To control member account access to Cost Explorer data

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Cost Management Preferences**.
3. On the **Preferences** page, under **Member account permissions** in the **General** tab, select or clear **Linked account access**.
4. Choose **Save preferences**.

Managing Cost Explorer access for users

After you enable Cost Explorer at the management account level, you can use IAM to manage access to your billing data for individual users. This way, you can grant or revoke access on an individual level for each account, rather than granting access to all member accounts.

A user must be granted explicit permissions to view pages in the Billing and Cost Management console. With the appropriate permissions, the user can view costs for the AWS account that the user belongs to. For the policy that grants the necessary permissions to a user, see Overview of managing access permissions.

Getting started with Cost Explorer

After you enable Cost Explorer, you can launch it from the AWS Cost Management console.

Starting Cost Explorer

Start Cost Explorer by opening the AWS Cost Management console.

To open Cost Explorer

- Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.

This opens the Cost dashboard that shows you the following:

- Your estimated costs for the month to date
- Your forecasted costs for the month
- A graph of your daily costs
- Your five top cost trends
- A list of reports that you recently viewed

Exploring your data using Cost Explorer

On the Cost Explorer dashboard, Cost Explorer shows your estimated costs for the month to date, your forecasted costs for the month, a graph of your daily costs, your five top cost trends, and a list of reports that you recently viewed.

All costs reflect your usage up to the previous day. For example, if today is December 2, the data includes your usage through December 1.

> **Note**
>
> In the current billing period, the data depends on your upstream data from your billing applications, and some data might be updated later than 24 hours.

- Your Cost Explorer costs
- Your Cost Explorer trends
- Your daily unblended costs
- Your monthly unblended costs

- Your net unblended costs
- Your recent Cost Explorer reports
- Your amortized costs
- Your net amortized costs

Navigating Cost Explorer

You can use the icons in the left pane to do the following:

- Go to the main Cost Explorer dashboard
- See a list of the default Cost Explorer reports
- See a list of your saved reports
- See information about your reservations
- See your reservation recommendations

Your Cost Explorer costs

At the top of the **Cost Explorer** page are the **Month-to-date costs** and **Forecasted month end costs**. The **Month-to-date costs** shows how much you're estimated to have incurred in charges so far this month and compares it to this time last month. The **Forecasted month end costs** shows how much Cost Explorer estimates that you will owe at the end of the month and compares your estimated costs to your actual costs of the previous month. The **Month-to-date costs** and the **Forecasted month end costs** don't include refunds.

The costs for Cost Explorer are only shown in US dollars.

Your Cost Explorer trends

In the ***this month*** **trends** section, Cost Explorer shows your top cost trends. For example, your costs related to a specific service have gone up, or your costs from a specific type of RI have gone up. To see all of your costs trends, choose **View all trends** in the upper-right corner of the trend section.

To understand a trend in more depth, choose it. You're taken to a Cost Explorer chart that shows the costs that went into calculating that trend.

Your daily unblended costs

In the center of the Cost Explorer dashboard, Cost Explorer shows a graph of your current unblended daily costs. You can access the filters and parameters used to create the graph by choosing **Explore costs** in the upper-right corner. That takes you to the Cost Explorer report page, enabling you to access the default Cost Explorer reports and modify the parameters used to create the chart. The Cost Explorer reports offer additional functionality such as downloading your data as a CSV file and saving your specific parameters as a report. For more information, see Using Cost Explorer reports. Your daily unblended costs don't include refunds.

Your monthly unblended costs

Monthly granularity

You can view your unblended costs at the monthly granularity and see the discounts applied to your monthly bill. When forecasting costs, discounts are included by default. To view your unblended costs, open the Cost Explorer page and choose **Cost Explorer** from the navigation pane. Discounts appear as the **RI Volume Discount** in the chart. The discount amount aligns with the discount amount shown in your Billing and Cost Management console.

To see the details in your Billing and Cost Management console

1. Sign in to the AWS Management Console and open the AWS Billing console at https://console.aws.amazon.com/billing/.
2. In the navigation pane, choose **Bills**.
3. To display the discount, select the arrow next to **Total Discounts**, under **Credits, Total Discounts and Tax Invoices**.

Monthly gross charges

You can view your gross monthly charges by excluding the **RI Volume Discount**.

To exclude RI volume discounts in your monthly view

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the left pane, choose **Cost Explorer**.
3. Choose **Cost & Usage**.

4. On the **Filters** pane, choose **Charge Type**.
5. Select **RI Volume Discount**.
6. To open a dropdown, select **Include only** and choose **Exclude only**.
7. Select **Apply filters**.

Your net unblended costs

This enables you to see your net costs after all applicable discounts are calculated. You should still exclude any manual adjustment such as refunds and credits as a best practice. **RI Volume Discounts** are no longer visible because these are post-discount amounts.

Your recent Cost Explorer reports

At the bottom of the Cost Explorer dashboard is a list of reports that you have accessed recently, when you accessed them, and a link back to the report. This enables you to switch between reports or remember the reports that you find most useful.

For more information about Cost Explorer reports, see Using Cost Explorer reports.

Your amortized costs

This enables you to see the cost of your AWS commitments, such as Amazon EC2 Reserved Instances or Savings Plans, spread across the usage of the selection period. AWS estimates your amortized costs by combining the unblended upfront and recurring reservation fees, and calculates the effective rate over the period of time that the upfront or recurring fee applies. In the daily view, Cost Explorer shows the unused portion of your commitment fees at the first of the month or the date of purchase.

Your net amortized costs

This enables you to see the cost of your AWS commitments, such as Amazon EC2 Reserved Instances or Savings Plans, after discounts with the additional logic that shows how the actual cost applies over time. Since Savings Plans and Reserved Instances usually have upfront or recurring monthly fees associated with them, the net amortized cost dataset reveals the true cost by showing how post-discount fees amortize over the period of time that the upfront or recurring fee applies.

Using the Cost Explorer chart

By default, you can view your costs at the chargeable rate as either a cash-based view with unblended costs or as an accrual-based view. In a cash-based view, your costs are recorded when cash is received or paid. In an accrual-based view, your costs are recorded when income is earned or costs are incurred. You can view data for up to the last 13 months, the current month, and forecast how much you're likely to spend for the next 12 months. You can also specify time ranges for the data and view time data by day or by month.

By default, Cost Explorer uses the **Group by** filter for the **Daily unblended costs** graph. When using the **Group by** filter, the Cost Explorer chart displays data for up to ten values in the **Group by** filter. If your data contains additional values, the chart displays nine bars or lines and then aggregates all remaining items in a tenth. The data table that's below the chart breaks out the data for individual services that are aggregated in the chart.

If your organization is onboarded to Billing Conductor, member accounts placed in billing groups automatically see your costs in Cost Explorer at the proforma rate configured in Billing Conductor. Member accounts can view costs and usage starting from when they joined their current billing group, and will lose access to the chargeable data for the period prior to joining their current billing group. If a backfill of proforma billing data is needed, submit a support ticket requesting a proforma backfill from the Billing Conductor team.

For more information about proforma rate configurations, see the Billing Conductor User Guide.

Topics

- Modifying your chart
- Reading the Cost Explorer data table
- Forecasting with Cost Explorer

Modifying your chart

You can modify the parameters that Cost Explorer uses to create your chart to explore different sets of data.

- Selecting a style for your chart
- Choosing time ranges for the data that you want to view
- Grouping data by filter type

- Filtering the data that you want to view
- Choosing advanced options

Selecting a style for your chart

Cost Explorer provides three styles for charting your cost data:

- Bar charts (**Bar**)
- Stacked bar charts (**Stack**)
- Line graphs (**Line**)

You can set the style by choosing one of the views on the top right corner of the chart.

Choosing time ranges for the data that you want to view

You can choose to view your cost data in monthly or daily *levels of granularity*. You can use preconfigured time ranges or set custom start and end dates.

To set the granularity and time range for your data

1. Start Cost Explorer.
2. Choose a time granularity of **Daily**, **Monthly**, or **Hourly**.

   > **Note**
   >
   > To enable hourly granularity, opt in through the Cost Explorer console **Preferences** page as the management account. When hourly granularity is enabled, information is available for the previous 14 days.

3. For your monthly or daily data, open the calendar and define a custom time range for your report. Or, alternatively, choose a preconfigured time range (**Auto-select**) using the dropdowns shown below the calendar. You can choose from a number of historical or forecast time ranges. The name of the time range that you choose appears in the calendar.
4. Choose **Apply**.

Historical time range options

In Cost Explorer, months are defined as calendar months. Days are defined as 12:00:00 AM to 11:59:59 PM. Based on these definitions, when you choose **Last 3 Months** for a date range, you see cost data for the 3 previous months. This doesn't include the present month. For example, if you view your chart on June 6, 2017, and select **Last 3 Months**, your chart includes data for March, April, and May 2017. All times are in Universal Coordinated Time (UTC).

You can choose time ranges for both your past costs and your forecasted future costs.

The following list defines each time range option for your past costs in Cost Explorer.

- Custom

  Displays data for the **From** and **To** time range that you specify with calendar controls.
- 1D (Last 1 Day)

  Displays cost data from the previous day.
- 7D (Last 7 Days)

  Displays cost data from the day before and the previous 6 days.
- Current Month

  Displays cost data and forecast data for the current month.
- 3M (Last 3 Months)

  Includes cost data from the previous 3 months but doesn't include the current month.
- 6M (Last 6 Months)

  Includes cost data from the previous 6 months but doesn't include the current month.
- 1Y (Last 12 Months)

  Includes cost data from the previous 12 months but doesn't include the current month.
- MTD (Month to Date)

  Displays cost data from the current calendar month.
- YTD (Year to Date)

  Displays cost data from the current calendar year.

Forecast time range options

With the **Daily** or **Monthly** time granularity, you have the option to view forecast costs in Cost Explorer. The following list defines each time range option for your forecast data. You can select a **Historical** time range and a **Forecasted** time range to display together. For example, you can select a **Historical** time range of 3 months (3M) and select a **Forecasted** time range of 3 months (+3M). Your report includes historical data for the previous 3 months plus forecasted data for the next 3 months. To clear a **Historical** time range and see only the forecast, choose the **Historical** time range option again.

> **Note**
>
> If you choose any forecasted dates, your current date’s cost and usage data shows as **Forecast**. The current date’s cost and usage won't include historical data.

- Custom

  Displays forecast data for the **From** and **To** time range that you specify with calendar controls.
- +1M

  Displays forecast data for the next month. This option is available if you choose the **Daily** time granularity.
- +3M

  Displays forecast data for the next 3 months. This option is available if you choose the **Daily** or **Monthly** time granularity.
- +12M

  Displays forecast data for the next 12 months. This option is available if you choose the **Monthly** time granularity.

Grouping data by filter type

Use the **Group by** button to have Cost Explorer display the cost data groups by filter type. By default, Cost Explorer doesn't use grouping. Forecasting isn't available for charts that have grouping. If you don't select a **Group by** option, Cost Explorer displays total costs for the specified date range.

To group your data by filter type

1. Launch Cost Explorer.
2. (Optional) Use the **Filters** controls to configure a view of your cost data.
3. Choose a **Group by** option to group by the category that you want. The data table below the chart also groups your cost figures by the category that you select.

Filtering the data that you want to view

With Cost Explorer, you can filter how you view your AWS costs by one or more of the following values:

- **API operation**
- **Availability Zone (AZ)**
- **Billing entity**
- **Charge type**
- **Include all**
- **Instance type**
- **Legal entity**
- **Linked account**
- **Platform**
- **Purchase option**
- **Region**
- **Resources**
- **Service**
- **Tag**
- **Tenancy**
- **Usage type**
- **Usage type group**

You can use Cost Explorer to see which service you use the most, which Availability Zone (AZ) most of your traffic is in, and which member account uses AWS the most. You can also apply multiple filters to look at intersecting datasets. For example, you can use the **Linked Account** and **Services** filters to identify the member account that spent the most money on Amazon EC2.

To filter your data

1. Open Cost Explorer.
2. For **Filters**, choose a value. After you make a selection, a new control appears with additional options.
3. In the new control, select the items from each list that you want to display in the chart. Or, start typing in the search box to have Cost Explorer autocomplete your selection. After you choose your filters, choose **Apply filters**.

   > **Note**
   >
   > Each time that you apply filters to your costs, Cost Explorer creates a new chart. However, you can use your browser's bookmark feature to save configuration settings for repeated use. Forecasts aren't saved, and Cost Explorer displays the most recent forecast when you revisit your saved chart.

You can continue refining your cost analysis by using multiple filters, grouping your data by filter type, and choosing **Advanced Options** tab options.

Combining filters to show data in common

Cost Explorer displays a chart that represents the data in common to all the filters that you have selected. You can use this view to analyze subsets of cost data. For example, assume that you set the **Service** filter to show costs that are related to Amazon EC2 and Amazon RDS services and then select **Reserved** using the filter. The cost chart will show how much money **Reserved** instances on Amazon EC2 and Amazon RDS cost for each of the three months.

> **Note**
>
> - AWS Cost and Usage Reports in Cost Explorer can use a maximum of 1024 filters.
> - You can filter RI Utilization reports by only one service at a time. You can do this only for the following services:
>   - Amazon EC2

- Amazon Redshift
- Amazon RDS
- ElastiCache
- OpenSearch Service

Filters and logical operations (AND/OR)

When you select multiple filters and multiple values for each filter, Cost Explorer applies rules that emulate the logical AND and OR operators to your selections. Within each filter, Cost Explorer emulates the logical OR filter to your selection of filter types. This means that the resulting chart adds the aggregate costs for each item together. Using the previous example, you see bars for both of the selected services, Amazon EC2 and Amazon RDS.

When you select multiple filters, Cost Explorer applies the logical AND operator to your selections. For a more concrete example, assume that you use the **Services** filter and specify Amazon EC2 and Amazon RDS costs for inclusion and then also apply the **Purchase Options** filter to select a single type of purchase option. You will see *only* the **Non-Reserved** charges incurred by Amazon EC2 and Amazon RDS.

Filter and group options

In Cost Explorer, you can filter by the following groups:

- **API operation**

  Requests made to and tasks performed by a service, such as write and get requests to Amazon S3.
- **Availability Zone**

  Distinct locations within a Region that are insulated from failures in other Availability Zones. They provide inexpensive, low-latency network connectivity to other Availability Zones in the same Region.
- **Billing entity**

  Helps you identify whether your invoices or transactions are for AWS Marketplace or for purchases of other AWS services. Possible values include:
  - AWS: Identifies a transaction for AWS services other than in AWS Marketplace.

  - AWS Marketplace: Identifies a purchase in AWS Marketplace.
- **Charge type**

  Different types of charges or fees.

  Credit

  Any AWS credits that are applied to your account.

  Other out-of-cycle charges

  Any subscription charges that aren't upfront reservation charges or support charges.

  Recurring reservation fee

  Any recurring charges to your account. When you purchase a Partial Upfront or No Upfront Reserved Instance from AWS, you pay a recurring charge in exchange for a lower rate for using the instance. The recurring fees can result in spikes on the first day of every month, when AWS charges your account.

  Refund

  Any refunds that you received. Refunds are listed as a separate line item in the data table. They don't appear as an item in the chart because they represent a negative value in the calculation of your costs. The chart displays only positive values.

  Reservation applied usage

  Usage that AWS applied reservation discounts to.

  Savings Plan upfront fee

  Any one-time upfront fee from your purchase of an All Upfront or Partial Upfront Savings Plan.

  Savings Plan recurring fee

  Any recurring hourly charges that correspond with your No Upfront or Partial Upfront Savings Plan. The Savings Plan recurring fee is initially added to your bill on the day that you purchase a No Upfront or Partial Upfront Savings Plan. After the initial purchase, AWS adds the recurring fee hourly.

  For an All Upfront Savings Plan, the line item indicates the portion of the Savings Plan unused during the billing period. For example, if a Savings Plan was 100% utilized for a billing period, this shows as “0” in your amortized costs view. Any number greater than “0” indicates an unused Savings Plan.

Savings Plan covered usage

Any on-demand cost that's covered by your Savings Plan. In an **Unblended costs** view, this represents the covered usage at on-demand rates. In an **Amortized costs** view, this represents the covered usage at your Savings Plan rates. Savings Plan covered usage line items are offset by the corresponding Savings Plan negation items.

Savings Plan negation

Any offset cost through your Savings Plan benefit that’s associated with the corresponding Savings Plan covered usage item.

Support fee

Any charges that AWS charges you for a support plan. When you purchase a support plan from AWS, you pay a monthly charge in exchange for service support. The monthly fees can result in spikes on the first day of every month, when AWS charges your account.

Tax

Any taxes that are associated with the charges or fees in your cost chart. Cost Explorer adds all taxes together as a single component of your costs. If you select five or fewer filters, Cost Explorer displays your tax expenses as a single bar. If you select six or more filters, Cost Explorer displays five bars, stacks, or lines, and then aggregates all remaining items, including taxes, into a sixth bar, stack slice, or plot line that's labeled **Other**.

If you choose to omit **RI upfront fees**, **RI recurring charges**, or **Support charges** from your chart, Cost Explorer continues to include any taxes that are associated with the charges.

Cost Explorer displays your tax costs in the chart only when you choose **Monthly** drop down. When you filter your cost chart, the following rules govern the inclusion of taxes:

1. Taxes are excluded if you select non-**Linked Account** filters, either singly or in combination with other filters.
2. Taxes are included if you select the **Linked Accounts** filters.

Upfront reservation fee

Any upfront fees that are charged to your account. When you purchase an All Upfront or Partial Upfront Reserved Instance from AWS, you pay an upfront fee in exchange for a lower rate for using the instance. The upfront fees can result in spikes in the chart for the days or months when you make your purchases.

Usage

Usage that AWS didn't apply reservation discounts to.

- **Instance type**

  The type of RI that you specified when you launched an Amazon EC2 host, Amazon RDS instance class, Amazon Redshift node, or Amazon ElastiCache node. The instance type determines the hardware of the computer used to host your instance.

- **Legal entity**

  The Seller of Record of a specific product or service. In most cases, the invoicing entity and legal entity are the same. The values might differ for third-party AWS Marketplace transactions. Possible values include:

  - Amazon Web Services, Inc. – The entity that sells AWS services.
  - Amazon Web Services India Private Limited – The local Indian entity that acts as a reseller for AWS services in India.

- **Linked account**

  The member accounts in an organization. For more information, see Consolidated billing for AWS Organizations.

- **Platform**

  The operating system that your RI runs on. **Platform** is either **Linux** or **Windows**.

- **Purchase option**

  The method you choose to pay for your Amazon EC2 instances. This includes Reserved Instances, Spot Instances, Scheduled Reserved Instances, and On-Demand Instances.

- **Region**

  The geographic areas where AWS hosts your resources.

- **Resources**

  The unique identifier for your resources.

> **Note**
>
> To enable resource granularity, opt-in through on the Cost Explorer settings page as the management account. This is available for Amazon EC2 instances.

- **Service**

  AWS products. To learn what's available, see AWS Products and Services. You can use this dimension to filter costs by specific AWS Marketplace software, including your costs for AMIs, web services, and desktop apps. See the What is AWS Marketplace? guide for more information.

  > **Note**
  >
  > You can only filter RI Utilization reports by one service at a time and only for these services: **Amazon EC2**, **Amazon Redshift**, **Amazon RDS**, and **ElastiCache**.

- **Tag**

  A label that you can use to track the costs associated with specific areas or entities within your business. For more information about working with tags, see Applying User-Defined Cost Allocation Tags.

- **Tenancy**

  Specifies if the Amazon EC2 instance is hosted on shared or single-tenant hardware. Some tenancy values include **Shared (Default)**, **Dedicated**, and **Host**.

- **Usage type**

  Usage types are the units that each service uses to measure the usage of a specific type of resource. For example, the `BoxUsage:t2.micro(Hrs)` usage type filters by the running hours of Amazon EC2 `t2.micro` instances.

- **Usage type group**

  Usage type groups are filters that collect a specific category of usage type filters into one filter. For example, `BoxUsage:c1.medium(Hrs)`, `BoxUsage:m3.xlarge(Hrs)`, and `BoxUsage:t1.micro(Hrs)` are all filters for Amazon EC2 instance running hours, so they are collected into the `EC2: Running Hours` filter.

Usage type groups are available for DynamoDB, Amazon EC2, ElastiCache, Amazon RDS, Amazon Redshift, and Amazon S3. The specific groups available to your account depend on what services you've used. The list of groups that might be available includes but isn't limited to the following:

- **DDB: Data Transfer - Internet (In)**

  Filters by the costs associated with how many GB are transferred to your DynamoDB databases.
- **DDB: Data Transfer - Internet (Out)**

  Filters by the costs associated with how many GB are transferred from your DynamoDB databases.
- **DDB: Indexed Data Storage**

  Filters by the costs associated with how many GB that you have stored in DynamoDB.
- **DDB: Provisioned Throughput Capacity - Read**

  Filters by the costs associated with how many units of read capacity that your DynamoDB databases used.
- **DDB: Provisioned Throughput Capacity - Write**

  Filters by the costs associated with how many units of write capacity that your DynamoDB databases used.
- **EC2: CloudWatch - Alarms**

  Filters by the costs associated with how many CloudWatch alarms that you have.
- **EC2: CloudWatch - Metrics**

  Filters by the costs associated with how many CloudWatch metrics that you have.
- **EC2: CloudWatch - Requests**

  Filters by the costs associated with how many CloudWatch requests that you make.
- **EC2: Data Transfer - CloudFront (Out)**

  Filters by the costs associated with how many GB are transferred from your Amazon EC2 instances to a CloudFront distribution.
- **EC2: Data Transfer - CloudFront (In)**

Filters by the costs associated with how many GB are transferred to your Amazon EC2 instances from a CloudFront distribution.

- **EC2: Data Transfer - Inter AZ**

  Filters by the costs associated with how many GB are transferred into, out of, or between your Amazon EC2 instances in different AZs.
- **EC2: Data Transfer - Internet (In)**

  Filters by the costs associated with how many GB are transferred to your Amazon EC2 instances from outside the AWS network.
- **EC2: Data Transfer - Internet (Out)**

  Filters by the costs associated with how many GB are transferred from an Amazon EC2 instance to a host outside the AWS network.
- **EC2: Data Transfer - Region to Region (In)**

  Filters by the costs associated with how many GB are transferred to your Amazon EC2 instances from a different AWS Region.
- **EC2: Data Transfer - Region to Region (Out)**

  Filters by the costs associated with how many GB are transferred from your Amazon EC2 instances to a different AWS Region.
- **EC2: EBS - I/O Requests**

  Filters by the costs associated with how many I/O requests that you make to your Amazon EBS volumes.
- **EC2: EBS - Magnetic**

  Filters by the costs associated with how many GB that you have stored on Amazon EBS Magnetic volumes.
- **EC2: EBS - Provisioned IOPS**

  Filters by the costs associated with how many IOPS-months that you have provisioned for Amazon EBS.
- **EC2: EBS - SSD(gp2)**

Filters by the costs associated with how many GB per month of General Purpose storage that your Amazon EBS volumes use.

- **EC2: EBS - SSD(io1)**

  Filters by the costs associated with how many GB per month of Provisioned IOPS SSD storage that your Amazon EBS volumes use.
- **EC2: EBS - Snapshots**

  Filters by the costs associated with how many GB per month that your Amazon EBS snapshots store.
- **EC2: EBS - Optimized**

  Filters by the costs associated with how many MB per instance hour that your Amazon EBS-optimized instances use.
- **EC2: ELB - Running Hours**

  Filters by the costs associated with how many hours that your Elastic Load Balancing load balancers ran.
- **EC2: Elastic IP - Additional Address**

  Filters by the costs associated with how many Elastic IP addresses that you attached to running Amazon EC2 instances.
- **EC2: Elastic IP - Idle Address**

  Filters by the costs associated with Elastic IP addresses that you have that aren't attached to running Amazon EC2 instances.
- **EC2: NAT Gateway - Data Processed**

  Filters by the costs associated with how many GB that your network address translation gateways (NAT gateways) processed.
- **EC2: NAT Gateway - Running Hours**

  Filters by the costs associated with how many hours that your NAT gateways ran.
- **EC2: Running Hours**

  Filters by the costs associated with how many hours that your Amazon EC2 instances ran.

  This **Usage Type Group** contains only the following **Usage Types**:

  - BoxUsage
  - DedicatedUsage
  - HostBoxUsage
  - HostUsage
  - ReservedHostUsage
  - SchedUsage
  - SpotUsage
  - UnusedBox

- **ElastiCache: Running Hours**

  Filters by the costs associated with how many hours that your Amazon ElastiCache nodes ran.

- **ElastiCache: Storage**

  Filters by the costs associated with how many GB that you stored in Amazon ElastiCache.

- **RDS: Running Hours**

  Filters by the costs associated with how many hours that your Amazon RDS databases ran.

  This **Usage Type Group** contains only the following **Usage Types**:

  - AlwaysOnUsage
  - BoxUsage
  - DedicatedUsage
  - HighUsage
  - InstanceUsage
  - MirrorUsage
  - Multi-AZUsage
  - SpotUsage

- **RDS: Data Transfer – CloudFront – In**

  Filters by the costs associated with how many GB are transferred into Amazon RDS from a CloudFront distribution.

- **RDS: Data Transfer – CloudFront – Out**

Filters by the costs associated with how many GB are transferred from a CloudFront distribution to Amazon RDS data transfers.

- **RDS: Data Transfer – Direct Connect Locations – In**

  Filters by the costs associated with how many GB are transferred into Amazon RDS through a Direct Connect network connection.
- **RDS: Data Transfer – Direct Connect Locations – Out**

  Filters by the costs associated with how many GB are transferred from Amazon RDS through a Direct Connect network connection.
- **RDS: Data Transfer – InterAZ**

  Filters by the costs associated with how many GB are transferred into, out of, or between Amazon RDS buckets in different Availability Zones.
- **RDS: Data Transfer – Internet – In**

  Filters by the costs associated with how many GB are transferred to your Amazon RDS databases.
- **RDS: Data Transfer – Internet – Out**

  Filters by the costs associated with how many GB are transferred from your Amazon RDS databases.
- **RDS: Data Transfer – Region to Region – In**

  Filters by the costs associated with how many GB are transferred to your Amazon RDS instances from a different AWS Region.
- **RDS: Data Transfer – Region to Region – Out**

  Filters by the costs associated with how many GB are transferred from your Amazon RDS instances to a different AWS Region.
- **RDS: I/O Requests**

  Filters by the costs associated with how many I/O requests that you make to your Amazon RDS instance.
- **RDS: Provisioned IOPS**

Filters by the costs associated with how many IOPS-months that you have provisioned for Amazon RDS.

- **RDS: Storage**

  Filters by the costs associated with how many GB that you have stored in Amazon RDS.
- **Redshift: DataScanned**

  Filters by the costs associated with how many GB that your Amazon Redshift nodes scanned.
- **Redshift: Running Hours**

  Filters by the costs associated with how many hours that your Amazon Redshift nodes ran.
- **S3: API Requests - Standard**

  Filters by the costs associated with GET and all other standard storage Amazon S3 requests.
- **S3: Data Transfer - CloudFront (In)**

  Filters by the costs associated with how many GB are transferred into Amazon S3 from a CloudFront distribution.
- **S3: Data Transfer - CloudFront (Out)**

  Filters by costs associated with how many GB are transferred from a CloudFront distribution to Amazon S3 data transfers, such as how much data was uploaded from your Amazon S3 bucket to your CloudFront distribution.
- **S3: Data Transfer - Inter AZ**

  Filters by the costs associated with how many GB are transferred into, out of, or between Amazon S3 buckets in different Availability Zones.
- **S3: Data Transfer - Internet (In)**

  Filters by the costs associated with how many GB are transferred to an Amazon S3 bucket from outside the AWS network.
- **S3: Data Transfer - Internet (Out)**

  Filters by the costs associated with how many GB are transferred from an Amazon S3 bucket to a host outside the AWS network.
- **S3: Data Transfer - Region to Region (In)**

Filters by the costs associated with how many GB are transferred to Amazon S3 from a different AWS Region.

- **S3: Data Transfer - Region to Region (Out)**

  Filters by the costs associated with how many GB are transferred from Amazon S3 to a different AWS Region.
- **S3: Storage - Standard**

  Filters by the costs associated with how many GB that you have stored in Amazon S3.

Choosing advanced options

You can customize how you view your data in Cost Explorer using **Advanced options** to include or exclude specific types of data.

To include or exclude data

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Cost Explorer**.
3. In the right pane, under **Advanced options**, under **Aggregate costs by**, choose between the following:

   - **Unblended costs**: This cost metric reflects the cost of the usage. When grouped by **Charge type**, unblended costs separate discounts into their own line items. This enables you to view the amount of each discount received.
   - **Amortized costs**: This cost metric reflects the effective cost of the upfront and monthly reservation fees spread across the billing period. By default, Cost Explorer shows the fees for Reserved Instances as a spike on the day that you're charged. However, if you choose to show costs as amortized costs, the costs are amortized over the billing period. This means that the costs are broken out into the effective daily rate. AWS estimates your amortized costs by combining your unblended costs with the amortized portion of your upfront and recurring reservation fees. For the daily view, Cost Explorer shows the unused portion of your upfront reservation fees and recurring RI charges on the first of the month.

     For example, suppose that Alejandro purchases a Partial Upfront `t2.micro` RI for a one-year term at $30 dollars upfront. The monthly fee is $2.48. Cost Explorer shows the costs for this RI as a spike on the first of the month. If Alejandro chooses **Amortized costs** for a 30-day month, the Cost Explorer chart shows a daily effective rate of $0.165. This is the EC2 effective rate multiplied by the number of hours in a day.

Amortized costs aren't available for billing periods before 2018. If you want to see how much of your reservation was unused, group by purchase option.

- **Blended costs**: This cost metric reflects the average cost of usage across the consolidated billing family. If you use the consolidated billing feature in AWS Organizations, you can view costs using *blended rates*. For more information, see Blended Rates and Costs.
- **Net unblended costs**: This cost metric reflects the cost after discounts.
- **Net amortized costs**: This cost metric amortizes the upfront and monthly reservation fees while including discounts such as RI volume discounts.

4. Under **Additional data settings**, select from the following:

- **Show forecasted values**: Cost Explorer displays a forecast for how much AWS predicts you will spend over the forecast time period that you select, based on your past costs.
- **Show only untagged resources**: By default, Cost Explorer includes costs both for resources that have cost allocation tags and for resources that don't have cost allocation tags. To find untagged resources that add to your costs, select **Show only untagged resources**. For more information about cost allocation tags, see Organizing and tracking costs using AWS cost allocation tags.
- **Show only uncategorized resources**: By default, Cost Explorer includes costs both for resources that are mapped to a cost category and for resources that aren’t mapped to a cost category. To find uncategorized resources that add to your costs, select **Show only uncategorized resources**. For more information about cost categories, see Organizing costs using AWS Cost Categories.

Reading the Cost Explorer data table

A data table follows each Cost Explorer chart. The data table displays the cost figures that the chart represents. If your chart is using a grouping, the data table displays the aggregate amounts for the filter types that you choose for your chart. If your chart isn't using a grouping, the table displays the aggregate amounts for your past and forecasted cost data. You can download the .csv file that contains the complete data set for your chart.

Note

For the RI Utilization and Savings report, the maximum table size is 20 rows. If the data exceeds this, it appears in a truncated form.

In the grouped data table, each row is a value for one of the filter type options: API operations, Availability Zones, AWS services, custom cost allocation tags, instance types, member accounts, purchase options, Region, usage type, or usage type group. The columns represent time intervals. For example, the data table shows the costs for selected services for the last three months in separate columns. Then, the last column of the data table shows the aggregated total for the 3 months.

Note

Data transfer costs are included in the services that they're associated with, such as Amazon EC2 or Amazon S3. They aren't represented as either a separate line item in the data table or a bar in the chart.

In the ungrouped data table, the row is your costs. The columns represent time intervals.

Forecasting with Cost Explorer

You create a forecast by selecting a future time range for your report. For more information, see Choosing time ranges for the data that you want to view. The following section discusses the accuracy of the forecasts created by Cost Explorer and how to read them.

A forecast is a prediction of how much you will use AWS services over the forecast time period that you selected. This forecast is based on your past usage. You can use a forecast to estimate your AWS bill and set alarms and budgets for based on predictions. Because forecasts are predictions, the forecasted billing amounts are estimated and might differ from your actual charges for each statement period.

Like weather forecasts, billing forecasts can vary in accuracy. Different ranges of accuracy have different prediction intervals. The higher the prediction interval, the more likely the forecast has a wider range. For example, suppose that you have a budget set to 100 dollars for a given month. An 80% prediction interval might forecast your spend between 90 and 100, with a mean of 95. The range in the prediction band is dependent on your historical spend volatility, or fluctuations. The more consistent and predictable the historical spend, the narrower the prediction range in forecast spend.

Cost Explorer forecasts have a prediction interval of 80%. If AWS doesn't have enough data to forecast an 80% prediction interval, Cost Explorer doesn't provide a forecast. This is common for accounts that have less than one full billing cycle.

Reading forecasts

How you read the Cost Explorer forecasts depends on the type of chart that you're using. Forecasts are available for both line charts and bar charts.

The 80% prediction interval appears differently on each type of chart:

- Line charts represent the prediction interval as a set of lines that are on either side of your costs line.
- Bar charts represent the prediction interval as two lines that are on either side of the top of your bar.

When forecasting costs, discounts are included by default.

> **Note**
>
> If you want your forecasts to include non-recurring discounts such as refunds, we encourage you to use **Show net unblended costs**. For more information about different costs, see Cost Explorer Advanced Options.

Using forecasts with consolidated billing

If you use the consolidated billing feature in AWS Organizations, the forecasts are calculated with the data from all the accounts. If you add a new member account to an organization, forecasts don't include that new member account until the new spending patterns of the organization are analyzed. For more information about consolidated billing, see Consolidated billing for AWS Organizations.

Exploring more data for advanced cost analysis

Cost Explorer provides AWS cost and usage data for the current month and up to the previous 13 months at daily and monthly granularity. You can query this data in the console or using the Cost Explorer API.

You can enable multi-year data (at monthly granularity) and more granular data (at hourly and daily granularity) for the previous 14 days. Once enabled, you can use this data in the console or using the Cost Explorer API.

Topics

- Multi-year data at monthly granularity
- Granular data
- Understanding your estimated monthly usage summary
- Configuring multi-year and granular data

Multi-year data at monthly granularity

While you can use the default 14-month historical data to perform cost analysis at quarterly or monthly level, you should enable multi-year data in Cost Explorer if you want to evaluate your year-over-year cost or identify long-term cost trends.

You can enable up to 38 months of multi-year data at monthly granularity for your entire organization. Using multi-year data to perform cost analysis over a longer duration, you can track changes in your AWS costs as your business or applications mature, or after implementing infrastructure optimizations.

Once enabled, multi-year data is available within 48 hours. Note that this data is only available in Cost Explorer, as Savings Plans and Reservations utilization and coverage reports don't support this data.

To enable multi-year data in Cost Explorer, see Configuring multi-year and granular data.

> **Note**
>
> We will disable multi-year data for your organization if no one in the organization accesses it in three consecutive months. However, if you need the data, you can re-enable it in Cost Management preferences.

Multi-year data is only available for chargeable costs in Cost Explorer. If you're onboarded to AWS Billing Conductor, you won’t be able to use this feature.

Granular data

Cost Explorer provides hourly and resource-level granularity through three features:

- Resource-level data at daily granularity
- Cost and usage data for all AWS services at hourly granularity (without resource-level data)
- EC2-Instances (Elastic Compute Cloud) resource-level data at hourly granularity

Enable one or all of these features based on how you plan on using granular data for your in-depth cost and usage analysis.

To enable granular data in Cost Explorer, see Configuring multi-year and granular data.

Note

Visibility into granular data is only supported for chargeable costs. If you’re onboarded to AWS Billing Conductor, you will not be able to view granular data in Cost Explorer.

Topics

- Resource-level data at daily granularity
- Cost and usage data for all AWS services at hourly granularity (without resource-level data) - paid feature
- EC2-Instances (Elastic Compute Cloud) resource-level data at hourly granularity

Resource-level data at daily granularity

In Cost Explorer, you can enable resource-level data for your chosen AWS services at daily granularity for the past 14 days.

You can apply **Group by: Resource** to understand the cost of services by resource ID that you have enabled resource-level data for. Costs associated with services that you have not enabled resource-level data for appear under **No resource ID** in Cost Explorer. If you want to focus on resource-level costs for a specific service, choose the **Resource** filter in Cost Explorer, select the service you want to analyze, and then select all resources (if you don't have a specific resource in mind) or a specific resource ID to understand cost and usage driven by that specific resource.

Use resource-level data to identify your cost drivers. When analyzing variances or anomalies in your AWS costs, you can group by service to first understand which service is causing the variance or anomaly. Then you can filter for that service in Cost Explorer and group by resource to create a view of costs per resource in that service. Use the Cost Explorer table and graphs to understand which specific resource has deviated from the normal usage pattern and is contributing to the variance or anomaly. If you want to understand how your spend on a specific resource has evolved over time, such as your spend on an S3 bucket, you can filter for that resource in Cost Explorer by selecting that resource ID in the **Resource** filter. Moreover, resource-level data is useful in order to understand which specific resources are consuming your Savings Plans and Reservations commitments. To create this view, you can filter for "Savings Plan Covered Usage" or "Reservation applied usage" charge types, group by resource, and filter for specific services that you have purchased Savings Plans and Reservations for.

Once enabled, resource-level data at daily granularity is available within 48 hours. Note that this data is not available for Savings Plans and Reservations utilization and coverage reports.

> **Note**
>
> We will disable resource-level data at daily granularity for your organization if no one in the organization accesses it in three consecutive months. However, if you need the data, you can re-enable it in Cost Management preferences.
> Cost Explorer displays the top 5,000 most costly resources per service. If you have more than 5,000 resources, you might not see all of them in the console. However, you can search for those resources using the resource ID. Consider using Cost and Usage Reports (CUR) to retrieve the cost and usage associated with all resources as a CSV file.

Cost and usage data for all AWS services at hourly granularity (without resource-level data) - paid feature

By default, Cost Explorer provides up to 14 months of data at daily and monthly granularity. However, you can opt in to hourly granularity for the past 14 days.

You can use hourly granularity to monitor cost and usage patterns at the most granular hourly level. Such data is especially useful to understand the peak hours for your AWS usage and how high the cost can go during those peak hours. If you're thinking about purchasing Savings Plans or Reserved Instances, hourly granularity can help you understand your average spend per hour so that you make optimal purchases. If you're thinking about fine tuning your architecture or planning to start a new project, enabling hourly granularity can help your developers monitor the performance of your architecture at hourly level and identify optimization opportunities.

Once enabled, data at hourly granularity is available within 48 hours in Cost Explorer, and in Savings Plans utilization and coverage reports.

EC2-Instances (Elastic Compute Cloud) resource-level data at hourly granularity

In Cost Explorer, you can enable EC2 resource-level data at hourly granularity for the past 14 days. Using this data, you can view your hourly cost and usage at each EC2 instance level in Cost Explorer. This helps you to understand cost and usage driven by each EC2 instance by grouping on resource and filtering your Cost Explorer view for the EC2 service.

Such data can help you analyze for variances or anomalies. For example, if you see a spike in your EC2 cost, you can use hourly granularity to pinpoint the hour when the variance started, and then group your cost by resource to understand which specific EC2 instance is causing the spike. The ability to identify the source of variance to the exact hour can help your developers understand which specific changes in their architecture caused this variance, or if this is an actual anomaly or valid spike due to increased traffic. If you're thinking about how many EC2 Reserved Instances you should buy, understanding the number and type of instances running each hour can be useful, as you can make an informed decision to ensure you get the maximum Reserved Instances utilization. If you currently have Savings Plans or Reserved Instances, enable EC2 resource-level data at hourly granularity to understand which specific instances used your Savings Plans or Reserved Instances.

Once enabled, EC2 resource-level data at hourly granularity is available within 48 hours. This data is not available for Savings Plans and Reservations utilization and coverage reports.

Understanding your estimated monthly usage summary

When you enable granular data in Cost Explorer, it increases the number of usage records Cost Explorer needs to host for your organization. To ensure Cost Explorer can respond to queries as quickly as possible, Cost Explorer limits the amount of granular data stored for your organization.

> **Note**
>
> If you enable hourly granularity for both **EC2-Instances (Elastic Compute Cloud - Compute) resource-level data** and **Cost and usage data for all AWS services at hourly**

granularity (without resource-level data), you will see a drop in the hourly usage records reported against **Cost and usage**. This is because the EC2 hourly usage records are moved and reported under **EC2-Instances**.

In Cost Management preferences, you can view the estimated usage records count for your granular data preference selections and understand how close you are to the Cost Explorer data limits. See "Understanding Cost Explorer data threshold limits".

Hourly granularity in Cost Explorer is a paid feature and the cost depends on your hourly usage records count. Understanding your estimated usage records count for hourly granularity features can help you estimate the cost of these features before enabling them. See "Estimating cost for Cost Explorer hourly granularity".

Note

The usage records displayed in Cost Management preferences are for your entire organization and are estimates based on your average past usage. The actual usage records in any given past, current, or future month might differ from these values. If you're a new AWS customer and haven't used AWS for at least a month, we can't estimate your usage records due to insufficient data.

Topics

- Understanding Cost Explorer data threshold limits
- Estimating cost for Cost Explorer hourly granularity

Understanding Cost Explorer data threshold limits

Cost Explorer supports up to 500 million usage records for resource-level data at daily granularity and up to 500 million usage records for hourly granularity features (EC2 resource-level data at hourly granularity and hourly granularity for all services without resources).

To make sure Cost Explorer can deliver an optimal customer experience, if your estimated usage records is above these limits, you'll receive a data threshold error and you won't be able to save your preferences.

If you receive the data threshold error while setting resource-level data at daily granularity, you can reduce the number of services you want to enable resource-level data for. If the error still persists, consider retrieving your data using Cost and Usage Reports (CUR). You can set CUR to include resource IDs.

If you receive the data threshold error while setting hourly granularity, consider choosing between hourly cost and usage data for all services without resource-level data and EC2 resource-level data at hourly granularity. If the error still persists, consider retrieving your data using Cost and Usage Reports (CUR). You can set CUR to get cost and usage information at hourly granularity with resource IDs.

Estimating cost for Cost Explorer hourly granularity

Cost Explorer offers hourly granularity data at a daily charge of $0.00000033 per usage record, which translates to $0.01 per 1,000 usage records monthly. A usage record corresponds to a line item with a specific resource and usage type.

Cost Explorer bills you daily based on the total hourly usage records hosted in Cost Explorer for the past 14 days. For example, if you run one EC2 instance all day every day for the past month, and you have hourly granularity enabled, Cost Explorer will host 336 records per day (24 hours x 14 days) and charge you $0.0001 daily ($0.00000033 per record x 336 records), resulting in a monthly bill of $0.003 ($0.0001 daily cost x 30).

For the provided estimated usage records count, you can calculate the cost yourself using the provided formula, or you can use AWS Pricing Calculator.

Configuring multi-year and granular data

Using the management account, you can enable multi-year data and granular data in Cost Explorer. You do this in the Cost Management preferences in the console.

However, in order to enable multi-year and granular data, you first need to manage access to view and edit your Cost Management preferences. See Controlling access using IAM.

To set up multi-year and granular data

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home
2. In the navigation pane, choose **Cost Management preferences**.

3. To get historical data for up to 38 months, select **Multi-year data at monthly granularity**.

4. To enable resource-level or hourly granular data, consider the following options:

   > **Note**
   >
   > The hourly data as well as daily resource-level data is available for the past 14 days.

   - Hourly granularity
     - Select **Cost and usage data for all AWS services at hourly granularity** to get hourly data for all AWS services without resource-level data.
     - Select **EC2-Instances (Elastic Compute Cloud) resource-level data** to track EC2 cost and usage at instance level at hourly granularity.
   - Daily granularity
     - Select **Resource-level data at daily granularity** to get resource-level data for individual or all AWS services.
     - Choose services from the **AWS services at daily granularity** dropdown list that you want to enable resource-level data for.

       > **Note**
       >
       > The dropdown list contains only those services that were used in your organization in the last six months. They are ranked starting with the costliest.

5. Choose **Save preferences**.

> **Note**
>
> It can take up to 48 hours for changes to your data settings to reflect in Cost Explorer. Also, after saving your preferences, you won’t be able to make any additional changes for 48 hours.
> If the estimated data volume for your preferences is above the Cost Explorer limit, you'll receive an error stating that you have reached the data threshold limit and you won’t be able to save your preferences. See "Understanding Cost Explorer data threshold limits".

Controlling access using IAM

You can use AWS Identity and Access Management (IAM) to manage access to your Cost Management preferences for individual users. You can then grant or revoke access on an individual level for each IAM role or user. You'll need to add the following actions in order to be able to view and edit preferences: `ce:GetPreferences`, `ce:UpdatePreferences`, `ce:GetDimensionValues`, and `ce:GetApproximateUsageRecords`.

The following is a sample IAM policy with the relevant actions that would provide you with access to view and edit your Cost Management preferences in order to enable multi-year and granular data:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ce:GetPreferences",
                "ce:UpdatePreferences",
                "ce:GetDimensionValues",
                "ce:GetApproximateUsageRecords"
            ],
            "Resource": "*"
        }
    ]
}
```

Using the AWS Cost Explorer API

The Cost Explorer API allows you to programmatically query your cost and usage data. You can query for aggregated data such as total monthly costs or total daily usage. You can also query for granular data, such as the number of daily write operations for DynamoDB database tables in your production environment.

If you use a programming language that AWS provides an SDK for, we recommend that you use the SDK. All the AWS SDKs greatly simplify the process of signing requests and save you a significant amount of time when compared with using the AWS Cost Explorer API. In addition, the SDKs integrate easily with your development environment and provide easy access to related commands.

For more information about available SDKs, see Tools for Amazon Web Services. For more information about the AWS Cost Explorer API, see the AWS Billing and Cost Management API Reference.

Service endpoint

The Cost Explorer API provides the following endpoint:

https://ce.us-east-1.amazonaws.com

Granting IAM permissions to use the AWS Cost Explorer API

A user must be granted explicit permission to query the AWS Cost Explorer API. For the policy that grants the necessary permissions to a user, see View costs and usage.

Best practices for the AWS Cost Explorer API

The following are best practices when working with the Cost Explorer API.

Topics

- Best practices for configuring access to the Cost Explorer API
- Best practices for querying the Cost Explorer API
- Best practices for optimizing your Cost Explorer API costs

Best practices for configuring access to the Cost Explorer API

A user must be granted explicit permissions to query the Cost Explorer API. Granting a user access to the Cost Explorer API gives that user query access to any cost and usage data available to that account. For the policy that grants the necessary permissions to a user, see View costs and usage.

When configuring access to the Cost Explorer API, we recommend creating a unique role for the user. If you want to give multiple users query access to the Cost Explorer API, we recommend creating a role for each of them.

Best practices for querying the Cost Explorer API

When querying the Cost Explorer API, we recommend using filtering conditions to refine your queries so that you receive only the data that you need. You can do this by restricting the time range to a smaller interval or by using filters to limit the result set that your request returns. This enables your queries to return data more quickly than if you're accessing a larger set of data.

Adding one or more grouping dimensions to your query can increase the size of your result and can impact query performance. Depending on your use case, it can make sense to filter your data instead.

The Cost Explorer API can access up to 13 months of historical data and data for the current month. It can also provide 3 months of cost forecast data at the daily level of granularity and 12 months of cost forecast data at the monthly level of granularity.

Best practices for optimizing your Cost Explorer API costs

Because you're charged for the Cost Explorer API per paginated request, we recommend identifying the exact dataset to access before submitting queries.

AWS billing information is updated up to three times daily. Typical workloads and use cases for the Cost Explorer API anticipate a call pattern cadence ranging from daily to several times per day. To receive the most up-to-date data available, query for the time period that you're interested in.

If you're creating an application using the Cost Explorer API, we recommend architecting the application so that it has a caching layer. This enables you to regularly update the underlying data for your end users, but doesn't trigger queries every time that an individual in your organization accesses it.

Analyzing your Cost Explorer data with Amazon Q (preview)

> Amazon Q's cost analysis capability is in preview and can make mistakes. Please verify your cost data with AWS Cost Explorer. Use the thumb icon in Amazon Q to provide feedback and help us improve.

You can use Amazon Q, the generative AI assistant for AWS, to retrieve and analyze your cost data from AWS Cost Explorer. You can ask questions about your AWS costs and receive answers in natural language that reflect the actual costs of your AWS account. The following topics describe how to access and use the Amazon Q cost analysis capability.

For more information about Amazon Q, see What is Amazon Q Developer in the *Amazon Q Developer User Guide*.

Topics

- Overview of the Amazon Q cost analysis capability
- Security for the Amazon Q cost analysis capability

Overview of the Amazon Q cost analysis capability

> Amazon Q's cost analysis capability is in preview and can make mistakes. Please verify your cost data with AWS Cost Explorer. Use the thumb icon in Amazon Q to provide feedback and help us improve.

Amazon Q’s cost analysis capability is a feature of Amazon Q that works with Cost Explorer. With the cost analysis capability in Amazon Q, you can ask questions about your AWS costs and receive answers in natural language that reflect the actual historical costs of your AWS services. Amazon Q’s cost analysis capability uses generative AI and large language models (LLMs) to interpret your question and then requests the relevant cost data from Cost Explorer. Because LLMs are not well-suited to mathematical operations, Amazon Q instead uses traditional computing for all calculations on your cost data. With each response, Amazon Q provides transparency on the parameters that were used to retrieve your cost data, as well as a link to a matching visualization in the Cost Explorer console.

For example, if you ask Amazon Q a question such as *“What services did I spend the most on last month?”*, Amazon Q might return a response similar to the following:

The AWS services with the highest costs for your account last month were:

1. Amazon Relational Database Service: $2,595.55 (36.65% of total cost)
2. EC2 - Other: $1,222.71 (17.26% of total cost)
3. Amazon QuickSight: $1,006.32 (14.21% of total cost)
4. Amazon OpenSearch Service: $695.07 (9.81% of total cost)
5. Amazon ElastiCache: $482.11 (6.81% of total cost)
6. Amazon Elastic Load Balancing: $269.05 (3.80% of total cost)
7. AWS Supply Chain: $208.32 (2.94% of total cost)
8. Amazon Elastic Kubernetes Service: $148.80 (2.10% of total cost)
9. Amazon Virtual Private Cloud: $141.50 (2.00% of total cost)

10AWS Glue: $67.57 (0.95% of total cost)

The following Cost Explorer parameters were used to answer your question:

- Date range: *2024-03-01 through 2024-03-31 (inclusive)*
- Granularity: *"MONTHLY"*
- Group-by dimensions: *"Service"*
- Filter: *Excludes charge types “Refund”, “Credit”*
- Metric: *"UnblendedCosts"*

If the response isn’t immediately useful, you can ask follow-up questions to expand on the initial response. Amazon Q’s cost analysis capability looks at your entire conversation history to create follow-up responses.

Supported Cost Explorer features and dimensions

You can ask questions about the historical cost data that is available in Cost Explorer, using most common dimensions of cost data:

- Service (for example, Amazon Simple Storage Service)
- Charge type (for example, usage, tax, refund)
- Linked account
- AWS Region
- Instance type (for example, c7g.xlarge)
- Instance family (for example, compute-optimized)
- Purchase type (for example, on-demand, Savings Plans, spot)
- Platform (for example, Windows, Linux)
- Tenancy (shared or dedicated)
- Availability Zone

Amazon Q’s cost analysis capability cannot provide forecast information, responses with resource-level granularity (regarding specific EC2 instances, for example), costs by tag or cost category, or usage quantities. The following dimensions available in Cost Explorer are not available using the cost analysis capability in Amazon Q (preview):

- Usage type
- Billing entity
- Operation
- Database engine
- Operating system
- Savings Plan ARN
- Legal entity name
- Reservation ID
- Deployment option
- Cache engine
- Savings Plans type
- Invoicing entity

Examples of types of questions supported

- How much did I spend last month?
- Were any credits applied to our September bill?
- What were my cost trends by Region over the last three months?
- What were the top five highest-cost linked accounts in Q1?
- What instance type had the highest increase from February to March?
- What AWS service increased the most in February?
- Which Availability Zone had the highest costs last month?
- What were my costs by day last week?
- What was the cost of running c5.xlarge Linux instances last quarter?

Getting started

To use the cost analysis capability in Amazon Q, you must first opt in to Cost Explorer. To opt in to Cost Explorer, open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home. Once you've opted in to Cost Explorer, it can take up to 24 hours for your cost data to be available.

To start a conversation with Amazon Q

1. Log in to the AWS Management Console at https://console.aws.amazon.com.
2. Choose the Amazon Q icon on the right side of the console.

Pricing

There are no additional charges for using the cost analysis capability in Amazon Q. For information about Amazon Q Developer pricing, see Amazon Q Developer pricing.

Security for the Amazon Q cost analysis capability

> Amazon Q's cost analysis capability is in preview and can make mistakes. Please verify your cost data with AWS Cost Explorer. Use the thumb icon in Amazon Q to provide feedback and help us improve.

This page provides an overview of permissions and data protection for the Amazon Q cost analysis capability.

Permissions

All cost data provided by Amazon Q is sourced from Cost Explorer. The IAM user who accesses Amazon Q’s cost analysis capabilities must have permissions to use Amazon Q, and permissions to retrieve cost and usage data from Cost Explorer. The quickest way for an administrator to grant users access to Amazon Q is to use the `AmazonQFullAccess` managed policy. Users also need access to the `ce:GetCostAndUsage` permission.

The following IAM policy statement grants users access to the cost analysis capability in Amazon Q:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "EnablesCostAnalysisInAmazonQ",
   "Effect": "Allow",
   "Action": [
    "q:*",
    "ce:GetCostAndUsage"
   ],
   "Resource": "*"
  }
 ]
}
```

For users of AWS Organizations, management account administrators can restrict member account users' access to Cost Explorer data (including access to discounts, credits, and refunds) using the Cost Management preferences in the Billing and Cost Management console. These preferences apply to Amazon Q in the same way that they apply to the management console, SDK, and CLI. Amazon Q respects the existing preferences of customers.

Data protection

All of Amazon Q Developer's existing data protection policies also apply to cost data. AWS may use certain content from Amazon Q Developer for service improvement, including questions to Amazon Q and its responses, to provide better responses to common questions, fix Amazon Q operational issues, or for de-bugging. To learn more, see Amazon Q Developer service improvement in the *Amazon Q Developer User Guide*. For information on how to opt out of having your content used for service improvements, see AI services opt-out policies in the *AWS Organizations User Guide*.

Using Cost Explorer reports

Cost Explorer provides default reports, but also enables you to change the filters and constraints used to create the reports. Cost Explorer also provides you ways to save the reports that you made. You can save them as a bookmark, download the CSV file, or save them as a report.

Topics

- Using the default Cost Explorer reports
- Saving reports and results

Using the default Cost Explorer reports

Cost Explorer provides you with a couple of default reports. You can't modify these reports, but you can use them to create your own custom reports.

- Cost and usage reports
- Reserved Instance reports

Cost and usage reports

Cost Explorer provides you with the following reports for understanding your costs.

- AWS Marketplace
- Daily costs
- Monthly costs by linked account
- Monthly costs by service
- Monthly EC2 running hours costs and usage

AWS Marketplace

The **AWS Marketplace** report shows how much you have spent through AWS Marketplace.

Daily costs

The **Daily costs** report shows how much you've spent in the last six months, along with how much you're forecasted to spend over the next month.

Monthly costs by linked account

The **Monthly costs by linked account** report shows your costs for the last six months, grouped by linked, or member account. The top five member accounts are shown by themselves, and the rest are grouped into one bar.

Monthly costs by service

The **Monthly costs by service** report shows your costs for the last six months, grouped by service. The top five services are shown by themselves, and the rest are grouped into one bar.

Monthly EC2 running hours costs and usage

The **Monthly EC2 running hours costs and usage** report shows how much you have spent on active Reserved Instances (RIs).

Reserved Instance reports

Cost Explorer provides you with the following reports for understanding your reservations.

The reservation reports show your Amazon EC2 coverage and utilization in either hours or normalized units. Normalized units enable you to see your Amazon EC2 usage for multiple sizes of instances in a uniform way. For example, suppose you run an `xlarge` instance and a `2xlarge` instance. If you run both instances for the same amount of time, the `2xlarge` instance uses twice as much of your reservation as the `xlarge` instance, even though both instances show only one instance-hour. Using normalized units instead of instance-hours, the `xlarge` instance used 8 normalized units, and the `2xlarge` instance used 16 normalized units. For more information, see Instance Size Flexibility for EC2 Reserved Instances.

- RI utilization reports
- RI coverage reports

RI utilization reports

The RI Utilization reports show how much of your Amazon EC2, Amazon Redshift, Amazon RDS, Amazon OpenSearch Service, and Amazon ElastiCache Reserved Instance (RIs) that you use, how much you saved by using RIs, how much you overspent on RIs, and your net savings from purchasing RIs during the selected time range. This helps you to see if you have purchased too many RIs.

The RI Utilization charts display the number of RI hours that your account uses, helping you to understand and monitor your combined usage (utilization) across all of your RIs and services. It also shows how much you saved over On-Demand Instance costs by purchasing a reservation, the amortized costs of your unused reservations, and your total net savings from purchasing reservations. AWS calculates your total net savings by subtracting the costs of your unused reservations from your reservations savings.

The following table shows an example of potential savings (all costs are in USD).

RI utilization example

Account	RI utilization	RI hours purchase	RI hours used	RI hours unused	On-Demand cost of RI hours used	Effective RI cost	Net savings	Total potential savings
Martha	0.50	100	50	50	$200	$150	$50	$250
Liu Jie	0.75	100	75	25	$300	$150	$150	$250
Saanvi	1.00	50	50	0	$200	$75	$125	$125

As shown in the preceding table, Martha, Liu Jie, and Saanvi purchase RIs at $1.50 an hour and On-Demand hours at $4.00 an hour. Breaking down this example further, you can see how much each of them saves by purchasing RIs:

- Martha purchases 100 RI hours for $150. She uses 50 hours, which would cost $200 if she used On-Demand Instances. She saves $50, which is the cost of 50 On-Demand hours minus the cost of the RI. She could optimize her savings by using more of her purchased RI hours, by converting her RI to cover other instances, or by selling her RIs on the RI Marketplace. For more information about selling an RI on the RI Marketplace, see Selling on the Reserved Instance Marketplace in the Amazon EC2 User Guide.

- Liu Jie purchases 100 RI hours for $150. He uses 75 of them, which would cost $300 if he used On-Demand Instances. So he saves $150, which is the cost of 300 On-Demand hours minus the cost of the RI.
- Saanvi purchases 50 RI hours for $75. She uses all 50 of them, which would cost $200 if she used On-Demand Instances. So she saves $125, which is the cost of 200 On-Demand hours minus the cost of the RI.

The reports allow you to define a utilization threshold, known as a *utilization target*, and identify RIs that meet your utilization target and RIs that are underutilized. The chart shows RI utilization as the percentage of purchased RI hours that are used by matching instances, rounded to the nearest percentage.

Target utilization is shown on the chart as a dotted line in the chart and in the table below the chart as a colored RI utilization status bar. RIs with a red status bar are RIs with no hours used. RIs with a yellow status bar are under your utilization target. RIs with a green status bar have met your utilization target. Instances with a gray bar aren't using reservations. You can change the utilization target in the **Display Options** section. To remove the utilization target line from the chart, clear the **Show target line on chart** check box. You can also create budgets that enable AWS to notify you if you fall below your utilization targets. For more information, see Managing your costs with AWS Budgets.

You can filter the chart to analyze the purchasing accounts, instance types, and more. RI reports use a combination of RI-specific filters and regular Cost Explorer filters. The RI-specific filters are available only for the Cost Explorer RI Utilization and RI Coverage reports. They aren't available anywhere else that AWS uses Cost Explorer filters. The following filters are available:

- **Availability Zone –** Filter your RI usage by specific Availability Zones.
- **Instance Type –** Filter your RI usage by specific instance types, such as **t2.micro** or **m3.medium**. This also applies to Amazon RDS instance classes, such as **db.m4**, and Amazon Redshift and ElastiCache node types, such as **dc2.large**.
- **Linked Account –** Filter your reservations by specific member accounts.
- **Platform –** Filter your RI usage by platform, such as **Linux** or **Windows**. This also applies to Amazon RDS database engines.
- **Region –** Filter your RI usage by specific regions, such as **US East (N. Virginia)** or **Asia Pacific (Singapore)**.

- **Scope** (Amazon EC2) – Filter your Amazon EC2 usage to show RIs that are purchased for use in specific Availability Zones or regions.
- **Tenancy** (Amazon EC2) – Filter your Amazon EC2 usage by tenancy, such as **Dedicated** or **Default**. An RI with a **Dedicated** tenancy is reserved for a single tenant, and an RI with a **Default** tenancy might share hardware with another RI.

In addition to changing your utilization target and filtering your RIs, you can choose a single RI or a group of RIs to show in the chart. To choose a single RI or a selection of RIs to see in the chart, select the check box next to the RI in the table below the chart. You can select up to 10 leases at one time.

Cost Explorer shows the combined utilization across all of your RIs in the chart and shows utilization for individual RI reservations in the table below the chart. The table also includes a subset of the information for each RI reservation. You can find the following information for each reservation in the downloadable .csv file:

- **Account Name –** The name of the account that owns the RI reservation.
- **Subscription ID –** The unique subscription ID for the RI reservation.
- **Reservation ID –** The unique ID for the RI reservation.
- **Instance Type –** The RI instance class, instance type, or node type, such as **t2.micro**, **db.m4**, or **dc2.large**.
- **RI Utilization –** The percentage of purchased RI hours that were used by matching instances.
- **RI Hours Purchased –** The number of purchased hours for the RI reservation.
- **RI Hours Used –** The number of purchased hours that were used by matching instances.
- **RI Hours Unused –** The number of purchased hours that weren't used by matching instances.
- **Account ID –** The unique ID of the account that owns the RI reservation.
- **Start Date –** The date that the RI starts.
- **End Date –** The date that the RI expires.
- **Numbers of RIs –** The numbers of RIs that are associated with the reservation.
- **Scope –** Whether this RI is for a specific Availability Zone or region.
- **Region –** The region that the RI is available in.
- **Availability Zone –** The Availability Zone that the RI is available in.
- **Platform** (Amazon EC2) – The platform that this RI is for.

- **Tenancy** (Amazon EC2) – Whether this RI is for a shared or dedicated instance.
- **Payment Option –** Whether this RI is a Full Upfront, Partial Upfront, or No Upfront RI.
- **Offering Type –** Whether this RI is Convertible or Standard.
- **On-Demand Cost Equivalent –** The cost of the RI hours that you used, based on the public On-Demand prices.
- **Amortized Upfront Fee –** The upfront cost of this reservation, amortized over the RI period.
- **Amortized Recurring Charges –** The monthly cost of this reservation, amortized over the RI period.
- **Effective RI Cost –** The combined amortized upfront and amortized recurring costs of the RI hours that you purchased.
- **Net Savings –** The amount that Cost Explorer estimates that you saved by purchasing reservations.
- **Potential Savings –** The total potential savings that you might see if you use your entire RI.
- **Average On-Demand Rate –** The On-Demand rate of the RI hours that you used. When you view the On-Demand rates for an extended period of time, the On-Demand rate reflects any price changes made during that time period.

  If there isn't any usage for the given time period, the average On-Demand rate shows **N/A**.
- **Total Asset Value –** The effective cost of your reservation term. The total asset value takes both your start date and either your end date or your cancellation date into consideration.
- **Effective Hourly Rate –** The effective hourly rate of your total RI costs. The hourly rate takes both your upfront fees and your recurring fees into consideration.
- **Upfront Fee –** The one-time upfront cost of the RI hours that you purchased.
- **Hourly Recurring Fee –** The effective hourly rate of your monthly RI costs. The hourly recurring fee takes only your recurring fees into consideration.
- **RI Cost For Unused Hours –** The amount that you spent on RI hours that you didn't use.

You can use this information to track how many RI usage hours you used and how many RI hours you reserved but didn't use during the selected time range.

The Daily RI Utilization chart displays your RI utilization for the previous three months on a daily basis. The Monthly RI Utilization chart displays your RI utilization for the previous 12 months on a monthly basis.

RI coverage reports

The RI Coverage reports show how many of your Amazon EC2, Amazon Redshift, Amazon RDS, Amazon OpenSearch Service, and Amazon ElastiCache instance hours are covered by RIs, how much you spent on On-Demand Instances, and how much you might have saved had you purchased more reservations. This enables you to see if you have under-purchased RIs.

The RI coverage charts display the percentage of instance hours that your account used that were covered by reservations, helping you to understand and monitor the combined coverage across all of your RIs. It also shows how much you spent on On-Demand Instances and how much you might have saved had you purchased more reservations.

You can define a threshold for how much coverage you want from RIs, known as a *coverage target*, which enables you to see where you can reserve more RIs.

Target coverage is shown on the chart as a dotted line, and the average coverage is shown in the table below the chart as a colored status bar. Instances with a red status bar are instances with no RI coverage. Instances with a yellow status bar are under your coverage target. Instances with a green status bar have met your coverage target. Instances with a gray bar aren't using reservations. You can change the coverage target in the **Display Options** section. To remove the coverage target line from the chart, clear the **Show target line on chart** check box. You can also create coverage budgets that enable AWS to notify you if you fall below your coverage target. For more information, see Managing your costs with AWS Budgets.

The RI coverage reports use the Cost Explorer filters instead of the RI Utilization filters. You can filter the chart to analyze the purchasing accounts, instance types, and more. RI reports use a combination of RI-specific filters and regular Cost Explorer filters. The RI-specific filters are available only for the Cost Explorer RI Utilization and RI Coverage reports, and aren't available anywhere else that AWS uses Cost Explorer filters. The following filters are available:

- **Availability Zone –** Filter your RI usage by specific Availability Zones.
- **Instance Type –** Filter your RI usage by specific instance types, such as **t2.micro** or **m3.medium**. This also applies to Amazon RDS instance classes such as **db.m4**.
- **Linked Account –** Filter your RI usage by specific member accounts.
- **Platform –** Filter your RI usage by platform, such as **Linux** or **Windows**. This also applies to Amazon RDS database engines.
- **Region –** Filter your RI usage by specific regions, such as **US East (N. Virginia)** or **Asia Pacific (Singapore)**.

- **Scope** (Amazon EC2) – Filter your Amazon EC2 usage to show RIs that are purchased for use in specific Availability Zones or regions.
- **Tenancy** (Amazon EC2) – Filter your Amazon EC2 usage by tenancy, such as **Dedicated** or **Default**. A **Dedicated** RI is reserved for a single tenant, and a **Default** RI might share hardware with another RI.

In addition to changing your coverage target and filtering your instance types with the available filters, you can choose a single instance type or a group of instance types to show in the chart. To choose a single instance type or a selection of instance types to see in the chart, select the check box next to the instance type in the table below the chart. You can select up to 10 instances at one time.

Cost Explorer shows the combined coverage across all of your instance types in the chart and shows coverage for individual instance types in the table below the chart. The table also includes a subset of the information for each instance type. You can find the following information for each instance type in the downloadable .csv file:

- **Instance Type** (Amazon EC2), **Instance Class** (Amazon RDS), or **Node Type** (Amazon Redshift or Amazon ElastiCache) – The RI instance class, instance type, or node type, such as **t2.micro**, **db.m4**, or **dc2.large**.
- **Database Engine** (Amazon RDS) – Filter your Amazon RDS coverage to show RIs that cover a specific database engine, such as **Amazon Aurora**, **MySQL**, or **Oracle**.
- **Deployment Option** (Amazon RDS) – Filter your Amazon RDS coverage to show RIs that cover a specific deployment option, such as **Multi-AZ** deployments.
- **Region** – The region that the instance ran in, such as **us-east-1**.
- **Platform** (Amazon EC2) – The platform that this RI is for.
- **Tenancy** (Amazon EC2) – Whether this RI is for a shared, dedicated, or host instance.
- **Average Coverage** – The average number of usage hours that a reservation covers.
- **RI Covered Hours** – The number of usage hours that a reservation covers.
- **On-Demand Hours** – The number of usage hours that aren't covered by reservations.
- **On-Demand Cost** – The amount that you spent on On-Demand Instances.
- **Total Running Hours** – The total number of usage hours, both covered and uncovered.

You can use this information to track how many hours you use and how many of those hours are covered by RIs.

The daily chart displays the number of RI hours that your account used on a daily basis for the last three months. The monthly chart displays your RI coverage for the previous 12 months, listed by month.

Saving reports and results

You can save your Cost Explorer filters and data multiple ways. You can save the exact configuration as a bookmark, you can download the CSV file of the data that Cost Explorer used to create your graphs, or you can save the Cost Explorer configuration as a saved report. Cost Explorer keeps your saved reports and lists them on your report page along with the default Cost Explorer reports.

Topics

- Saving your Cost Explorer configuration with bookmarks or favorites
- Downloading the cost data CSV file
- Managing your saved Cost Explorer reports

Saving your Cost Explorer configuration with bookmarks or favorites

You can save your date, filter, chart style, group by, and advanced settings by saving the Cost Explorer URLs as favorites or bookmarks in your browser. When you return to the link that you saved, Cost Explorer refreshes the page using current cost data for time range you selected and displays the most recent forecast. This feature enables you to save a configuration that you're likely to refresh and return to often. You can also save a configuration for a specific, unchanging range of time by using the **Custom** time range and setting fixed start and end dates for your chart.

> ⚠ **Warning**
>
> If you want to save a number of configurations, make sure to give each bookmark or favorite a unique name so that you don't overwrite older configurations when you save a new URL.

Downloading the cost data CSV file

When you want to review comprehensive detail, you can download a comma-separated values (CSV) file of the cost data that Cost Explorer uses to generate the chart. This is the same data that appears in the data table under the chart. The data table sometimes doesn't display the complete dataset that is used for the chart. For more information, see Reading the Cost Explorer data table.

To download a CSV file

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. Configure Cost Explorer to use the options that you want to see in the CSV file.
3. Choose **Download CSV**.

Note the following about the format of the CSV download:

- If you view the CSV file in a table format, the file’s columns represent costs and the rows represent time. When compared to the Cost Explorer data table in the console, the columns and rows are transposed.
- The file shows data with up to 15 decimal places of precision.
- The file shows dates in the YYYY-MM-DD format.

Managing your saved Cost Explorer reports

You can save the results of a Cost Explorer query as a Cost Explorer report. This enables you to track your Cost Explorer results and forecasts over time.

Topics

- Creating a Cost Explorer report
- Viewing a Cost Explorer report
- Editing a Cost Explorer report
- Deleting a Cost Explorer report

Creating a Cost Explorer report

You can use the console to save the results of a Cost Explorer query as a report.

Note

Cost Explorer reports can be modified. We strongly recommend that you don't use them for auditing purposes.

To save a Cost Explorer report

1. Open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Cost Explorer Saved Reports**.
3. Choose **Create new report**. This resets all of your Cost Explorer settings to your default settings.
4. Select a report type.
5. Choose **Create report**.
6. Customize your Cost Explorer settings.
7. Choose **Save to report library**.
8. In the **Save to report library** dialog box, enter a name for your report, and then choose **Save report**.

Viewing a Cost Explorer report

You can use the console to view saved Cost Explorer reports.

To view your saved reports

1. Open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Cost Explorer Saved Reports**.

Editing a Cost Explorer report

You can use the console to edit Cost Explorer reports.

To edit a report

1. Open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Cost Explorer Saved Reports**.
3. Choose the report that you want to edit.

   > **Note**
   >
   > You can't edit the predefined reports. If you choose one of the predefined reports as a starting point for a report, enter a new report name in the report name field and continue with this procedure.

4. Customize your Cost Explorer settings.
5. Choose **Save** to overwrite the existing report, or else choose **Save as a new report**.
6. In the **Save to report library** dialog box, enter a name for your report, and then choose **Save report**.

Deleting a Cost Explorer report

You can use the console to delete saved Cost Explorer reports.

To delete a saved report

1. Open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Cost Explorer Saved Reports**.
3. Select the check box next to the report you want to delete.

   > **Note**
   >
   > The **Reports** page contains predefined reports that cannot be deleted. These default reports are identified by a lock icon. You can, however, delete custom reports.

4. Choose **Delete**.
5. In the **Delete reports** dialog box, choose **Delete**.

Managing your costs with AWS Budgets

You can use AWS Budgets to track and take action on your AWS costs and usage. You can use AWS Budgets to monitor your aggregate utilization and coverage metrics for your Reserved Instances (RIs) or Savings Plans. If you're new to AWS Budgets, see Best practices for AWS Budgets.

You can use AWS Budgets to enable simple-to-complex cost and usage tracking. Some examples include:

- Setting a monthly cost budget with a fixed target amount to track all costs associated with your account. You can choose to be alerted for both actual (after accruing) and forecasted (before accruing) spends.
- Setting a monthly cost budget with a variable target amount, with each subsequent month growing the budget target by 5 percent. Then, you can configure your notifications for 80 percent of your budgeted amount and apply an action. For example, you could automatically apply a custom IAM policy that denies you the ability to provision additional resources within an account.
- Setting a monthly usage budget with a fixed usage amount and forecasted notifications to help ensure that you are staying within the service limits for a specific service. You can also be sure you are staying under a specific AWS Free Tier offering.
- Setting a daily utilization or coverage budget to track your RI or Savings Plans. You can choose to be notified through email and Amazon SNS topics when your utilization drops below 80 percent for a given day.

AWS Budgets information is updated up to three times a day. Updates typically occur 8–12 hours after the previous update. Budgets can track your unblended, amortized, and blended costs. Budgets can include or exclude charges such as discounts, refunds, support fees, and taxes.

You can create the following types of budgets:

- **Cost budgets** – Plan how much you want to spend on a service.
- **Usage budgets** – Plan how much you want to use one or more services.
- **RI utilization budgets** – Define a utilization threshold and receive alerts when your RI usage falls below that threshold. This lets you see if your RIs are unused or under-utilized.

- **RI coverage budgets –** Define a coverage threshold and receive alerts when the number of your instance hours that are covered by RIs fall below that threshold. This lets you see how much of your instance usage is covered by a reservation.
- **Savings Plans utilization budgets –** Define a utilization threshold and receive alerts when the usage of your Savings Plans falls below that threshold. This lets you see if your Savings Plans are unused or under-utilized.
- **Savings Plans coverage budgets –** Define a coverage threshold and receive alerts when your Savings Plans eligible usage that is covered by Savings Plans fall below that threshold. This lets you see how much of your instance usage is covered by Savings Plans.

You can set up optional notifications that warn you if you exceed, or are forecasted to exceed, your budgeted amount for cost or usage budgets. Or if you fall below your target utilization and coverage for RI or Savings Plans budgets. You can have notifications sent to an Amazon SNS topic, to an email address, or to both. For more information, see Creating an Amazon SNS topic for budget notifications.

If you use consolidated billing in an organization and you own the management account, you can use IAM policies to control access to budgets by member accounts. By default, owners of member accounts can create their own budgets but can't create or edit budgets for other users. You can create roles with permissions that allow users to create, edit, delete, or read budgets in a specific account. However, we don't support cross-account usage.

A budget is only visible to users with access to the account that created the budget, and with access to the budget itself. For example, a management account can create a budget that tracks a specific member account's cost, but the member account can only view the same budget if they receive access to the management account. For more information, see Overview of managing access permissions. For more information about AWS Organizations, see the AWS Organizations User Guide.

> **Note**
>
> There can be a delay between when you incur a charge and when you receive a notification from AWS Budgets for the charge. This is due to a delay between when an AWS resource is used and when that resource usage is billed. You might incur additional costs or usage that exceed your budget notification threshold before AWS Budgets can notify you.

Topics

- Best practices for AWS Budgets
- Creating a budget
- Viewing your budgets
- Editing a budget
- Downloading a budget
- Copying a budget
- Deleting a budget
- Configuring AWS Budgets actions
- Creating an Amazon SNS topic for budget notifications
- Receiving budget alerts in Amazon Chime and Slack

Best practices for AWS Budgets

Note the following best practices when you're working with budgets.

Topics

- Best practices for controlling access to AWS Budgets
- Best practices for budget actions
- Best practices for setting budgets
- Best practices for using the advanced options when setting cost budgets
- Understanding the AWS Budgets update frequency
- Best practices for setting budget alerts
- Best practices for setting budget alerts using Amazon SNS topics
- Best practices for tagging budgets

Best practices for controlling access to AWS Budgets

To allow users to create budgets in the AWS Billing and Cost Management console, you must also allow users to do the following:

- View your billing information

- Create Amazon CloudWatch alarms
- Create Amazon Simple Notification Service (Amazon SNS) notifications

To learn more about giving users the ability to create budgets on the AWS Budgets console, see Allow users to create budgets.

You can also create budgets programmatically using the Budgets API. When configuring access to the Budgets API, we recommend creating a unique user role for making programmatic requests. This helps you define more precise access controls between who in your organization has access to the AWS Budgets console and the API. To give multiple users query access to the Budgets API, we recommend creating a role for each of them.

Best practices for budget actions

Using managed policies

There are two AWS managed policies to help get you started with budget actions. One for the user, and the other for budgets. These policies are related. The first policy ensures a user can pass a role to the budgets service, and the second allows budgets to execute the action.

If you don't have proper permissions configured and assigned for the user and for AWS Budgets, AWS Budgets can't execute your configured actions. To ensure proper configuration and execution, we've configured these managed policies so your AWS Budgets actions work as intended. We recommend you use these IAM policies to be sure you don't have to update your existing IAM policy for AWS Budgets when a new functionality is included. We will add new capabilities to the managed policy by default.

For details about managed policies, see Managed policies.

To learn more about AWS Budgets actions, see the Configuring AWS Budgets actions section.

Using Amazon EC2 Auto Scaling

If a budget action is used to stop an Amazon EC2 instance in an Auto Scaling Group (ASG), Amazon EC2 Auto Scaling restarts the instance, or launches new instances to replace the stopped instance. Therefore, "shutdown budget actions is not effective to Amazon EC2/Amazon RDS budget actions" aren't effective unless you combine a second budget action that removes permissions on the role used by the Launch Configuration managing the ASG.

Best practices for setting budgets

Use AWS Budgets to set custom budgets based on your costs, usage, reservation utilization, and reservation coverage.

With AWS Budgets, you can set budgets on a recurring basis or for a specific time frame. However, we recommend setting your budget on a recurring basis so that you don't unexpectedly stop receiving budget alerts.

Best practices for using the advanced options when setting cost budgets

Cost budgets can be aggregated by unblended costs, amortized costs, or blended costs. Cost budgets can also either include or exclude refunds, credits, upfront reservation fees, recurring reservation charges, non-reservation subscription costs, taxes, and support charges.

Understanding the AWS Budgets update frequency

AWS billing data, which Budgets uses to monitor resources, is updated at least once per day. Keep in mind that budget information and associated alerts are updated and sent according to this data refresh cadence.

Best practices for setting budget alerts

Budget alerts can be sent to up to 10 email addresses and one Amazon SNS topic per alert. You can set budgets to alert against either actual values or forecasted values.

Actual alerts are only sent out once per budget, per budget period, when a budget first reached the actual alert threshold.

Forecast-based budget alerts are sent out on a per-budget, per-budget period basis. They might alert more than once in a budgeted period if the forecasted values exceed, dip below, and then exceed the alert threshold again during the budgeted period.

AWS requires approximately 5 weeks of usage data to generate budget forecasts. If you set a budget to alert based on a forecasted amount, this budget alert isn't triggered until you have enough historical usage information.

The following video highlights the importance of setting up budget alerts, which give you control over your spending. It also touches on the use of multi-factor authentication (MFA) to increase the security of your account.

How to set up AWS multi-factor authentication (MFA) and AWS Budgets alerts

Best practices for setting budget alerts using Amazon SNS topics

When you create a budget that sends notifications to an Amazon SNS topic, you must either have a preexisting Amazon SNS topic or create an Amazon SNS topic. Amazon SNS topics enable you to send notifications over SMS in addition to email.

For budget notifications to be sent successfully, your budget must have permissions to send a notification to your topic, and you must accept the subscription to the Amazon SNS notification topic. For more information, see Creating an Amazon SNS topic for budget notifications.

Best practices for tagging budgets

You can use tags to control access to your AWS Budgets resources. You can also use resource-level permissions to allow or deny access to one or more AWS Budgets resources in an AWS Identity and Access Management (IAM) policy. This allows for easy budget management and auditing, improving governance and information security. You can specify the users, roles, and actions that are permitted on the AWS Budgets resources.

To add tags to budgets, use AWS Budgets in the Billing and Cost Management console or programmatically using the Budgets API.

You can add tags when creating an AWS Budgets resource, or later using the console or the `TagResource` operation.

You can view the tags on an AWS Budgets resource using the console or by calling the `ListTagsForResource` operation.

You can remove tags from an AWS Budgets resource using the console or by calling the `UntagResource` operation.

Note

AWS Budgets does not support tags for cost allocation. This means you will not see tag information in cost and usage data—in Data Exports, Cost and Usage Reports, or Cost Explorer, for example.

Creating a budget

You can create budgets to track and take action on your costs and usage. You can also create budgets to track your aggregate Reserved Instance (RI) and Savings Plans utilization and coverage. By default, single accounts, the management account, and member accounts in an organization can create budgets.

When you create a budget, AWS Budgets provides a Cost Explorer graph to help you see your incurred costs and usage. If you didn't enable Cost Explorer yet, this graph is blank and AWS Budgets will enable Cost Explorer when you create your first budget. You can create your budget without enabling Cost Explorer. It can take up to 24 hours for this graph to appear after you or AWS Budgets enable Cost Explorer.

You can create and set up a budget in two ways:

- Using a budget template (simplified)
- Customizing a budget (advanced)

You can also use our walk-through tutorials to learn how to achieve your objectives with AWS Budgets.

To access tutorials

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Budgets**.
3. Next to **Overview**, choose **Info**.
4. In the help panel, choose **Tutorials**.

Using a budget template (simplified)

You can create a budget using a template with recommended configurations. Budget templates are a simplified way to start using AWS Budgets, with a single page workflow, unlike the 5-step workflow that is required for Customizing a budget (advanced).

To create a budget using a template

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.
4. Under **Budget setup**, choose **Use a template (simplified)**.
5. Under **Templates**, choose a template that best matches your use case:
    - **Zero spend budget**: A budget that notifies you after your spending exceeds AWS Free Tier limits.
    - **Monthly cost budget**: A monthly budget that notifies you if you exceed, or are forecasted to exceed, the budget amount.
    - **Daily Savings Plans coverage budget**: A coverage budget for your Savings Plans that notifies you when you fall below the defined target. This helps you to identify your on-demand spend sooner so that you can consider purchasing a new commitment.
    - **Daily reservation utilization budget**: A utilization budget for your Reserved Instances that notifies you when you fall below the defined target. This helps you to identify when you're not using some of your hourly commitment that you already purchased.
6. Update the details and settings for your specific template.
7. Choose **Create budget**.

While each template has default configurations, they can be changed later. This way, you can use it to create most of the budget, and then edit certain settings in the advanced workflow, such as adding a linked account or a cost category filter. To change any of the settings, under **Template settings**, choose **Custom**.

You can also download a template for offline use in AWS CLI or CloudFormation, for example. To download a template, under **Template settings**, choose **JSON**.

Customizing a budget (advanced)

You can customize a budget to set parameters specific to your use case. You can customize the time period, the start month, and specific accounts. Creating a customized budget involves a 5-step workflow.

You can choose between four main budget types that track against the following:

- Cost (see Creating a cost budget)
- Usage (see Creating a usage budget)
- Savings Plans (see Creating a Savings Plans budget)
  - Savings Plans utilization
  - Savings Plans coverage
- Reservation (see Creating a reservation budget)
  - Reservation utilization
  - Reservation coverage

Creating a cost budget

Use this procedure to create a budget that's based on your costs.

To create a cost budget

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.
4. Under **Budget setup**, choose **Customize (advanced)**.
5. Under **Budget types**, choose **Cost budget**. Then, choose **Next**.
6. Under **Details**, for **Budget name**, enter the name of your budget. Your budget name must be unique within your account. It can contain A-Z, a-z, spaces, and the following characters:

   ```
   _.:/=+-%@
   ```

7. Under **Set budget amount**, for **Period**, choose how often you want the budget to reset the actual and forecasted spend. Select **Daily** for every day, **Monthly** for every month, **Quarterly** for every three months, or **Annually** for every year.

   > **Note**
   >
   > With a **Monthly** or **Quarterly** budget period, you can set future budgeted amounts using the budget planning feature.

8. For **Budget renewal type**, choose **Recurring budget** for a budget that resets after the budget period. Or, choose **Expiring budget** for a one-time budget that doesn't reset after the budget period.

9. Choose the start date or period to begin tracking against your budgeted amount. For an **Expiring budget**, choose the end date or period for the budget to end on.

   All budget times are in the UTC format.

10. For **Budgeting method**, select the way that you want your budget amount to be determined each budget period:

    - **Fixed**: Set one amount to monitor every budget period.
    - **Planned**: Set different amounts to monitor each budget period.
    - **Auto-adjusting**: Set your budget amount to be adjusted automatically based on your spending pattern over a time range that you specify.

    For more information about each method, see the section called “Budget methods”

11. (Optional) Under **Budget scope**, for **Filters**, choose **Add filter** to apply one or more of the available filters. Your choice of budget type determines the set of filters that's displayed on the console.

    > **Note**
    >
    > You can't use the **Linked account** filter within a linked account.

12. (Optional) **Under Budget scope**, for **Advanced options**, choose one or more of the following filters. If you're signed in from a member account in an organization, you might not see all of the advanced options. To see all of the advanced options, sign in from a management account.

Refunds

Any refunds that you received.

Credits

Any AWS credits that are applied to your account.

Upfront reservation fees

Any upfront fees that are charged to your account. When you purchase an All Upfront or Partial Upfront Reserved Instance from AWS, you pay an upfront fee in exchange for a lower rate for using the instance.

Recurring reservation charges

Any recurring charges to your account. When you purchase a Partial Upfront or No Upfront Reserved Instance from AWS, you pay a recurring charge in exchange for a lower rate for using the instance.

Taxes

Any taxes that are associated with the charges or fees in your budget.

Support charges

Any charges that AWS charges you for a support plan. When you purchase a support plan from AWS, you pay a monthly charge in exchange for service support.

Other subscription costs

Other applicable subscription costs that aren't covered by the other data categories. These costs can include data such as AWS training fees, AWS competency fees, out-of-cycle charges such as registering a domain with Route 53.

Use blended costs

The cost of the instance hours that you used. A blended rate doesn't include either the RI upfront costs or the RI discounted hourly rate.

Use amortized costs

The amortized cost of any reservation hours that you used. For more information about amortized costs, see Choosing advanced options.

Discounts

Any enterprise discount such as RI volume discounts. Discount line items don't contain tags.

13. Choose **Next**.
14. Choose **Add an alert threshold**.
15. Under **Set alert threshold**, for **Threshold**, enter the amount that must be reached for you to be notified. This can be either an absolute value or a percentage. For example, say you have a budget of 200 dollars. To be notified at 160 dollars (80% of your budget), enter **`160`** for an absolute budget or **`80`** for a percentage budget.

    Next to the amount, choose **Absolute value** to be notified when your costs exceed the threshold amount. Or, choose **% of budgeted amount** to be notified when your costs exceed the threshold percentage.

    Next to the threshold, choose **Actual** to create an alert for actual spend. Or, choose **Forecasted** to create an alert for forecasted spend.
16. (Optional) Under **Notification preferences**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can be sent to a maximum of 10 email addresses.
17. (Optional) Under **Notification preferences**, for **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

    > ⚠ **Important**
    >
    > After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.
18. (Optional) Under **Notification preferences**, for **AWS Chatbot Alerts**, you can choose to configure AWS Chatbot to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts on the AWS Chatbot console.
19. Choose **Next**.

20. (Optional) For **Attach actions**, you can configure an action that AWS Budgets performs on your behalf when the alert threshold is exceeded. For more information and instructions, see To configure a budget action.

21. Choose **Next**.

> **Note**
>
> To proceed, you must configure at least one of the following parameters for each alert:
>
> - An email recipient for notifications
> - An Amazon SNS topic for notifications
> - A budget action

22. Review your budget settings, and then choose **Create budget**.

Creating a usage budget

Use this procedure to create a budget that's based on your usage.

To create a usage budget

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.

2. In the navigation pane, choose **Budgets**.

3. At the top of the page, choose **Create budget**.

4. Under **Budget setup**, choose **Customize (advanced)**.

5. Under **Budget types**, choose **Usage budget**. Then, choose **Next**.

6. Under **Details**, for **Budget name**, enter the name of your budget. Your budget name must be unique within your account. It can contain A-Z, a-z, spaces, and the following characters:

   ```
   _.:/=+-%@
   ```

7. Under **Choose what you're budgeting against**, for **Budget against**, choose **Usage type groups** or **Usage types**. A usage type group is a collection of usage types that have the same unit of measure. For example, resources that measure usage by the hour is one usage type group.

- For **Usage type groups**, choose the unit of measurement and the applicable service usage that you want the budget to monitor.
- For **Usage types**, choose the specific service usage measurements that you want the budget to monitor.

8. Under **Set budget amount**, for **Period**, choose how often you want the budget to reset the actual and forecasted usage. Select **Daily** for every day, **Monthly** for every month, **Quarterly** for every three months, or **Annually** for every year.

   > **Note**
   >
   > With a **Monthly** or **Quarterly** budget period, you can set future budgeted amounts using the budget planning feature.

9. For **Budget renewal type**, choose **Recurring budget** for a budget that resets at the end of each budget period. Or, choose **Expiring budget** for a one-time budget that doesn't reset after the given budget period.
10. Choose the start date or period to begin tracking against your budgeted amount. For an **Expiring budget**, choose the end date or period for the budget to end on.

    All budget times are in the UTC format.
11. For **Budgeting method**, select the way that you want your budget amount to be determined each budget period:

    - **Fixed**: Set one amount to monitor every budget period.
    - **Planned**: Set different amounts to monitor each budget period.
    - **Auto-adjusting**: Set your budget amount to be adjusted automatically based on your usage pattern over a time range that you specify.

    For more information about each method, see the section called “Budget methods”
12. (Optional) Under **Budget scope**, for **Filters**, choose **Add filter** to apply one or more of the available filters. Your choice of budget type determines the set of filters that's displayed on the console.

> **Note**
>
> You can't use the **Linked account** filter within a linked account.

13. Choose **Next**.
14. Choose **Add an alert threshold**.
15. Under **Set alert threshold**, for **Threshold**, enter the amount that must be reached for you to be notified. This can be either an absolute value or a percentage. For example, say you have a budget of 200 hours. To be notified at 160 hours (80% of your budget), enter **`160`** for an absolute budget or **`80`** for a percentage budget.

    Next to the amount, choose **Absolute value** to be notified when your usage exceeds the threshold amount. Or, choose **% of budgeted amount** to be notified when your usage exceeds the threshold percentage.

    Next to the threshold, choose **Actual** to create an alert for actual usage. Or, choose **Forecasted** to create an alert for forecasted usage.
16. (Optional) Under **Notification preferences**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can be sent to a maximum of 10 email addresses.
17. (Optional) Under **Notification preferences**, for **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

    > **Important**
    >
    > After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.
18. (Optional) Under **Notification preferences**, for **AWS Chatbot Alerts**, you can choose to configure AWS Chatbot to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts on the AWS Chatbot console.
19. Choose **Next**.

20. (Optional) For **Attach actions**, you can configure an action that AWS Budgets performs on your behalf when the alert threshold is exceeded. For more information and instructions, see To configure a budget action.

21. Choose **Next**.

> **Note**
>
> To proceed, you must configure at least one of the following parameters for each alert:
>
> - An email recipient for notifications
> - An Amazon SNS topic for notifications
> - A budget action

22. Review your budget settings, and then choose **Create budget**.

Creating a Savings Plans budget

Use this procedure to create a budget that's specifically for Savings Plans utilization or coverage.

> **Note**
>
> It can take up to 48 hours for Savings Plans utilization and coverage metrics to generate, which is longer than the time frame for cost and usage data.

To create a Savings Plans budget

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.
4. Under **Budget setup**, choose **Customize (advanced)**.
5. Under **Budget types**, choose **Savings Plans budget**. Then, choose **Next**.
6. Under **Details**, for **Budget name**, enter the name of your budget. Your budget name must be unique within your account. It can contain A-Z, a-z, spaces, and the following characters:

```
_.:/=+-%@
```

7. Under **Utilization threshold**, for **Period**, choose how often you want the budget to reset the tracked utilization or coverage. Select **Daily** for every day, **Monthly** for every month, **Quarterly** for every three months, or **Annually** for every year.

   All budget times are in the UTC format.

8. For **Monitor my spend against**, choose **Utilization of Savings Plans** to track how much of your Savings Plans you used. Or, choose **Coverage of Savings Plans** to track how much of your instance usage is covered by Savings Plans.

   For **Utilization threshold**, enter the utilization percentage that you want AWS to notify you at. For example, for a utilization budget where you want to stay above 90% Savings Plans utilization, enter **90**. The budget notifies you when your overall Savings Plans utilization is below 90%.

   For **Coverage threshold**, enter the coverage percentage that you want AWS to notify you at. For example, for a coverage budget where you want to stay above 80%, enter **80**. The budget notifies you when your overall coverage is below 80%.

9. (Optional) Under **Budget scope**, for **Filters**, choose **Add filter** to apply one or more of the available filters. Your choice of budget type determines the set of filters that's displayed on the console.

   > **Note**
   >
   > You can't use the **Linked account** filter within a linked account.

10. Choose **Next**.

11. Under **Notification preferences**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can be sent to a maximum of 10 email addresses.

12. (Optional) For **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

> ⚠ **Important**
>
> After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.

13. (Optional) For **AWS Chatbot Alerts**, you can choose to configure AWS Chatbot to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts through the AWS Chatbot console.
14. Choose **Next**.

> ⓘ **Note**
>
> To proceed, you must configure at least one email recipient or an Amazon SNS topic for notifications.

15. Review your budget settings, and then choose **Create budget**.

Creating a reservation budget

Use this procedure to create a budget for RI utilization or coverage.

> ⓘ **Note**
>
> It can take up to 48 hours for Reservations utilization and coverage metrics to generate, which is longer than the time frame for cost and usage data.

To create a reservation budget

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.
4. Under **Budget setup**, choose **Customize (advanced)**.

5. Under **Budget types**, choose **Reservation budget**. Then, choose **Next**.
6. Under **Details**, for **Budget name**, enter the name of your budget. Your budget name must be unique within your account. It can contain A-Z, a-z, spaces, and the following characters:

   ```
   _.:/=+-%@
   ```

7. Under **Utilization threshold**, for **Period**, choose how often you want the budget to reset the tracked utilization or coverage. Select **Daily** for every day, **Monthly** for every month, **Quarterly** for every three months, or **Annually** for every year.

   All budget times are in the UTC format.
8. For **Monitor my spend against**, choose **Utilization of reservations** to track how much of your reservation you used. Or, choose **Coverage of reservations** to track how much of your instance usage is covered by reservations.
9. For **Service**, choose the service that you want the budget to track.
10. For **Utilization threshold**, enter the utilization percentage that you want AWS to notify you at. For example, for a utilization budget where you want to stay above 90% RI utilization, enter **`90`**. The budget notifies you when your overall RI utilization is below 90%.

    For **Coverage threshold**, enter the coverage percentage that you want AWS to notify you at. For example, for a coverage budget where you want to stay above 80%, enter **`80`**. The budget notifies you when your overall coverage is below 80%.
11. (Optional) Under **Budget scope**, for **Filters**, choose **Add filter** to apply one or more of the available filters. Your choice of budget type determines the set of filters that's displayed on the console.

    > **Note**
    >
    > You can't use the **Linked account** filter within a linked account.
12. Choose **Next**.
13. Under **Notification preferences**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can be sent to a maximum of 10 email addresses.
14. (Optional) For **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

> ⚠ **Important**
>
> After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.

15. (Optional) For **AWS Chatbot Alerts**, you can choose to configure AWS Chatbot to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts through the AWS Chatbot console.
16. Choose **Next**.

> ⓘ **Note**
>
> To proceed, you must configure at least one email recipient or an Amazon SNS topic for notifications.

17. Review your budget settings, and then choose **Create budget**.

Budget methods

You can set the budgeted amount of your cost or usage budget in one of the following ways. You can set one of these budgets no matter whether you're budgeting in a traditional sense—tracking to plan, for example—or if you want to monitor spend and receive alerts when costs increase beyond your threshold.

Fixed

With a fixed budget, you can monitor the same amount every budget period. For example, you can use a cost budget with the fixed method to monitor your costs against $100 every budget period.

Planned

The planned budgeting method is available for only monthly or quarterly budgets. With a planned budget, you can set a different amount to monitor each budget period. For example, you can use a monthly cost budget with the planned method to monitor your costs against

$100 in the first month, $110 in the second month, and other amounts in the remaining months.

With a planned budget, you can set the budget amount for up to 12 months or 4 quarters. After 12 months or 4 quarters, your budget amount is fixed at the last budget amount.

Auto-adjusting

An auto-adjusting budget dynamically sets your budget amount based on your spending or usage over a time range that you specify. The historical or forecast time range that you select is the auto-adjustment baseline for your budget.

At the beginning of each new period, AWS Budgets calculates your budget amount from your cost or usage data within the baseline time range. Make sure to select a time range that best matches your expectations for your account's AWS costs or usage. If you select a time range with lower usage than you typically expect, then you might get more budget alerts than you need. If you select a time range with higher usage than you typically expect, then you might not get as many budget alerts as you need.

For example, you can create an auto-adjusting cost budget with a baseline time range of the last six months. In this scenario, if your average spending each budget period in the last six months was $100, your auto-adjusted budget amount in the new period is $100.

If AWS Budgets updates your budget amount based on changes in your spending or usage, all budget alert notification subscribers get a notification that the budget amount changed.

> **Note**
>
> - When calculating your auto-adjusted budget amount, AWS Budgets doesn't include periods at the beginning of your baseline time range that don't have cost or usage data. For example, assume that you set your baseline time range as the last four quarters. However, your account had no cost data in the first quarter. Then, in this case, AWS Budgets calculates your auto-adjusted budget amount from only the last three quarters.
> - You see a temporary forecast while you're creating or editing a budget. After you save your budget, your auto-adjusted budget is set for the first time.

Budget filters

Based on your choice of budget type, you can choose one or more of the available budget filters.

API operation

Choose an action, such as `CreateBucket`.

Availability zone

Choose the `Availability zone` in which the resource that you want to create a budget for is running.

Billing entity

Helps you identify whether your invoices or transactions are for AWS Marketplace or for purchases of other AWS services. Possible values include:

- AWS: Identifies a transaction for AWS services other than in AWS Marketplace.
- AWS Marketplace: Identifies a purchase in AWS Marketplace.

Cost category

Choose the cost category group and value to track with this budget.

Instance family

Choose the family of instances to track using this budget.

Instance type

Choose the type of instance that you want to track with this budget.

Invoicing entity

The AWS entity that issues the invoice. Possible values include:

- Amazon Web Services, Inc. – The entity that issues invoices to customer globally, where applicable.
- Amazon Web Services India Private Limited – The entity that issues invoices to customers based in India.
- Amazon Web Services South Africa Proprietary Limited – The entity that issues invoices to customers in South Africa.

Legal entity

The Seller of Record of a specific product or service. In most cases, the invoicing entity and legal entity are the same. The values might differ for third-party AWS Marketplace transactions. Possible values include:

- Amazon Web Services, Inc. – The entity that sells AWS services.
- Amazon Web Services India Private Limited – The local Indian entity that acts as a reseller for AWS services in India.

> **Note**
>
> Amazon Web Services EMEA SARL is the marketplace operator for your purchases if your account is located in EMEA (excluding Turkey and South Africa), and the seller is eligible in EMEA. Purchases include subscriptions. Amazon Web Services, Inc. is the marketplace operator for purchases if the seller isn't eligible for EMEA. For more information, see AWS Europe.

Linked account

Choose an AWS account that is a member of the consolidated billing family that you're creating the budget for. For more information, see Consolidated billing for AWS Organizations in the *AWS Billing User Guide*.

> **Note**
>
> Do not use this filter within a member account. If the current account is a member account, filtering by `linked account` is not supported.

Platform

Choose the operating system that your RI runs on. **Platform** is either **Linux** or **Windows**.

Purchase option

Choose `On Demand Instances`, `Standard Reserved Instances`, or `Savings Plans`.

Region

Choose the Region in which the resource that you want to create a budget for is running.

Savings Plans type

Choose what you want to budget for, between **Compute Savings Plans** and **EC2 Instance Savings Plans**. The Savings Plans type filter is only available for Savings Plans utilization budgets.

Scope

Choose the scope of your RI. The scope is either regional or zonal.

Service

Choose an AWS service. Combined with **Billing entity**, **Invoicing entity**, and **Legal entity**, you can also use the **Service** dimension to filter costs by specific AWS Marketplace purchases. This includes your costs for specific AMIs, web services, and desktop apps. For more information, see What Is AWS Marketplace?

> **Note**
>
> You can use this filter only for cost, Savings Plans and Reserved Instance (RI) utilization, or Savings Plans and RI coverage budgets. Cost Explorer doesn't show revenue or usage for the AWS Marketplace software seller.
> The Savings Plans utilization, RI utilization, Savings Plans coverage reports, and RI coverage reports lets you filter by only one service at a time and only for the following services:
>
> - Amazon Elastic Compute Cloud
> - Amazon Redshift
> - Amazon Relational Database Service
> - Amazon ElastiCache
> - Amazon OpenSearch Service

Tag

If you activated any tags, choose a resource tag. A tag is a label that you can use to organize your resource costs and track them on a detailed level. There are AWS generated tags and user-defined tags. User-defined tag keys must use the `user:` prefix. You must activate tags to use them. For more information, see Activating the AWS-Generated Cost Allocation Tags and Activating User-Defined Cost Allocation Tags.

Tenancy

Choose whether you share an RI with another user. **Tenancy** is either **Dedicated** or **Default**.

Usage type

Usage types are the units each service uses to measure the usage for specific types of resources. If you choose a filter such as S3 and then choose a usage type value, such as `DataTransfer-Out-Bytes (GB)`, your costs are limited to S3 `DataTransfer-Out-Bytes (GB)`. You can create a usage budget only for a specific unit of measure. If you choose **Usage type** but not **Usage type group**, the budget monitors all of the available units of measure for the usage type.

Usage type group

A usage type group is a collection of usage types that have the same unit of measure. If you choose both the **Usage type group** and the **Usage type** filters, Cost Explorer shows you usage types that are automatically constrained to the group unit of measure. For example, assume you choose the group `EC2: Running Hours (Hrs)`, and then choose the `EC2-Instances` filter for **Usage type**. Cost Explorer shows you only the usage types that are measured in hours.

Viewing your budgets

You can view the state of your budgets at a glance on the **Budgets Overview** page. Your budgets are listed in a filterable table along with the following data:

- Your current costs and usage incurred for a budget during the budget period
- Your budgeted costs or usage for the budget period
- Your forecasted usage or costs for the budget period
- A percentage that shows your costs or usage compared to your budgeted amount
- A percentage that shows your forecasted costs or usage compared to your budgeted amount

To view your budgets

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. On the navigation pane, choose **Budgets**.
3. To see the filters and cost variances for your budgets, choose the budget's name in your list of budgets.

Note

You can view information about multiple budgets at once by selecting the check boxes in the Overview table. This opens a split-view panel on the right-hand side, where you can sort or filter the alerts to customize a budget report.

Reading your budgets

You can view detailed information about your budgets in two ways.

- Select your budget in the table to open a split-view panel with budget history and alert status on the right-hand side. In the split-view panel, navigation buttons allow you to move between budgets without leaving the page. To use the navigation buttons, select one budget at a time. When multiple budgets are selected, the navigation buttons are hidden.
- Choose your budget's name to see the budget details page. This page includes the following information:
  - **Current vs. budgeted** – Your current incurred costs compared to your budgeted costs.
  - **Forecasted vs. budgeted** – Your forecasted costs compared to your budgeted costs.
  - **Alerts** – Any alerts or notifications about the state of your budgets.
  - **Details** – The amount, type, time period, and any other additional parameters for your budget.
  - **Budget history** tab – A chart and table that show the history of your budget. `QUARTERLY` budgets show the last four quarters of history, and `MONTHLY` budgets show the last 12 months. Budget history isn't available for `ANNUAL` budgets.

    If you change the budgeted amount for a budget period, then the budgeted amount in the table is the last budgeted amount. For example, if you have a monthly budget set for 100 in January and you change the budget to 200 in February, then the February line in the table shows only the 200 budget.
  - **Alerts** tab – More details for any alerts about the state of your budget, including a **Definition** that describes the conditions for exceeding the alert threshold.

You can use this information to see how well your budget has matched your costs and usage in the past. You can also download all of the data that Budgets used to create the table through the following procedure.

To download a budget in a CSV file

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. On the navigation pane, choose **Budgets**.
3. To see the filters and cost variances for your budgets, choose the budget name in your list of budgets.
4. On the **Budget history** tab, choose **Download as CSV**.
5. Follow the instructions onscreen.

Editing a budget

> **Note**
>
> You can't edit the budget name.

To edit a budget

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. On the navigation pane, choose **Budgets**.
3. On the **Budgets** page, from your list of budgets, choose the budget that you want to edit.
4. Choose **Edit**.
5. Change the parameters that you want to edit. You can't change the budget name.
6. After you make your changes on each page, choose **Next**.
7. Choose **Save**.

Downloading a budget

You can download your budgets as a CSV file. The file includes all of the data for all of your budgets, such as Budget Name, Current Value and Forecasted Value, Budgeted Value, and more.

To download a budget

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. On the navigation pane, choose **Budgets**.
3. Choose **Download CSV**.
4. Open or save your file.

Copying a budget

You can copy an existing budget to a new one. By doing this, you can retain the filters and notification settings from your original budget, or change them. Billing and Cost Management automatically populates the fields on the page that you create the new budget on. You can update the budget parameters on this page.

To copy a budget

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. On the navigation pane, choose **Budgets**.
3. From the list of budgets, select the budget that you want to copy.
4. At the top of the page, choose **Actions**, and then choose **Copy**.
5. Change the parameters that you want to update. You must change the budget name.
6. After you make any necessary changes on each page, choose **Next**.
7. Choose **Copy budget**.

Deleting a budget

You can delete your budgets and the associated email and Amazon SNS notifications at any time. However, you can't recover a budget after you delete it. If you delete a budget, all email notifications and notification subscribers that are associated with the budget are also deleted.

To delete a budget

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. On the navigation pane, choose **Budgets**.
3. From your list of budgets, select one or more budgets that you want to delete.
4. At the top of the page, choose **Actions**, and then choose **Delete**.
5. Choose **Confirm**.

Configuring AWS Budgets actions

You can use AWS Budgets to run an action on your behalf when a budget exceeds a certain cost or usage threshold. To do this, after you set a threshold, configure a budget action to run either automatically or after your manual approval.

Your available actions include applying an IAM policy or a service control policy (SCP). They also include targeting specific Amazon EC2 or Amazon RDS instances in your account. You can use SCPs so that you don't need to provision any new resources during the budget period.

> **Note**
>
> From the management account, you can apply an SCP to another account. However, you can't target Amazon EC2 or Amazon RDS instances in another account.

You can also configure multiple actions to initiate at the same notification threshold. For example, you can configure actions to initiate automatically when you reach 90 percent of your forecasted costs for the month. To do so, perform the following actions:

- Apply a custom `Deny IAM` policy that restricts the ability for a user, group, or role to provision additional Amazon EC2 resources.

- Target specific Amazon EC2 instances in US `East (N. Virginia) us-east-1`.

Setting up a role for AWS Budgets to run budget actions

To use budget actions, you must create a service role for AWS Budgets. A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.

To allow AWS Budgets to perform actions on your behalf, you must grant the necessary permissions to the service role. The following table lists the permissions that you can grant the service role.

Permissions policy for budget actions	Instructions
Allows permission to control AWS resources	This is an AWS managed policy. For instructions on how to attach a managed policy, see To use a managed policy as a permissions policy for an identity (console) in the *IAM User Guide*
Allow AWS Budgets to apply IAM policies and SCPs	You can use this example policy as an inline policy or a customer managed policy. For instructions on how to embed an inline policy, see To embed an inline policy for a user or role (console) in the *IAM User Guide*. For instructions on how to create a customer managed policy, see Creating IAM policies (console) in the *IAM User Guide*.
Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances	You can use this example policy as an inline policy or a customer managed policy. For instructions on how to embed an inline policy, see To embed an inline policy for a user or role (console) in the *IAM User Guide*.

Permissions policy for budget actions	Instructions
	For instructions on how to create a customer managed policy, see Creating IAM policies (console) in the *IAM User Guide*.

Configuring a budget action

You can attach budget actions to an alert for either a cost budget or a usage budget. To configure a budget action on a new budget, first follow the steps for Creating a cost budget or Creating a usage budget. To configure a budget action on an existing cost or usage budget, first follow the steps for Editing a budget. Then, after you reach the **Configure alerts** step of creating or editing the budget, use the following procedure.

To configure a budget action

1. To configure a budget action on a new alert, choose **Add an alert threshold**. To configure a budget action on an existing alert, skip to step 7.
2. Under **Set alert threshold**, for **Threshold**, enter the amount that needs to be reached for you to be notified. This can be either an absolute value or a percentage. For example, say you have a budget of 200 dollars. To be notified at 160 dollars (80% of your budget), enter **`160`** for an absolute budget or **`80`** for a percentage budget.

   Next to the amount, choose **Absolute value** to be notified when your costs exceed the threshold amount. Or, choose **% of budgeted amount** to be notified when your costs exceed the threshold percentage.

   Next to the threshold, choose **Actual** to create an alert for actual spend. Or, choose **Forecasted** to create an alert for forecasted spend.
3. (Optional) Under **Notification preferences - Optional**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can have up to 10 email addresses.
4. (Optional) Under **Notification preferences - Optional**, for **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

> ⚠ **Important**
>
> After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.

5. (Optional) Under **Notification preferences - Optional**, for **AWS Chatbot Alerts**, you can configure AWS Chatbot to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts through the AWS Chatbot console.
6. Choose **Next**.
7. For **Attach actions - Optional**, choose **Add Action**.

   a. For **Select IAM role**, choose an IAM role to allow AWS Budgets to perform an action on your behalf.

   > ⓘ **Note**
   >
   > If you didn't configure and assign the appropriate permissions for the IAM role and for AWS Budgets, then AWS Budgets can't run your configured actions.
   > For simplified permissions management, we recommend that you use the managed policy. This ensures that your AWS Budgets actions work as intended and eliminates the need to update your existing IAM policy for AWS Budgets whenever any new functionality is added. This is because new functions and capabilities are added to the managed policy by default. For more information about managed policies, see Managed policies.

   For more information and examples of IAM role permissions, see Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances.

   b. For **Which action type should be applied when the budget threshold has been exceeded**, select the action that you want AWS Budgets to take on your behalf.

   You can choose from applying an IAM policy, attaching a service control policy (SCP), or targeting specific Amazon EC2 or Amazon RDS instances. You can apply multiple budget actions to a single alert. Only a management account can apply SCPs.

c. Depending on the action that you chose, complete the fields related to the resources that you want to apply the action to.

d. For **Do you want to automatically run this action when this threshold is exceeded**, choose **Yes** or **No**. If you choose **No**, then you run the action manually on the **Alert details** page. For instructions, see Reviewing and approving your budget action.

e. For **How do you want to be alerted when this action is run**, choose **Use the same alert settings when you defined this threshold** or **Use different alert settings**. To use different alert settings, complete the **Notification preferences** specific to this action.

8. Choose **Next**.

> **Note**
>
> To proceed, you must configure at least one of the following for each alert:
>
> - An email recipient for notifications
> - An Amazon SNS topic for notifications
> - A budget action

9. Review your budget settings, and then choose **Create budget** or **Save**.

After you create an action, you can view its status from the AWS Budgets page on the **Actions** column. This column shows your configured actions count, actions waiting for your approval (**Requires approval**), and your successfully completed actions.

Reviewing and approving your budget action

You receive a notification to inform you that an action is pending or has already run on your behalf, regardless of your action preferences. The notification includes a link to the **Budget details** page of the action. You can also navigate to the **Budget details** page by choosing the budget name on the AWS Budgets page.

On the **Budget details** page, you can review and approve your budget action.

To review and approve your budget action

1. On the **Budget details** page, in the **Alerts** section, choose **Requires approval**.
2. In the **Actions** pop-up, choose the name of the alert that requires an action.

3. On the **Alert details** page, in the **Action** section, review the action that requires approval.
4. Select the action that you want to run, and then choose **Run action**.
5. Choose **Yes, I am sure**.

Your pending actions move from the `pending` status in **Action history**, listing the newest actions at the top. AWS Budgets shows actions configured and run in the last 60 days. You can view the full history of actions by using AWS CloudTrail or by calling the `DescribeBudgetActionHistories` API.

Reversing a previous action

You can review and undo previously completed actions from the **Action history** table. Each status is defined as follows:

- **Standby** - AWS Budgets is actively evaluating the action.
- **Requires approval** - The action was initiated, and is waiting for your approval.
- **Completed** - The action successfully completed.
- **Reversed** - The action was undone, and AWS Budgets will no longer evaluate the action for the remaining budgeted period.

If you want AWS Budgets to re-evaluate the reversed action during the same period, you can choose **Reset**. You can do this, for example, if you initiated a read-only policy but then received approval from your manager to increase your budget and adjust your budgeted amount during the current period.

Creating an Amazon SNS topic for budget notifications

When you create a budget that sends notifications to an Amazon Simple Notification Service (Amazon SNS) topic, you need to either have a preexisting Amazon SNS topic or create one. Amazon SNS topics allow you to send notifications over SNS in addition to email. Your budget must have permissions to send a notification to your topic.

To create an Amazon SNS topic and grant permissions to your budget, use the Amazon SNS console.

> **Note**
>
> Amazon SNS topics must be in the same account as the Budgets you're configuring. Cross-account Amazon SNS isn't supported.

To create an Amazon SNS notification topic and grant permissions

1. Sign in to the AWS Management Console and open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. On the navigation pane, choose **Topics**.
3. Choose **Create topic**.
4. For **Name**, enter the name for your notification topic.
5. (Optional) For **Display name**, enter the name that you want displayed when you receive a notification.
6. In **Access policy**, choose **Advanced**.
7. In the policy text field, after **"Statement": [**, add the following text:

```
{
  "Sid": "E.g., AWSBudgetsSNSPublishingPermissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "budgets.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "your topic ARN",
   "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "<account-id>"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:budgets::<account-id>:*"
        }
      }
}
```

8. Replace **E.g., AWSBudgetsSNSPublishingPermissions** with a string. The `Sid` must be unique within the policy.
9. Choose **Create topic**.

10. Under **Details**, save your ARN.
11. Choose **Edit**.
12. Under **Access policy**, replace `your topic ARN` with the Amazon SNS topic ARN from step 10.
13. Choose **Save changes**.

    Your topic now appears in the list of topics on the **Topics** page.

Troubleshooting

You might encounter the following error messages when you're creating your Amazon SNS topic for budget notifications.

Please comply with SNS ARN format

There's a syntax error in the ARN you replaced (step 9). Confirm the ARN for proper syntax and formatting.

Invalid SNS topic

AWS Budgets doesn't have access to the SNS topic. Confirm that you've allowed budgets.amazonaws.com the ability to publish messages to this SNS topic, in the SNS topic's resource based policy.

The SNS topic is encrypted

You have **encryption** enabled on the SNS topic. The SNS topic won't work without additional permissions. Disable encryption on the topic, and refresh the **Budget edit** page.

Checking or resending notification confirmation emails

When you create a budget with notifications, you also create Amazon SNS notifications. For notifications to be sent, you must accept the subscription to the Amazon SNS notification topic.

To confirm that your notification subscriptions have been accepted or to resend a subscription confirmation email, use the Amazon SNS console.

To check your notification status or to resend a notification confirmation email

1. Sign in to the AWS Management Console and open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.

2. On the navigation pane, choose **Subscriptions**.
3. On the **Subscriptions** page, for **Filter**, enter `budget`. A list of your budget notifications appears.
4. Check the status of your notification. Under **Status**, `PendingConfirmation` appears if a subscription hasn't been accepted and confirmed.
5. (Optional) To resend a confirmation request, select the subscription with a pending confirmation and choose **Request confirmation**. Amazon SNS sends a confirmation request to the endpoints that are subscribed to the notification.

   When each owner of an endpoint receives the email, they must choose the **Confirm subscription** link to activate the notification.

Protecting your Amazon SNS budget alerts data with SSE and AWS KMS

You can use server-side encryption (SSE) to transfer sensitive data in encrypted topics. SSE protects Amazon SNS messages by using keys managed in AWS Key Management Service (AWS KMS).

To manage SSE using AWS Management Console or the AWS Service Development Kit (SDK), see Enabling Server-Side Encryption (SSE) for an Amazon SNS Topic in the *Amazon Simple Notification Service Getting Started Guide*.

To create encrypted topics using AWS CloudFormation, see the AWS CloudFormation User Guide.

SSE encrypts messages as soon as Amazon SNS receives them. The messages are stored encrypted and are decrypted using Amazon SNS only when they're sent.

Configuring AWS KMS permissions

You must configure your AWS KMS key policies before you can use SSE. The configuration enables you to encrypt topics, as well as encrypt and decrypt messages. For details about AWS KMS permissions, see AWS KMS API Permissions: Actions and Resources Reference in the *AWS Key Management Service Developer Guide*.

You can also use IAM policies to manage AWS KMS key permissions. For more information, see Using IAM Policies with AWS KMS.

> **Note**
>
> Although you can configure global permissions to send and receive message from Amazon SNS, AWS KMS requires you to name the full ARN of AWS KMS keys (KMS key) in the specific Regions. You can find this in the **Resource** section of an IAM policy.
> You must ensure that the key policies of the KMS keys allow the necessary permissions. To do this, name the principals that produce and consume encrypted messages in Amazon SNS as users in the KMS key policy.

To enable compatibility between AWS Budgets and encrypted Amazon SNS topics

1. Create a KMS key.
2. Add the following text to the KMS key policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "budgets.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "<account-id>"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:budgets::<account-id>:*"
        }
      }
    }
  ]
}
```

3. Enable SSE for your SNS topic.

> **Note**
>
> Be sure that you're using the same KMS key that grants AWS Budgets the permissions to publish to encrypted Amazon SNS topics.

4. Choose **Save Changes**.

Receiving budget alerts in Amazon Chime and Slack

You can receive your AWS Budgets alerts in Amazon Chime and Slack by using AWS Chatbot.

AWS Chatbot enables you to receive AWS Budgets alerts directly into your designated Slack channel or Amazon Chime chat room.

To begin receiving your budget alerts in Slack and Amazon Chime

1. Follow Creating a budget or Editing a budget and select **Configure alerts**.
2. Add an Amazon SNS topic as an alert recipient to a specific alert or alerts. To ensure that AWS Budgets has permissions to publish to your Amazon SNS topics, see Creating an Amazon SNS Topic for Budget Notifications.
3. Select **Confirm Budget**.
4. Select **Done**.
5. Open the AWS Chatbot console.
6. Select your chat client.
7. Choose **Configure**.

   There are specific authorization processes for each endpoint: for example, Slack channel, Amazon Chime rooms, AWS Chatbot IAM permissions, and SNS topics receiving the budget alerts.
8. Choose **Slack workspace**.
9. Choose a **channel type**.
   - **Public**: Everyone in your workspace can see or join the channel
   - **Private**: The channel is viewable only by invitation
10. Either select an existing IAM role for AWS Chatbot to assign or create a new IAM role.

11. Choose a **role name**.
12. Select the Amazon SNS Region.
13. Select the **SNS topic**.

> **Note**
>
> You can send AWS Budgets alerts to multiple Amazon SNS topics and Regions.
> At least one of the Amazon SNS topics must match the Amazon SNS topic or topics of your budget or budgets.

14. Select **Configure**.

Reporting your budget metrics with budget reports

With AWS Budgets, you can configure a report to monitor the performance of your existing budgets on a daily, weekly, or monthly cadence and deliver that report to up to 50 email addresses.

You can create up to 50 reports for each standalone account or AWS Organizations management account. Each budget report costs $.01 USD for each report delivered. This is regardless of the number of recipients receiving the report. For example, a daily budget report costs $.01 a day, a weekly budget report costs $.01 a week, and a monthly budget report costs $.01 a month.

If you use consolidated billing in an organization and you own the management account, you can use IAM policies to control access to budgets by member accounts. By default, owners of member accounts can create their own budgets but can't create or edit budgets for other users. You can use IAM to allow users in a member account to create, edit, delete, or read the budget for your management account. Do this, for example, to allow another account to administer your budget. For more information, see Overview of managing access permissions. For more information about AWS Organizations, see the AWS Organizations User Guide.

Topics

- Creating an AWS Budgets report
- Editing an AWS Budgets report
- Copying an AWS Budgets report
- Deleting an AWS Budgets report

Creating an AWS Budgets report

Use the following procedure to create an AWS Budgets report.

To create an AWS Budgets report

1. Sign in to the AWS Management Console and open the AWS Billing console at https://console.aws.amazon.com/billing/.
2. In the navigation pane, choose **Budgets Reports**.
3. On the top right of the page, choose **Create budget report**.
4. Select the budgets that you want to include in your report. You can select up to 50 budgets.

> ⓘ **Note**
>
> If you select more, you can't proceed to the next step until you change your selection to 50 or fewer budgets.

5. For **Report frequency**, choose **Daily**, **Weekly**, or **Monthly**.

   - If you choose a **Weekly** report: For **Day of week**, choose the day of the week that you want the report delivered.
   - If you choose a **Monthly** report: For **Day of month**, choose the calendar day of the month that you want the report delivered. If you choose any day after the 28th day, and the next month doesn't have that calendar day, then your report is delivered on the last day of that month.

   Reports are delivered at approximately 0:00 UTC+0 on the specified day.
6. For **Email recipients**, enter the email addresses to deliver the report to. Separate multiple email addresses with commas. You can include up to 50 email recipients for each budget report.
7. For **Budget report name**, enter the name of your budget report. This name appears on the subject line of the budget report email. You can change the report name at any time.
8. Choose **Create budget report**.

Your report appears on the AWS Budgets Reports dashboard. On the dashboard, you can filter your reports by **Report name**. For each report, the dashboard also shows **Frequency**, **Budgets included**, and **Recipient(s)**.

Editing an AWS Budgets report

You can use this procedure to edit an AWS Budgets report.

To edit an AWS Budgets report

1. Sign in to the AWS Management Console and open the AWS Billing console at https://console.aws.amazon.com/billing/.
2. In the navigation pane, choose **Budgets Reports**.

3. Choose the name of the report that you want to edit.
4. On the **Edit budget report** page, change the parameters that you want to edit.
5. Choose **Save**.

Copying an AWS Budgets report

Use the following procedure to copy an AWS Budgets report.

To copy an AWS Budgets report

1. Sign in to the AWS Management Console and open the AWS Billing console at https://console.aws.amazon.com/billing/.
2. In the navigation pane, choose **Budgets Reports**.
3. From the list of reports, select the report that you want to copy.
4. At the top of the page, choose **Actions**, and then choose **Copy**.
5. Change the parameters that you want to update.
6. Choose **Create budget report**.

Deleting an AWS Budgets report

Use the following procedure to delete an AWS Budgets report.

To delete an AWS Budgets report

1. Sign in to the AWS Management Console and open the AWS Billing console at https://console.aws.amazon.com/billing/.
2. In the navigation pane, choose **Budgets Reports**.
3. From the list of reports, select the report that you want to delete.
4. At the top of the page, choose **Actions**, and then choose **Delete**.
5. Choose **Confirm**.

Detecting unusual spend with AWS Cost Anomaly Detection

AWS Cost Anomaly Detection is a feature that uses machine learning models to detect and alert on anomalous spend patterns in your deployed AWS services.

Using AWS Cost Anomaly Detection includes the following benefits:

- You receive alerts individually in aggregated reports either in an email message or an Amazon SNS topic.

  For Amazon SNS topics, create an AWS Chatbot configuration that maps the SNS topic to a Slack channel or an Amazon Chime chat room. For more information, see Receiving AWS Cost Anomaly Detection alerts in Amazon Chime and Slack.
- You can evaluate your spend patterns using machine learning methods to minimize false positive alerts. For example, you can evaluate weekly or monthly seasonality and natural growth.
- You can investigate the root cause of the anomaly, such as the AWS account, service, Region, or usage type that's driving the cost increase.
- You can configure how to evaluate your costs. Choose whether you want to analyze all of your AWS services independently or analyze specific member accounts, cost allocation tags, or cost categories.

After your billing data is processed, AWS Cost Anomaly Detection runs approximately three times a day in order to monitor for anomalies in your net unblended cost data (that is, net costs after all applicable discounts are calculated). You might experience a slight delay in receiving alerts. Cost Anomaly Detection uses data from Cost Explorer, which has a delay of up to 24 hours. As a result, it can take up to 24 hours to detect an anomaly after a usage occurs. If you create a new monitor, it can take 24 hours to begin detecting new anomalies. For a new service subscription, 10 days of historical service usage data is needed before anomalies can be detected for that service.

Note

You can opt out of Cost Anomaly Detection at any time. For more information, see Opting out of Cost Anomaly Detection.

Topics

- Setting up your anomaly detection
- Access control and examples for Cost Anomaly Detection
- Getting started with AWS Cost Anomaly Detection
- Editing your alerting preferences
- Creating an Amazon SNS topic for anomaly notifications
- Receiving AWS Cost Anomaly Detection alerts in Amazon Chime and Slack
- Opting out of Cost Anomaly Detection

Setting up your anomaly detection

The overviews in this section describe how to get started with AWS Cost Anomaly Detection in AWS Billing and Cost Management.

Topics

- Enabling Cost Explorer
- Controlling access using IAM
- Accessing the console
- Quotas

Enabling Cost Explorer

AWS Cost Anomaly Detection is a feature within Cost Explorer. To access AWS Cost Anomaly Detection, enable Cost Explorer. For instructions on how to enable Cost Explorer using the console, see Enabling Cost Explorer.

Controlling access using IAM

After you enable Cost Explorer at the management account level, you can use AWS Identity and Access Management (IAM) to manage access to your billing data for individual users. You can then grant or revoke access on an individual level for each user role, rather than granting access to all users.

A user must be granted explicit permission to view pages in the Billing and Cost Management console. With the appropriate permissions, the user can view costs for the AWS account that the user belongs to. For the policy that grants the necessary permissions to a user, see Billing and Cost Management actions policies.

For more information about using resource-level access and attribute-based access control (ABAC) for Cost Anomaly Detection, see Access control and examples for Cost Anomaly Detection.

Accessing the console

When your setup is complete, access AWS Cost Anomaly Detection.

To access AWS Cost Anomaly Detection

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Anomaly Detection**.

Quotas

For the default quotas, see AWS Cost Anomaly Detection.

Access control and examples for Cost Anomaly Detection

You can use resource-level access controls and attribute-based access control (ABAC) tags for cost anomaly monitors and anomaly subscriptions. Each anomaly monitor and anomaly subscription resource has a unique Amazon Resource Name (ARN). You can also attach tags (key-value pairs) to each feature. Both resource ARNs and ABAC tags can be used to give granular access control to user roles or groups within your AWS accounts.

For more information about resource-level access controls and ABAC tags, see How AWS Cost Management works with IAM.

> **Note**
>
> Cost Anomaly Detection doesn't support resource-based policies. Resource-based policies are directly attached to AWS resources. For more information about the difference between policies and permissions, see Identity-based policies and resource-based policies in the *IAM User Guide*.

Controlling access using resource-level policies

You can use resource-level permissions to allow or deny access to one or more Cost Anomaly Detection resources in an IAM policy. Alternatively, use resource-level permissions to allow or deny access to all Cost Anomaly Detection resources.

When you create an IAM, use the following Amazon Resource Name (ARN) formats:

- `AnomalyMonitor` resource ARN

  `arn:${partition}:ce::${account-id}:anomalymonitor/${monitor-id}`
- `AnomalySubscription` resource ARN

  `arn:${partition}:ce::${account-id}:anomalysubscription/${subscription-id}`

To allow the IAM entity to get and create an anomaly monitor or anomaly subscription, use a policy similar to this example policy.

> **Note**
>
> - For `ce:GetAnomalyMonitor` and `ce:GetAnomalySubscription`, users have all or none of the resource-level access control. This requires the policy to use a generic ARN in the form of `arn:${partition}:ce::${account-id}:anomalymonitor/*`, `arn:${partition}:ce::${account-id}:anomalysubscription/*`, or `*`.
> - For `ce:CreateAnomalyMonitor` and `ce:CreateAnomalySubscription`, we don't have a resource ARN for this resource. So, the policy always uses the generic ARN that was mentioned in the previous bullet.
> - For `ce:GetAnomalies`, use the optional `monitorArn` parameter. When used with this parameter, we confirm if the user has access to the `monitorArn` passed.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ce:GetAnomalyMonitors",
                "ce:CreateAnomalyMonitor"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ce::999999999999:anomalymonitor/*"
        },
        {
            "Action": [
                "ce:GetAnomalySubscriptions",
                "ce:CreateAnomalySubscription"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ce::999999999999:anomalysubscription/*"
        }
    ]
}
```

To allow the IAM entity to update or delete anomaly monitors, use a policy similar to this example policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ce:UpdateAnomalyMonitor",
                "ce:DeleteAnomalyMonitor"
                ],
            "Resource": [
              "arn:aws:ce::999999999999:anomalymonitor/f558fa8a-
bd3c-462b-974a-000abc12a000",
              "arn:aws:ce::999999999999:anomalymonitor/f111fa8a-
bd3c-462b-974a-000abc12a001"
  ]
         }
    ]
}
```

Controlling access using tags (ABAC)

You can use tags (ABAC) to control access to Cost Anomaly Detection resources that support tagging. To control access using tags, provide the tag information in the `Condition` element of a policy. You can then create an IAM policy that allows or denies access to a resource based on the resource's tags. You can use tag condition keys to control access to resources, requests, or any part of the authorization process. For more information about IAM roles using tags, see Controlling access to and for users and roles using tags in the *IAM User Guide*.

Create an identity-based policy that allows updating anomaly monitors. If the monitor tag `Owner` has the value of the user name, use a policy that's similar to this example policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ce:UpdateAnomalyMonitor"
            ],
            "Resource": "arn:aws:ce::*:anomalymonitor/*",
            "Condition": {
                "StringEquals": {
   "aws:ResourceTag/Owner": "${aws:username}"
     }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ce:GetAnomalyMonitors",
            "Resource": "*"
        }
    ]
}
```

Getting started with AWS Cost Anomaly Detection

With AWS Cost Anomaly Detection in AWS Billing and Cost Management, you can configure your cost monitors and alert subscriptions in several different ways.

Topics

- Creating your cost monitors and alert subscriptions
- Detection history values
- Viewing your detected anomalies and root causes
- Monitor types

Creating your cost monitors and alert subscriptions

Configure AWS Cost Anomaly Detection so that it detects anomalies at a lower granularity and spend patterns, in context to your monitor type.

For example, your spend patterns for Amazon EC2 usage might be different from your AWS Lambda or Amazon S3 spend patterns. By segmenting spends by AWS services, AWS Cost Anomaly Detection can detect separate spend patterns that help decrease false positive alerts. You can also create cost monitors. They can evaluate specific cost allocation tags, member accounts within an organization (AWS Organizations), and cost categories based on your AWS account structure.

As you create your cost monitors, configure your alert subscriptions specific to each monitor.

To create a cost monitor

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. Choose the **Cost monitors** tab.
4. Choose **Create monitor**.
5. In **Step 1**, choose a monitor type and name your monitor.

   For more information about each monitor type and best practices, see Monitor types.

   For **Monitor name**, enter a name for your anomaly monitor. We recommend that the name is a short description. That way, you know what the monitor represents when you view your monitors on the **Cost monitors** tab.
6. (Optional) Add a tag to your monitor. For more information about tags, see Tagging AWS resources in the *AWS General Reference guide*.

   a. Enter the key value for the tag.

   b. Choose **Add new tag** to add additional tags. The maximum number of tags that you can add is 50.
7. Choose **Next**.
8. In **Step 2**, configure your alert subscriptions.

   For **Alert subscription**, if you don't have an existing subscription, choose **Create a new subscription**. If you have existing subscriptions, select **Choose an existing subscription**.

> **Note**
>
> An alert subscription notifies you when a cost monitor detects an anomaly. Depending on the alert frequency, you can notify designated individuals by email or Amazon SNS. For Amazon SNS topics, configure to create an AWS Chatbot configuration. This configuration maps the SNS topic to a Slack channel or an Amazon Chime chat room. For example, create a subscription for the Finance team in your organization. For more information, see Receiving AWS Cost Anomaly Detection alerts in Amazon Chime and Slack.

For **Subscription name**, enter a name that describes your use case. For example, if the subscription is meant for leadership, the subscription name might be “Leadership report.”

Under **Alerting frequency**, choose your preferred notification frequency.

- **Individual alerts** - The alert notifies you as soon as an anomaly is detected. You might receive multiple alerts throughout a day. These notifications require an Amazon SNS topic.

  You can configure the Amazon SNS topic to create an AWS Chatbot configuration that maps the SNS topic to a Slack channel or an Amazon Chime chat room. For more information, see Receiving AWS Cost Anomaly Detection alerts in Amazon Chime and Slack.
- **Daily summaries** - The alert notifies you with a daily summary when anomalies are detected. You receive one email that contains information for multiple anomalies that occurred that day. These notifications require at least one email recipient.
- **Weekly summaries** - The alert notifies you with a weekly summary when anomalies are detected. You receive one email that contains information for multiple anomalies that occurred that week. These notifications require at least one email recipient.

Under **Alert recipients**, enter email addresses for this subscription.

For **Threshold**, enter a number to configure the anomalies that you want to generate alerts for.

There are two types of thresholds: absolute and percentage. Absolute thresholds trigger alerts when an anomaly's total cost impact exceeds your chosen threshold. Percentage thresholds trigger alerts when an anomaly's total impact percentage exceeds your chosen threshold. Total impact percentage is the percentage difference between the total expected spend and total actual spend.

(Optional) Choose **Add threshold** to configure a second threshold on the same subscription. Thresholds can be combined by choosing **AND** or **OR** from the dropdown list.

> **Note**
>
> AWS Cost Anomaly Detection sends you a notification when an anomaly reaches or exceeds the **Threshold**. If an anomaly continues over multiple days, then alert recipients will continue to get notifications while the threshold is met.
> Even if an anomaly is below the alert threshold, the machine learning model continues to detect spend anomalies on your account. All the anomalies that the machine learning model detected (with cost impacts that are greater or less than the threshold) are available in the **Detection history** tab.

9. (Optional) Add a tag to your alert subscription. For more information about tags, see Tagging AWS resources in the *AWS General Reference guide*.

   a. Enter the key value for the tag.

   b. Choose **Add new tag** to add additional tags. The maximum number of tags that you can add is 50.

10. (Optional) Choose **Add alert subscriptions** to create another alert subscription. With this option, you can create a new subscription using the same monitor.

11. Choose **Create monitor**.

To create an alert subscription

You must create at least one alert subscription for each monitor. The "create cost monitor steps" that are described earlier already include the alert subscription creation process. If you want to create additional subscriptions, follow these steps.

1. Choose the **Alert subscriptions** tab.
2. Choose **Create a subscription**.
3. For **Subscription name**, enter a name that describes your use case. For example, if the subscription is meant for leadership, then the subscription name might be “Leadership report.”
4. Under **Alerting frequency**, choose your preferred notification frequency.

- **Individual alerts** - The alert notifies you as soon as an anomaly is detected. You might receive multiple alerts throughout a day. These notifications require an Amazon SNS topic.

  You can configure the Amazon SNS topic to create an AWS Chatbot configuration. This configuration maps the SNS topic to a Slack channel or an Amazon Chime chat room. For more information, see Receiving AWS Cost Anomaly Detection alerts in Amazon Chime and Slack.
- **Daily summaries** - The alert notifies you with a daily summary when anomalies are detected. You receive one email that contains information for multiple anomalies that occurred that day. These notifications require at least one email recipient.
- **Weekly summaries** - The alert notifies you with a weekly summary when anomalies are detected. You receive one email that contains information for multiple anomalies that occurred that week. These notifications require at least one email recipient.

5. Under **Alert recipients**, enter email addresses for this subscription.
6. For **Threshold**, enter a number to configure the anomalies that you want to generate alerts for.

   There are two types of thresholds: absolute and percentage. Absolute thresholds trigger alerts when an anomaly's total cost impact exceeds your chosen threshold. Percentage thresholds trigger alerts when an anomaly's total impact percentage exceeds your chosen threshold. Total impact percentage is the percentage difference between the total expected spend and total actual spend.

   (Optional) Choose **Add threshold** to configure a second threshold on the same subscription. Thresholds can be combined by choosing **AND** or **OR** from the dropdown list.

   > **Note**
   >
   > AWS Cost Anomaly Detection sends you a notification when an anomaly reaches or exceeds the **Threshold**. If an anomaly continues over multiple days, then alert recipients will continue to get notifications while the threshold is met.
   > Even if an anomaly is below the alert threshold, the machine learning model continues to detect spend anomalies on your account. All the anomalies that the machine learning model detected (with cost impacts that are greater or less than the threshold) are available in the **Detection history** tab.

7. In the **Cost monitors** section, select the monitors that you want to be associated with the alert subscription.
8. (Optional) Add a tag to your alert subscription. For more information about tags, see Tagging AWS resources in the *AWS General Reference guide*.

    a. Enter the key value for the tag.

    b. Choose **Add new tag** to add additional tags. The maximum number of tags that you can add is 50.
9. Choose **Create subscription**.

> **Note**
>
> You can only access cost monitors and alert subscriptions under the account that created them. For example, suppose that the cost monitor was created under a member account. Then, the management account can't view or edit the cost monitors, alert subscriptions, or detected anomalies.

Detection history values

On the **Detection history** tab, you can view a list of all the anomalies detected over the time frame that you selected. By default, you can see the anomalies that are detected in the last 90 days. You can search by **Severity**, **Assessment**, **Service**, **Account**, **Usage type**, **Region**, or **Monitor type**. You can sort by **Start date**, **Last detected date**, **Actual spend**, **Expected spend**, **Total cost impact**, and **Impact percentage**.

The following information is included on the **Detection history** tab:

Time frame

The options are **Last 30 days**, **Last 60 days**, and **Last 90 days**.

Start date

The day that the anomaly started.

Last detected date

The last time that the anomaly was detected.

Severity

Represents how abnormal a certain anomaly is accounting for historical spending patterns. A low severity generally suggests a small spike compared to historical spend and a high severity suggests a big spike. However, a small spike with historically consistent spend is categorized as high severity. And, similarly, a big spike with irregular historical spend is categorized as low severity.

Duration

The duration that the anomaly lasted. An anomaly can be on-going.

Monitor name

The name of the anomaly monitor.

Service

The service that caused the anomaly. If the service field is empty, AWS has detected an anomaly, but the root cause is unclear.

Account

The account ID and account name that caused the anomaly. If the account is empty, AWS has detected an anomaly, but the root cause is undetermined.

Actual spend

The total amount you actually spent during the anomaly's duration.

Expected spend

The amount our machine learning models expected you to spend during the anomaly's duration, based on your historical spending pattern.

Total cost impact

The spend increase detected compared to the expected spend amount. It is calculated as **actual spend - expected spend**. For example, a total cost impact of $20 on a service monitor means that there was a $20 increase detected in a particular service with a total duration of the specified days.

Impact percentage

The percentage difference between the actual spend and expected spend. It is calculated as **(total cost impact / expected spend) * 100**. For example, if the total cost impact was $20 and the expected spend was $60, then the impact percentage would be 33.33%. This value cannot be calculated when expected spend is zero, so in those situations the value will show as “N/A”.

Assessment

For each detected anomaly, you can submit an assessment to help improve our anomaly detection systems. The possible values are **Not submitted**, **Not an issue**, or **Accurate anomaly**.

Viewing your detected anomalies and root causes

After you create your monitors, AWS Cost Anomaly Detection evaluates your future spend. Based on your defined alert subscriptions, you might start receiving alerts within 24 hours.

To view your anomalies from an email alert

1. Choose the provided **View in Anomaly Detection** link.
2. On the **Anomaly details** page, you can view the root cause analysis and cost impact of the anomaly.
3. (Optional) Choose **View in Cost Explorer** to view a time series graph of the cost impact.
4. (Optional) Choose **View root cause** in the **Top ranked potential root causes** table to see a time series graph that's filtered by the root cause.
5. (Optional) Choose **Submit assessment** in the **Did you find this detected anomaly to be helpful?** information alert to provide feedback and help improve our detection accuracy.

To view your anomalies from the AWS Billing and Cost Management console

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. (Optional) On the **Detection history** tab, use the search area to narrow the list of detected anomalies for a particular category. The categories that you can choose are Severity, Assessment, Service, Account, Usage type, Region, and Monitor type.
4. (Optional) Choose the **Start date** for a particular anomaly to view the details.
5. On the **Anomaly details** page, you can view the root cause analysis and cost impact of the anomaly.

6. (Optional) Choose **View in Cost Explorer** to view a time series graph of the cost impact and, if necessary, dive deeper into the data.

7. (Optional) Choose **View root cause** in the **Top ranked potential root causes** table to see a time series graph that's filtered by the root cause.

8. (Optional) Choose **Submit assessment** in the **Did you find this detected anomaly to be helpful?** information alert to provide feedback and help improve our detection accuracy.

To view your anomalies from an Amazon SNS topic

1. Subscribe an endpoint to the Amazon SNS topic that you created for a cost monitor with individual alerts. For instructions, see Subscribing to an Amazon SNS topic in the *Amazon Simple Notification Service Developer Guide*.

2. After your endpoint receives messages from the Amazon SNS topic, open a message and then find the **anomalyDetailsLink** URL. The following example is a message from AWS Cost Anomaly Detection through Amazon SNS.

```
{
    "accountId": "123456789012",
    "anomalyDetailsLink": "https://console.aws.amazon.com/cost-management/home#/
anomaly-detection/monitors/abcdef12-1234-4ea0-84cc-918a97d736ef/anomalies/12345678-
abcd-ef12-3456-987654321a12",
    "anomalyEndDate": "2021-05-25T00:00:00Z",
    "anomalyId": "12345678-abcd-ef12-3456-987654321a12",
    "anomalyScore": {
        "currentScore": 0.47,
        "maxScore": 0.47
    },
    "anomalyStartDate": "2021-05-25T00:00:00Z",
    "dimensionalValue": "ServiceName",
    "impact": {
        "maxImpact": 151,
        "totalActualSpend": 1301,
        "totalExpectedSpend": 300,
        "totalImpact": 1001,
        "totalImpactPercentage": 333.67
    },
    "monitorArn": "arn:aws:ce::123456789012:anomalymonitor/
abcdef12-1234-4ea0-84cc-918a97d736ef",
    "rootCauses": [
        {
            "linkedAccount": "AnomalousLinkedAccount",
            "linkedAccountName": "AnomalousLinkedAccountName",
            "region": "AnomalousRegionName",
            "service": "AnomalousServiceName",
            "usageType": "AnomalousUsageType"
        }
    ],
    "subscriptionId": "874c100c-59a6-4abb-a10a-4682cc3f2d69",
    "subscriptionName": "alertSubscription"
}
```

3. Open the **anomalyDetailsLink** URL in a web browser. The URL takes you to the associated **Anomaly details** page. This page shows the root cause analysis and cost impact of the anomaly.

Monitor types

You can choose the monitor type that fits your account structure. Currently, we offer the following monitor types:

- **AWS services** - We recommend this monitor if you don't need to segment your spend by internal organizations or environments. This single monitor evaluates all the AWS services that are used by your individual AWS account for anomalies. When you add new AWS services, the monitor automatically begins to evaluate the new service for anomalies. That way, you don't have to manually configure your settings.

> **Note**
>
> Management accounts can have one AWS services monitor and up to 500 custom monitors (linked account, cost allocation tag, and cost category) for a total of 501 anomaly monitors. Member accounts only have access to the AWS services monitor.

- **Linked account** - This monitor evaluates the total spend of an individual, or group of, member accounts. If your Organizations need to segment spend by team, product, services, or environment, this monitor is useful. The maximum number of member accounts that you can select for each monitor is 10.
- **Cost category** - This monitor is recommended if you use cost categories to organize and manage your spend. This monitor type is restricted to one `key:value` pair.

- **Cost allocation tag** - This monitor is similar to **Linked account**. If you to need to segment your spend by team, product, services, or environment, this monitor is useful. This monitor type is restricted to one key, but accepts multiple values. The maximum number of values that you can select for each monitor is 10.

We recommend that you do not create monitors that span multiple monitor types. This might lead to evaluating overlapping spends that generate duplicate alerts.

For more information about creating your Amazon SNS topic, see Creating an Amazon SNS topic for anomaly notifications.

Editing your alerting preferences

You can adjust your cost monitors and alert subscriptions in AWS Billing and Cost Management to match your needs.

To edit your cost monitors

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. Choose the **Cost monitors** tab.
4. Select the monitor that you want to edit.
5. Choose **Edit**.
   - (Alternative) Choose the individual monitor name.
   - Choose **Edit monitor**.
6. On the **Edit monitor** page, change any settings for **monitor name** and **attached alert subscriptions**.
7. Choose **Manage tags** to add, edit, or remove tags for the monitor.
8. Choose **Save**.

To edit your alert subscriptions

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.

2. In the navigation pane, choose **Cost Anomaly Detection**.
3. Choose the **Alert subscriptions** tab.
4. Select the subscription that you want to edit.
5. Choose **Edit**.
   - (Alternative) Choose the individual monitor name.
   - Choose **Edit**.
6. On the **Edit alert subscription** page, change any settings for **subscription name**, **threshold**, **frequency**, **recipients**, or **cost monitors**.
7. Choose **Manage tags** to add, edit, or remove tags for the monitor.
8. Choose **Save**.

Creating an Amazon SNS topic for anomaly notifications

To create an anomaly detection monitor that sends notifications to an Amazon Simple Notification Service (Amazon SNS) topic, you must already have Amazon SNS topic or create a new one. You can use Amazon SNS topics to send notifications over SNS in addition to email. AWS Cost Anomaly Detection must have permissions to send a notification to your topic.

To create an Amazon SNS notification topic and grant permissions

1. Sign in to the AWS Management Console and open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. In the navigation pane, choose **Topics**.
3. Choose **Create topic**.
4. For **Name**, enter the name for your notification topic.
5. (Optional) For **Display name**, enter the name that you want displayed when you receive a notification.
6. In **Access policy**, choose **Advanced**.
7. In the policy text field, after **"Statement": [**, enter one of the following statements:

   To allow the AWS Cost Anomaly Detection service to publish to the Amazon SNS topic, use the following statement.

   ```
   {
     "Sid": "E.g., AWSAnomalyDetectionSNSPublishingPermissions",
   ```

```
  "Effect": "Allow",
  "Principal": {
    "Service": "costalerts.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "your topic ARN"
}
```

To allow the AWS Cost Anomaly Detection service to publish to the Amazon SNS topic only on behalf of a certain account, use the following statement.

```
{
  "Sid": "E.g., AWSAnomalyDetectionSNSPublishingPermissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "costalerts.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "your topic ARN",
  "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "account-ID"
          ]
        }
  }
}
```

Note

In this topic policy, you enter the subscription’s account ID as the value for the `aws:SourceAccount` condition. This condition has AWS Cost Anomaly Detection interact with the Amazon SNS topic only when performing operations for the account that owns the subscription.

You can restrict AWS Cost Anomaly Detection to interact with the topic only when performing operations on behalf of a specific subscription. To do this, use the `aws:SourceArn` condition in the topic policy.

For more information about these conditions, see `aws:SourceAccount` and `aws:SourceArn` in the *IAM User Guide*.

8. In the topic policy statement that you select, replace the following values:

   - Replace (for example, *`AWSAnomalyDetectionSNSPublishingPermissions`*) with a string. The `Sid` must be unique within the policy.
   - Replace *`your topic ARN`* with the Amazon SNS topic Amazon Resource Name (ARN).
   - If you're using the statement with the `aws:SourceAccount` condition, replace *`account-ID`* with the account ID that owns the subscription. If the Amazon SNS topic has multiple subscriptions from different accounts, add multiple account IDs to the `aws:SourceAccount` condition.

9. Choose **Create topic**.

   Your topic now appears in the list of topics on the **Topics** page.

Checking or resending notification confirmation email messages

When you create an anomaly detection monitor with notifications, you also create Amazon SNS notifications. For notifications to be sent, you must accept the subscription to the Amazon SNS notification topic.

To confirm that your notification subscriptions are accepted or to resend a subscription confirmation email, use the Amazon SNS console.

To check your notification status or to resend a notification confirmation email message

1. Sign in to the AWS Management Console and open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. In the navigation pane, choose **Subscriptions**.
3. Check the status of your notification. Under **Status**, `PendingConfirmation` appears if a subscription isn't accepted and confirmed.
4. (Optional) To resend a confirmation request, select the subscription with a pending confirmation and choose **Request confirmation**. Amazon SNS sends a confirmation request to the endpoints that are subscribed to the notification.

   When each owner of an endpoint receives the email, they must choose the **Confirm subscription** link to activate the notification.

Protecting your Amazon SNS anomaly detection alerts data with SSE and AWS KMS

You can use server-side encryption (SSE) to transfer sensitive data in encrypted topics. SSE protects Amazon SNS messages by using keys managed in AWS Key Management Service (AWS KMS).

To manage SSE using AWS Management Console or the AWS SDK, see Enabling Server-Side Encryption (SSE) for an Amazon SNS Topic in the *Amazon Simple Notification Service Getting Started Guide*.

To create encrypted topics using AWS CloudFormation, see the AWS CloudFormation User Guide.

SSE encrypts messages as soon as Amazon SNS receives them. The messages are stored encrypted and are decrypted using Amazon SNS only when they're sent.

Configuring AWS KMS permissions

You must configure your AWS KMS key policies before you can use server-side encryption (SSE). You can use this configuration to encrypt topics, in addition to encrypting and decrypting messages. For information about AWS KMS permissions, see AWS KMS API Permissions: Actions and Resources Reference in the *AWS Key Management Service Developer Guide*.

You can also use IAM policies to manage AWS KMS key permissions. For more information, see Using IAM Policies with AWS KMS.

> **Note**
>
> You can configure global permissions to send and receive message from Amazon SNS. However, AWS KMS requires that you name the full Amazon Resource Name (ARN) of the AWS KMS keys (KMS keys) in the specific AWS Regions. You can find this in the **Resource** section of an IAM policy.
> Ensure that the key policies of the KMS key allow the necessary permissions. To do this, name the principals that produce and consume encrypted messages in Amazon SNS as users in the KMS key policy.

To enable compatibility between AWS Cost Anomaly Detection and encrypted Amazon SNS topics

1. Create a KMS key.

2. Add one of the following policies as the KMS key policy:

    To grant the AWS Cost Anomaly Detection service access to the KMS key, use the following statement.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Service": "costalerts.amazonaws.com"
        },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
        ],
    "Resource": "*"
    }]
    }
```

    To grant the AWS Cost Anomaly Detection service access to the KMS key only when performing operations on behalf of a certain account, use the following statement.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Service": "costalerts.amazonaws.com"
        },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
        ],
     "Resource": "*",
     "Condition": {
         "StringEquals": {
            "aws:SourceAccount": [
               "account-ID"
            ]
         }
     }
    }]
}
```

> **Note**
>
> In this KMS key policy, you enter the subscription's account ID as the value for the `aws:SourceAccount` condition. This condition has AWS Cost Anomaly Detection interact with the KMS key only when performing operations for the account that owns the subscription.
> To have AWS Cost Anomaly Detection interact with the KMS key only when performing operations on behalf of a specific subscription, use the `aws:SourceArn` condition in the KMS key policy.
> For more information about these conditions, see `aws:SourceAccount` and `aws:SourceArn` in the *IAM User Guide*.

3. If you're using the KMS key policy with the `aws:SourceAccount` condition, replace *`account-ID`* with the account ID that owns the subscription. If the Amazon SNS topic has multiple subscriptions from different accounts, add multiple account IDs to the `aws:SourceAccount` condition.
4. Enable SSE for your SNS topic.

> **Note**
>
> Make sure that you're using the same KMS key that grants AWS Cost Anomaly Detection the permissions to publish to encrypted Amazon SNS topics.

5. Choose **Save Changes**.

Receiving AWS Cost Anomaly Detection alerts in Amazon Chime and Slack

You can receive your AWS Cost Anomaly Detection alerts in Amazon Chime and Slack by using AWS Chatbot.

You can use AWS Chatbot to receive AWS Cost Anomaly Detection alerts directly into your designated Slack channel or Amazon Chime chat room.

To begin receiving your anomaly alerts in Slack and Amazon Chime

1. Follow Getting started with AWS Cost Anomaly Detection to create a monitor.
2. Create an alert subscription using the `Individual alerts` type. Amazon SNS topics can be configured for `individual alerts` only.
3. Add an Amazon SNS topic as an alert recipient to a specific alert or alerts. To ensure that Cost Anomaly Detection has permissions to publish to your Amazon SNS topics, see Creating an Amazon SNS topic for anomaly notifications.
4. Attach the alert subscription to the monitor that you want to receive Slack or Amazon Chime alerts for.
5. Open the AWS Chatbot console.
6. Choose either Slack or Amazon Chime as your chat client.

To configure a Slack channel

1. Choose **Configure new channel**.
2. Enter a **Configuration name**.
3. Choose your **Slack Channel ID**.
4. In the **Permissions** section, choose a **Role setting**. Role settings determine what permissions channel members have.
   - **Channel IAM role**: This role is appropriate if channel members need the same permissions.
   - **User role**: This role is appropriate if channel members require different permissions.
5. (For Channel IAM role setting) Choose an existing IAM role for AWS Chatbot to assign or create a new IAM role.
6. Choose a **Policy template**. By default, the `Notification` permissions template is selected.
7. Choose a **Channel Guardrail**. Channel guardrails provide detailed control over what actions your channel members can take.
8. Select an **SNS topic**.

> **Note**
>
> Amazon SNS topics are scoped to specific AWS Regions. Choose the appropriate Region to see a list of Amazon SNS topics that are available in that Region.

> Your Amazon SNS topic must match the Amazon SNS topic in the **Begin receiving your anomaly alerts in Slack and Amazon Chime** process (Step 3).

9. Choose **Configure**.

To configure an Amazon Chime webhook

1. Choose **Configure a new webhook**.
2. Enter a **Configuration name**.
3. Enter a **Chime Webhook URL**. You can identify a webhook URL by following the onscreen instructions.
4. (Optional) Enter a description for your configuration.
5. In the **Permissions** section, configure an IAM role. Choose an existing IAM role, or create a new IAM role.
6. Enter a **Role name**.
7. Choose a **Policy template**. By default, the `Notification` permissions template is selected.
8. Select an **SNS topic**.

> **Note**
>
> Amazon SNS topics are scoped to specific AWS Regions. Choose the appropriate Region to see a list of Amazon SNS topics that are available in that Region.
> Your Amazon SNS topic must match the Amazon SNS topic in the **Begin receiving your anomaly alerts in Slack and Amazon Chime** process (Step 3).

9. Choose **Configure**.

Opting out of Cost Anomaly Detection

You can opt out of Cost Anomaly Detection at any time. To opt out, you need to delete all cost monitors and alert subscriptions in your account. After you opt out, Cost Anomaly Detection no longer monitors your spend patterns for anomalies. You also won't receive any further notifications.

To opt out of Cost Anomaly Detection

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. To delete any existing cost monitors:
   a. Choose the **Cost monitors** tab.
   b. Select the cost monitor that you want to delete.
   c. Choose **Delete**.
   d. In the **Delete cost monitor** dialog box, choose **Delete**.
   e. Repeat the steps for any additional cost monitors.
4. To delete any existing alert subscriptions:
   a. Choose the **Alert subscriptions** tab.
   b. Select the alert subscription that you want to delete.
   c. Choose **Delete**.
   d. In the **Delete alert subscription** dialog box, choose **Delete**.
   e. Repeat the steps for any additional alert subscriptions.

> **Note**
>
> You can also opt out of Cost Anomaly Detection by deleting your cost monitors and alert subscriptions in the Cost Explorer API. To do so, you need to use DeleteAnomalyMonitor and DeleteAnomalySubscription.

Cost Optimization Hub

Cost Optimization Hub is an AWS Billing and Cost Management feature that helps you consolidate and prioritize cost optimization recommendations across your AWS accounts and AWS Regions, so that you can get the most out of your AWS spend.

You can use Cost Optimization Hub to identify, filter, and aggregate AWS cost optimization recommendations across your AWS accounts and AWS Regions. It makes recommendations on resource rightsizing, idle resource deletion, Savings Plans, and Reserved Instances. With a single dashboard, you avoid having to go to multiple AWS products to identify cost optimization opportunities.

Cost Optimization Hub helps you quantify and aggregate estimated savings when you implement cost optimization recommendations. Cost Optimization Hub accounts for your specific commercial terms with AWS, such as Reserved Instances and Savings Plans, so you can easily compare and prioritize recommendations.

After you enable Cost Optimization Hub, you can see estimated monthly savings in AWS Compute Optimizer, consistent with the savings estimates in Cost Optimization Hub.

Cost Optimization Hub provides the following main benefits:

- Automatically identify and consolidate your AWS cost optimization opportunities.
- Quantify estimated savings that incorporate your AWS pricing and discounts.
- Aggregate and deduplicate savings across related cost optimization opportunities.
- Prioritize your cost optimization recommendations with filtering, sorting, and grouping.
- Measure and benchmark your cost efficiency.

Cost Optimization Hub provides you with a console experience and a set of API operations that you can use to view the findings of the analysis and recommendations for your resources across multiple AWS Regions. You can also view findings and recommendations across multiple accounts within your organization when you opt in the management account of an organization. The findings from the feature are also reported in the consoles of the supported services, such as the Amazon EC2 console.

Topics

- Getting started with Cost Optimization Hub
- Viewing your cost optimization opportunities
- Prioritizing your cost optimization opportunities
- Understanding cost optimization strategies
- Viewing your savings opportunities
- Understanding savings estimation and aggregation
- Supported resources

Getting started with Cost Optimization Hub

The overviews in this section describe how to get started with Cost Optimization Hub in AWS Billing and Cost Management.

When you access Cost Optimization Hub for the first time, you're asked to opt in using the account that you’re signed in with. Before you can use the feature, you must opt in. In addition, you can also opt in using the Cost Optimization Hub API, AWS Command Line Interface (AWS CLI), or SDKs.

By opting in, you authorize Cost Optimization Hub to import cost optimization recommendations generated by multiple AWS services in your account and all member accounts of your organization. These include rightsizing recommendations from AWS Compute Optimizer and Savings Plans recommendations from AWS Billing and Cost Management. These recommendations are saved in the US East (N. Virginia) Region.

In the future, AWS may expand the types of cost optimization recommendations that Cost Optimization Hub imports. AWS may also export recommendations from Cost Optimization Hub to other integrated AWS services.

Accounts supported by Cost Optimization Hub

The following AWS account types can opt in to Cost Optimization Hub:

- **Standalone AWS account**

  A standalone AWS account that doesn't have AWS Organizations enabled. For example, if you opt in to Cost Optimization Hub while signed in to a standalone account, Cost Optimization Hub identifies cost optimization opportunities and consolidates recommendations.

- **Member account of an organization**

  An AWS account that's a member of an organization. If you opt in to Cost Optimization Hub while signed in to a member account of an organization, Cost Optimization Hub identifies cost optimization opportunities and consolidates recommendations.
- **Management account of an organization**

  An AWS account that administers an organization. If you opt in to Cost Optimization Hub while signed in to a management account of an organization, Cost Optimization Hub gives you the option to opt in the management account only, or the management account and all member accounts of the organization.

  The management account can register a member account as a delegated administrator for Cost Optimization Hub. This enables the delegated administrator to see all recommendations on the management account's behalf. There can only be one delegated administrator per organization. For more information, see Delegate an administrator account.

> **Important**
>
> To opt in all member accounts for an organization, make sure that the organization has all features enabled. For more information, see Enabling All Features in Your Organization in the *AWS Organizations User Guide*.
> When you opt in using your organization's management account and include all member accounts within the organization, trusted access for Cost Optimization Hub is enabled in your organization account. For more information, see Cost Optimization Hub and AWS Organizations trusted access.

Policy to opt in to Cost Optimization Hub

The following policy statement grants you access to opt in to Cost Optimization Hub. It grants you access to create a service-linked role for Cost Optimization Hub. This role is required to opt in. For more information, see Service-linked roles for Cost Optimization Hub. It also grants access to update the enrollment status to the Cost Optimization Hub feature.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub",
            "Condition": {"StringLike": {"iam:AWSServiceName": "cost-optimization-
hub.bcm.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub"
        },
        {
            "Effect": "Allow",
            "Action": "cost-optimization-hub:UpdateEnrollmentStatus",
            "Resource": "*"
       }
    ]
}
```

There are two AWS managed policies to help get you started with Cost Optimization Hub actions. One policy provides you with read-only access to Cost Optimization Hub, and the other policy provides you with admin access. For full details, see Managed policies.

Enabling Cost Optimization Hub

To access Cost Optimization Hub, you must first enable the feature.

To enable Cost Optimization Hub

1. Sign in to the AWS Management Console and open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Optimization Hub**.
3. On the **Cost Optimization Hub** page, choose your relevant organization and member account settings:

   - **Enable Cost Optimization Hub for this account and all member accounts**: Recommendations in this account and all member accounts will be imported into Cost Optimization Hub.

- **Enable Cost Optimization Hub for this account only**: Only recommendations in this account will be imported into Cost Optimization Hub.

4. Choose **Enable**.

You can also enable Cost Optimization Hub through the **Cost Management preferences** in the console, or you can use the AWS CLI or AWS SDK.

After you enable Cost Optimization Hub, AWS starts to import cost optimization recommendations from various AWS products, such as AWS Compute Optimizer. It can take as long as 24 hours for Cost Optimization Hub to import recommendations for all supported AWS resources.

Opting in to Compute Optimizer

For Cost Optimization Hub to import recommendations from AWS Compute Optimizer, opt in to Compute Optimizer. Compute Optimizer supports standalone AWS accounts, member accounts of an organization, and the management account of an organization. For more information, see Getting started with AWS Compute Optimizer.

Accessing the console

When your setup is complete, access Cost Optimization Hub.

To access Cost Optimization Hub

1. Sign in to the AWS Management Console and open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Optimization Hub**.

Opting out of Cost Optimization Hub

You can opt out of Cost Optimization Hub at any time. However, the organization account can't opt out all member accounts. Each member needs to opt out at account level.

To opt out of Cost Optimization Hub

1. Sign in to the AWS Management Console and open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Management Preferences**.

3. In **Preferences**, choose **Cost Optimization Hub**.
4. On the **Cost Optimization Hub** tab, clear **Enable Cost Optimization Hub**.
5. Choose **Save preferences**.

Topics

- Cost Optimization Hub and AWS Organizations trusted access
- Delegate an administrator account

Cost Optimization Hub and AWS Organizations trusted access

When you opt in using your organization's management account and include all member accounts within the organization, trusted access for Cost Optimization Hub is automatically enabled in your organization account. Every time that you access recommendations for member accounts, Cost Optimization Hub verifies that trusted access is enabled in your organization account. If you disable Cost Optimization Hub trusted access after you opt in, Cost Optimization Hub denies access to recommendations for your organization's member accounts. Moreover, the member accounts within the organization aren't opted in to Cost Optimization Hub. To re-enable trusted access, opt in to Cost Optimization Hub again using your organization's management account and include all the member accounts within the organization. For more information, see Opting in your account. For more information about AWS Organizations trusted access, see Using AWS Organizations with other AWS services in the *AWS Organizations User Guide*.

Management account policy

This policy provides all the permissions necessary for a management account to opt in to Cost Optimization Hub and have full access to the service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CostOptimizationHubAdminAccess",
            "Effect": "Allow",
            "Action": [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:UpdateEnrollmentStatus",
                "cost-optimization-hub:GetPreferences",
                "cost-optimization-hub:UpdatePreferences",
                "cost-optimization-hub:GetRecommendation",
                "cost-optimization-hub:ListRecommendations",
                "cost-optimization-hub:ListRecommendationSummaries",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub"
            ],
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "cost-optimization-hub.bcm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowAWSServiceAccessForCostOptimizationHub",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "cost-optimization-hub.bcm.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Member account policy

This policy provides the permissions necessary for a member account to have full access to Cost Optimization Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CostOptimizationHubAdminAccess",
            "Effect": "Allow",
            "Action": [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:UpdateEnrollmentStatus",
                "cost-optimization-hub:GetPreferences",
                "cost-optimization-hub:UpdatePreferences",
                "cost-optimization-hub:GetRecommendation",
                "cost-optimization-hub:ListRecommendations",
                "cost-optimization-hub:ListRecommendationSummaries"
            ],
            "Resource": "*"
        }
    ]
}
```

Delegate an administrator account

You can delegate a member account in your organization as an administrator for Cost Optimization Hub. Delegating an administrator removes the need for you to use the management account to access and manage Cost Optimization Hub on behalf of the organization. This also enables you to adopt an AWS security best-practice, which recommends that you delegate responsibilities outside of the management account where possible.

A delegated administrator can perform most Cost Optimization Hub actions, including getting recommendations and setting preferences, without the need to access the management account. However, the delegated administrator cannot change the opt-in status of the management account.

The management account controls the delegated administrator option for its organization. Each organization can only have one delegated administrator for Cost Optimization Hub at a time.

To register or update an account as a delegated administrator:

Console

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Management preferences**.
3. In the **Preferences** page, choose the **Cost Optimization Hub** tab.
4. Under **Organization and member account settings**, select **Delegated administrator**.
5. Choose the account ID that you want to add as the delegated administrator.
6. Choose **Save preferences**.

CLI

1. Log in as the management account of your organization.
2. Open a terminal or command prompt window.
3. Call the following API operation. Replace `123456789012` with your account ID.

```
aws organizations register-delegated-administrator \
                   --account-id 123456789012 \
                   --service-principal cost-optimization-hub.bcm.amazonaws.com
```

To remove a member account as a delegated administrator:

Console

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Management preferences**.
3. In the **Preferences** page, choose the **Cost Optimization Hub** tab.
4. Under **Organization and member account settings**, clear **Delegated administrator**.
5. Choose **Save preferences**.

CLI

1. Log in as the management account of your organization.

2. Open a terminal or command prompt window.
3. Call the following API operation. Replace 123456789012 with your account ID.

   ```
   aws organizations deregister-delegated-administrator \
                     --account-id 123456789012 \
                     --service-principal cost-optimization-hub.bcm.amazonaws.com
   ```

Viewing your cost optimization opportunities

Cost optimization findings for your resources are displayed on the Cost Optimization Hub dashboard. You can use this dashboard to filter cost optimization opportunities and aggregate estimated savings. You can compare your total savings opportunities against your previous month's AWS spend.

Use the dashboard to group your savings opportunities by AWS account, AWS Region, resource types, and tags. View the distribution of your savings opportunities, explore the recommended actions, and identify the areas with the most savings opportunities. The dashboard is refreshed daily and all costs reflect your usage up to the previous day. For example, if today is December 2, the data includes your usage through December 1.

You can use the summary chart to filter recommendations.

Explore and narrow down the categories and recommended actions for cost optimization. To identify resources and specific actions per resource, choose **View opportunities** to go to the list of resources available for optimization. You can choose a particular recommendation, view its details, and deep link to the relevant pages in the AWS Billing and Cost Management console and AWS Compute Optimizer.

At the bottom of the dashboard, you can see your total estimated savings as a percentage of your previous month's net amortized cost. This way, you can benchmark your cost efficiency.

Topics

- Viewing the dashboard

Viewing the dashboard

Use the following procedure to view the dashboard and your cost optimization opportunities.

1. Sign in to the AWS Management Console and open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Optimization Hub**.

   By default, the dashboard displays an overview of cost optimization opportunities for AWS resources across all AWS Regions in the account that you're currently signed in to.
3. You can perform the following actions on the dashboard:

   - To view the cost optimization findings for a particular AWS Region in the account, choose the Region in the chart.
   - To view the cost optimization findings for resources in a particular account, under **Aggregate estimated savings by**, choose **AWS account**, and then choose an account ID in the chart.

     > **Note**
     >
     > Viewing cost optimization opportunities for resources in other accounts is available only if you're signed in to a management account of an organization, and you have opted in all member accounts of the organization.
   - To view cost optimization findings by resource type, under **Aggregate estimated savings by**, choose **Resource type**.
   - To view recommended actions, under **Aggregate estimated savings by**, choose **Recommended action**.
   - To filter findings on the dashboard, under **Filter**, choose from the filter options.
   - To go to the list of resources available for optimization, choose **View opportunities**.

Switching the dashboard view

The Cost Optimization Hub dashboard provides you two styles for viewing your cost optimization opportunities:

- Chart view
- Table view

You can set the style by choosing one of the views on the top right corner of the chart or table.

Prioritizing your cost optimization opportunities

In Cost Optimization Hub, you can use custom filters, sorting, and grouping, so that you can prioritize your cost optimization effort by return-on-investments.

You can continue refining your cost optimization recommendations by using the additional filters under **Chart view** or **Table view**. You can include or exclude accounts, Regions, instance types, purchase options, rightsizing options, and tags.

For example, if you want to understand which AWS accounts have the most savings opportunities for EC2 instances, you can select all accounts and set the resource type filter to **EC2 Instance**.

Choose a slice of a summary view to filter recommendations. You can also choose a particular recommendation, view its details, and deep link to the relevant pages in the Billing and Cost Management console and AWS Compute Optimizer.

At the center of the summary chart, you can see aggregated savings across all sections.

You can change to **Table view**, displaying a table for account-level estimated monthly cost savings, ordered by savings in descending order.

Understanding cost optimization strategies

Cost Optimization Hub groups your recommendations into the following cost optimization strategies:

Purchase Savings Plans

Purchase Compute, EC2 instance, and SageMaker Savings Plans.

Purchase Reserved Instances (reserved nodes)

Purchase EC2, Amazon RDS, and OpenSearch Reserved Instances; purchase Amazon Redshift and ElastiCache reserved nodes.

Stop

Stop idle or unused resources to save up to 100% of the resource cost.

Rightsize

Move to a smaller EC2 instance type of the same CPU architecture.

Upgrade

Move to a later generation product, such as moving from Amazon EBS io1 volume type to io2.

Migrate to Graviton

Move from x86 to Graviton to save costs.

The following table shows the full mapping of recommended actions and resource type.

Action	Resource type	Conditions	Implementation effort	Resource restart needed	Rollback possible
Purchase Savings Plans	Compute Savings Plans	All	Very low	No	No
	EC2 Instance Savings Plans	All	Very low	No	No
	SageMaker Savings Plans	All	Very low	No	No
Purchase Reserved Instances (reserved nodes)	EC2 Reserved Instances	All	Very low	No	Yes
	Amazon RDS Reserved Instances	All	Very low	No	No
	Amazon Redshift reserved nodes	All	Very low	No	No
	OpenSearch Reserved Instances	All	Very low	No	No

Action	Resource type	Conditions	Implementation effort	Resource restart needed	Rollback possible
	ElastiCache reserved nodes	All	Very low	No	No
Stop	EC2 instance	All	Low	No	Yes
	RDS DB instance	All	Low	Yes	Yes
Rightsize	EC2 instance (standalone)	No hypervisor change	Medium	Yes	Yes
	EC2 instance (standalone)	With hypervisor change	High	Yes	Yes
	EC2 instance (Auto Scaling group)	All	Medium	Yes	Yes
	EBS volume	All	Low	No	Yes
	Lambda function	All	Low	No	Yes
	Amazon ECS service	All	Low	Yes	Yes
	RDS DB instance	All	Medium	Yes	Yes
	RDS DB instance storage	All	Low	No	Yes

Action	Resource type	Conditions	Implementation effort	Resource restart needed	Rollback possible
Upgrade	EC2 instance (standalone)	No hypervisor change	Medium	Yes	Yes
	EC2 instance (standalone)	With hypervisor change	High	Yes	Yes
	EC2 instance (Auto Scaling group)	All	Medium	Yes	Yes
	EBS volume	All	Low	No	Yes
	RDS DB instance	All	Medium	Yes	Yes
	RDS DB instance storage	All	Low	No	Yes
Migrate to Graviton	EC2 instance (standalone)	With Graviton-compatible inferred workload type	High	Yes	Yes
	EC2 instance (standalone)	Without Graviton-compatible inferred workload type	Very high	Yes	Yes

Action	Resource type	Conditions	Implementation effort	Resource restart needed	Rollback possible
	EC2 instance (Auto Scaling group)	With Graviton-compatible inferred workload type	High	Yes	Yes
	EC2 instance (Auto Scaling group)	Without Graviton-compatible inferred workload type	Very high	Yes	Yes
	RDS DB instance	All	Medium	Yes	Yes

Viewing your savings opportunities

You can view details about your recommended actions on the **Savings opportunities** page. Use filters to refine the list of savings opportunities, and learn more about each recommendation by using a split-view panel.

You can also group related recommendations. Cost Optimization Hub identifies recommended actions that interact with each other, and it reduces estimated aggregated savings based on the degree of overlap.

Cost Optimization Hub deduplicates amongst resource optimization strategies, such as stop and rightsize, and proposes the recommendation with the highest savings. It also considers the reduction in usage by implementing the recommendations.

For example, an EC2 instance can either be stopped or rightsized, but not both. When Cost Optimization Hub estimates aggregated savings for the instance, it chooses the actions with the highest savings (in this case, stop), and ignores the savings from rightsizing.

Cost Optimization Hub also deduplicates amongst Savings Plans and Reserved Instances recommendations with parity being given to three-year or all upfront Compute Savings Plans over EC2 Instance Savings Plans or Reserved Instances.

Topics

- Viewing recommended actions and estimated savings
- Grouping related recommendations

Viewing recommended actions and estimated savings

Use the following procedure to view a recommended action and estimated savings for a specific resource ID.

1. On the **Savings opportunities** page, under **Resources with estimated savings**, choose a row in the table.

   This opens a split-view panel with a recommended action and estimated savings for your chosen resource.

   The recommended action includes the following information:

   - **Usage:** The usage based on a 14-day lookback period.
   - **Estimated cost (before discounts):** The savings estimate using AWS public (On-Demand) pricing without incorporating any discounts.
   - **Estimated other discounts:** Estimated other discounts include all discounts that are not itemized, which includes Free Tier. Itemized discounts include Savings Plans and Reserved Instances.
   - **Estimated cost (after discounts):** The savings estimate incorporating all discounts with AWS, such as Reserved Instances and Savings Plans.
   - **Estimated unused net amortized commitments:** The net amortized Savings Plans and Reserved Instances costs included in the cost of the current instance but can't be used for the recommended instance.
   - **Estimated monthly savings:** The estimated monthly savings amount for the recommendation.
   - **Estimated savings percentage:** The estimated savings percentage relative to the total cost.

2. Based on the recommended action, you can choose to view the recommendation in the AWS Billing and Cost Management console, or you can open it in AWS Compute Optimizer or the relevant console.

Grouping related recommendations

Use the following procedure to view related recommendations and their estimated savings.

1. On the **Savings opportunities** page, choose **Group related recommendations**.
2. Choose a row in the table.

   This opens a split-view panel with a choice of recommended actions for your chosen resource type.
3. Under **Recommended actions**, select one of the recommended actions.

   This updates the recommended action details on the left-hand side and the estimated savings on the right.
4. Based on the recommended action, you can choose to view the recommendation in the AWS Billing and Cost Management console, or you can open it in AWS Compute Optimizer or the relevant console.

Understanding savings estimation and aggregation

Cost Optimization Hub includes details on savings calculation, interaction among different cost optimization recommendations, savings deduplication, and savings aggregation.

Topics

- Savings estimation mode
- Estimated monthly savings
- Aggregating estimated savings

Savings estimation mode

You can customize how your estimated monthly savings are calculated. Savings estimation mode supports the following two options:

- **After discounts**: Cost Optimization Hub estimates savings incorporating all discounts with AWS, such as Reserved Instances and Savings Plans.
- **Before discounts**: Cost Optimization Hub estimates savings by using AWS public (On-Demand) pricing, without incorporating any discounts.

To customize how estimated monthly savings are calculated

1. Sign in to the AWS Management Console and open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Management preferences**.
3. In the **Preferences page**, choose the **Cost Optimization Hub** tab.
4. Under **Savings estimation mode**, choose **After discounts** or **Before discounts**.
5. Choose **Save preferences**.

Estimated monthly savings

Cost Optimization Hub analyzes specific pricing discounts to provide you with a measure of your cost efficiency. This is done by dividing the aggregated estimated monthly savings of your cost optimization opportunities by your amortized monthly AWS costs, exclusive of credits and refunds.

For recommendations associated with a resource, estimated monthly cost impact is an estimation of how much your AWS bill will change over a 730-hour period (365 * 24 /12). This estimate excludes the periods when the resources were not running and if you had implemented the recommended action 730 hours ago. If the recommendation has a different lookback period, the cost impact is normalized to a 730-hour period, which is the average number of hours per month.

Note that your estimated monthly savings is a quick approximation of future savings. The actual savings that you realize is dependent on your future AWS usage patterns.

Aggregating estimated savings

Cost Optimization Hub aggregates AWS cost optimization recommendations for you across your AWS accounts and AWS Regions. For example, it makes recommendations on resource rightsizing, idle resource deletion, Savings Plans, and Reserved Instances.

You can aggregate estimated savings by the following categories:

- AWS account
- AWS Region
- Resource type
- Recommended action
- Implementation effort
- Is resource restart needed
- Is rollback possible
- Tag key

To aggregate your cost optimization recommendations

1. Sign in to the AWS Management Console and open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/home.
2. In the navigation pane, choose **Cost Optimization Hub**.
3. Choose to view your savings opportunities in **Chart view** or **Table view**.
4. Choose **Aggregate estimated savings by**, and then choose a category.

Supported resources

Cost Optimization Hub generates recommendations for the following resources:

- Amazon Elastic Compute Cloud (Amazon EC2) instances
- Amazon EC2 Auto Scaling groups
- Amazon Elastic Block Store (Amazon EBS) volumes
- AWS Lambda functions
- Amazon Elastic Container Service (Amazon ECS) tasks on AWS Fargate
- Compute Savings Plans
- EC2 Instance Savings Plans
- SageMaker Savings Plans
- EC2 Reserved Instances
- Amazon RDS Reserved Instances
- OpenSearch Reserved Instances

- Amazon Redshift reserved nodes
- ElastiCache reserved nodes
- Amazon RDS DB instances
- Amazon RDS DB instance storage

Optimizing your cost with Rightsizing Recommendations

The rightsizing recommendations feature in Cost Explorer helps you identify cost-saving opportunities by downsizing or terminating instances in Amazon Elastic Compute Cloud (Amazon EC2). Rightsizing recommendations analyze your Amazon EC2 resources and usage to show opportunities for how you can lower your spending. You can see all of your underutilized Amazon EC2 instances across member accounts in a single view to immediately identify how much you can save. After you identify your recommendations, you can take action on the Amazon EC2 console.

Note

We recommend that you use Cost Optimization Hub to identify cost optimization opportunities. For full details, see Cost Optimization Hub.

Topics

- Getting started with rightsizing recommendations
- Using your rightsizing recommendations
- CSV details
- Understanding your rightsizing recommendations calculations
- Understanding your reservations with Cost Explorer
- Accessing Reserved Instance Recommendations

Getting started with rightsizing recommendations

You can access your reservation recommendations and resource-based recommendations on the Cost Explorer console. After you enable the feature, it can take up to 24 hours to generate your recommendations.

To access rightsizing recommendations

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Rightsizing recommendations**.

To enable rightsizing recommendations

1. Open the AWS Cost Management at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, choose **Cost Management Preferences**.
3. On the **Preferences** page, under **Rightsizing** in the **General** tab, select **Enable Rightsizing recommendations**.
4. Choose **Save preferences**.

> **Note**
>
> Only regular or a management account can enable rightsizing recommendations. After you enable the feature, both member and management account can access rightsizing recommendations unless the management account specifically prohibits member account access on the **settings** page.
> To improve the recommendation quality, AWS might use your published utilization metrics, such as disk or memory utilization, to improve our recommendation models and algorithms. All metrics are anonymized and aggregated before AWS uses them for model training. If you want to opt out of this experience and request that your metrics not be stored and used for model improvement, contact AWS Support. For more information, see AWS Service Terms.

Using your rightsizing recommendations

You can see the following top-level key performance indicators (KPIs) in your rightsizing recommendations:

- **Optimization opportunities** – The number of recommendations available based on your resources and usage
- **Estimated monthly savings** – The sum of the projected monthly savings associated with each of the recommendations provided
- **Estimated savings (%)** – The available savings relative to the direct instance costs (On-Demand) associated with the instances in the recommendation list

To filter your rightsizing recommendations

1. Open the AWS Cost Management at https://console.aws.amazon.com/cost-management/home.
2. In the left navigation pane, choose **Rightsizing recommendations**.
3. At the top of the **Rightsizing Recommendations** page, filter your recommendations by selecting any or all of the following check boxes:
    - Idle instances (termination recommendations)
    - Underutilized instances
    - Include Savings Plans and Reserved Instances (option to consider existing Savings Plans or RI coverage in recommendation savings calculations)
    - Generate recommendations (option to generate recommendations within the instance family, or across multiple instance families)
4. Above the **Findings** table, use the search bar to filter by the following parameters:
    - Account ID (option available from the management account)
    - Region
    - Cost allocation tag

To view your rightsizing recommendations details

1. Open the AWS Cost Management at https://console.aws.amazon.com/cost-management/home.
2. In the left navigation pane, choose **Rightsizing recommendations**.
3. Choose **View**.

    The **View** button on the right of each recommendation opens a window that provides details on the instances and recommended actions.

To download your recommendations in CSV format

1. Choose **Launch Cost Explorer**.
2. In the left navigation pane, choose **Recommendations**.
3. Select **Download CSV**.

For definitions for the CSV file fields, see CSV details.

Enhancing your recommendations using CloudWatch metrics

We can examine your memory utilization if you enable your Amazon CloudWatch agent.

To enable memory utilization, see Installing the CloudWatch Agent.

> ⚠ **Important**
>
> When you create a CloudWatch configuration file, use the default namespace and default names for the collected metrics.
> For **InstanceID**, choose `append_Dimension`. Do not add additional dimensions for individual memory or disk metrics. Disk utilization is currently not examined.
> For Linux instances, choose `mem_used_percent` as your metric for your CloudWatch agent to collect. For Windows instances, choose `"% Committed Bytes In Use"`.

For more information about the CloudWatch agent, see Collecting Metrics and Logs from Amazon EC2 Instances and On-Premises Servers with the CloudWatch Agent in the *Amazon CloudWatch User Guide*.

CSV details

The following is a list of fields in the downloadable CSV form from the **Rightsizing Recommendations** page. The fields are repeated if there are multiple rightsizing options available. The file also contains all of your relevant cost allocation tags.

- **Account ID –** The AWS account ID that owns the instance that the recommendation is based off of.
- **Account Name –** The name of the account that owns the instance that the recommendation is based off of.
- **Instance ID –** The unique instance identifier.
- **Instance Name –** The name you've given to the instance.
- **Instance Type –** The instance family and size of the original instance.
- **Instance Name –** The name you've given an instance. This field will show as blank if you haven't given the instance a name.

- **OS –** The operating system or platform of the current instance.
- **Region –** The AWS Region that the instance is running in.
- **Running Hours –** The total number of running hours of the instance over the last 14 days.
- **RI Hours –** The subset of the total running hours that are covered by an AWS reservation over the look-back period.
- **OD Hours –** The subset of the total running hours that are On-Demand over the look-back period.
- **SP Hours –** The subset of the total running hours that are covered by Savings Plans over the look-back period.
- **CPU Utilization –** The maximum CPU utilization of the instance over the look-back period.
- **Memory Utilization –** The maximum memory utilization of the instance over the look-back period (if available from the Amazon CloudWatch agent).
- **Disk Utilization –** The maximum disk utilization of the instance over the look-back period (if available from the CloudWatch agent - currently not supported).
- **Network Capacity –** The maximum network input/output operations per second capacity of the current instance. This isn't a measure of actual instance use or performance, only capacity. It's not considered in the recommendation.
- **EBS Read Throughput –** The maximum number of read operations per second.
- **EBS Write Throughput –** The maximum number of write operations per second.
- **EBS Read Bandwidth –** The maximum volume of read KiB per second.
- **EBS Write Bandwidth –** The maximum volume of write KiB per second.
- **Recommended Action –** The recommended action, either modify or terminate the instance.
- **Recommended Instance Type 1 –** The instance family and size of the recommended instance type. For termination recommendations, this field is empty.
- **Recommended Instance Type 1 Estimated Saving –** The projected savings based on the recommended action, instance type, associated rates, and your current Reserved Instance (RI) portfolio.
- **Recommended Instance Type 1 Projected CPU –** The projected value of the CPU utilization based on utilization of current instance CPU and recommended instance specifications.
- **Recommended Instance Type 1 Projected Memory –** The projected value of the memory utilization based on utilization of current instance memory and recommended instance specifications.

- **Recommended Instance Type 1 Projected Disk –** The projected value of the disk utilization based on utilization of current instance disk and recommended instance specifications.
- **Recommended Instance Type 1 Network Capacity –** The maximum network input/output operations per second capacity of the recommended instance. This isn't a measure of actual instance use or performance, only capacity. It's not considered in the recommendation.

Understanding your rightsizing recommendations calculations

This section provides an overview of the savings calculations that are used in your rightsizing recommendations algorithms.

Consolidated billing family

To identify all instances for all accounts in the consolidated billing family, rightsizing recommendations look at the usage for the last 14 days for each account. If the instance was stopped or terminated, we remove it from consideration. For all remaining instances, we call CloudWatch to get maximum CPU utilization data, memory utilization (if enabled), network in/out, local disk input/ output (I/O), and performance of attached EBS volumes for the last 14 days. This is to produce conservative recommendations, not to recommend instance modifications that could be detrimental to application performance or that could unexpectedly impact your performance.

Determining if an instance is idle, underutilized, or neither

We look at the maximum CPU utilization of the instance for the last 14 days to make one of the following assessments:

- **Idle –** If the maximum CPU utilization is at or below 1%. A termination recommendation is generated, and savings are calculated. For more information, see Savings calculation.
- **Underutilized –** If the maximum CPU utilization is above 1% and cost savings are available in modifying the instance type, a modification recommendation is generated.

If the instance isn't idle or underutilized, we don't generate any recommendations.

Generating modification recommendations

Recommendations use a machine learning engine to identify the optimal Amazon EC2 instance types for a particular workload. Instance types include those that are a part of AWS Auto Scaling groups.

The recommendations engine analyzes the configuration and resource usage of a workload to identify dozens of defining characteristics. For example, it can determine whether a workload is CPU-intensive or whether it exhibits a daily pattern. The recommendations engine analyzes these characteristics and identifies the hardware resources that the workload requires.

Finally, it concludes how the workload would perform on various Amazon EC2 instances to make recommendations for the optimal AWS compute resources that the specific workload.

Savings calculation

We first examine the instance running in the last 14 days to identify whether it was partially or fully covered by an RI or Savings Plans, or running On-Demand. Another factor is whether the RI is size-flexible. The cost to run the instance is calculated based on the On-Demand hours and the rate of the instance type.

For each recommendation, we calculate the cost to operate a new instance. We assume that a size-flexible RI covers the new instance in the same way as the previous instance if the new instance is within the same instance family. Estimated savings are calculated based on the number of On-Demand running hours and the difference in On-Demand rates. If the RI isn't size-flexible, or if the new instance is in a different instance family, the estimated savings calculation is based on whether the new instance had been running during the last 14 days as On-Demand.

Cost Explorer only provides recommendations with an estimated savings greater than or equal to $0. These recommendations are a subset of Compute Optimizer results. For more performance-based recommendations that might result in a cost increase, see Compute Optimizer.

You can choose to view saving with or without consideration for RI or Savings Plans discounts. Recommendations consider both discounts by default. Considering RI or Savings Plans discounts might result in some recommendations showing a savings value of $0. To change this option, see Using your rightsizing recommendations.

Note

Rightsizing recommendations doesn't capture second-order effects of rightsizing, such as the resulting RI hour’s availability and how they will apply to other instances. Potential savings based on reallocation of the RI hours aren't included in the calculation.

Understanding your reservations with Cost Explorer

Balancing your Reserved Instance (RI) usage and your On-Demand Instance usage can help you achieve better efficiency. To help, Cost Explorer provides tools that help you understand where your greatest RI costs are and how you can potentially lower your costs. Cost Explorer provides you with an overview of your current reservations, shows your RI utilization and coverage, and calculates recommended Reserved Instances (RIs) that could save you money if you purchase them.

Using your RI reports

You can use the **RI reports** page in the Cost Explorer console to see how many reservations you have, how much your reservations are saving you compared to similar usage of On-Demand Instances, and how many of your reservations are expiring this month.

Cost Explorer breaks down your reservations and savings by service and lists your potential savings: that is, the costs of On-Demand usage compared to what that usage could cost you with an RI.

To use your potential savings, see Accessing Reserved Instance Recommendations.

Managing your reservation expiration alerts

You can track your reservations and when your reservations expire in Cost Explorer. With reservation expiration alerts, you can receive email alerts 7, 30, or 60 days in advance before your reservation expires. These alerts can be sent to up to 10 email recipients. You can also choose to be notified on the day that your reservation expires. Reservation expiration alerts are supported for Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon OpenSearch Service reservations.

To turn on reservation expiration alerts

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. Navigate to the **Overview** page under the **Reservations** section.
3. Choose **Manage alert subscriptions** in the upper right corner.
4. Select the check boxes for when you want to receive your alerts.
5. Enter email addresses for who you want to notify. You can have up to 10 email recipients.
6. Choose **Save**.

AWS starts monitoring your reservation portfolio and sends alerts based on the preferences that you specify.

Accessing Reserved Instance Recommendations

If you enable Cost Explorer, you automatically get Amazon EC2, Amazon RDS, ElastiCache, OpenSearch Service, Amazon Redshift, and Amazon MemoryDB Reserved Instance (RI) purchase recommendations that could help you reduce your costs. RIs provide a discounted hourly rate (up to 75%) compared to On-Demand pricing. Cost Explorer generates your RI recommendations using the following process:

- Identifies your On-Demand Instance usage for a service during a specific time period
- Collects your usage into categories that are eligible for an RI
- Simulates every combination of RIs in each category of usage
- Identifies the best number of each type of RI to purchase to maximize your estimated savings

For example, Cost Explorer automatically aggregates your Amazon EC2 Linux, shared tenancy, and c4 family usage in the US West (Oregon) Region and recommends that you buy size-flexible regional RIs to apply to the c4 family usage. Cost Explorer recommends the smallest size instance in an instance family. This makes it easier to purchase a size-flexible RI. Cost Explorer also shows the equal number of normalized units so that you can purchase any instance size that you want. For this example, your RI recommendation would be for `c4.large` because that is the smallest size instance in the c4 instance family.

Cost Explorer recommendations are based on a single account or organization usage of the past seven, 30, or 60 days. Cost Explorer uses On-Demand instance usage during the selected look-back period to generate recommendations. All other usage in the look-back period that are covered by features such as RI, SPOT, and Savings Plans aren't included. Amazon EC2, ElastiCache, OpenSearch Service, Amazon Redshift, and Amazon MemoryDB recommendations are for RIs scoped to Region, not Availability Zones, and your estimated savings reflects the application of those RIs to your usage. Amazon RDS recommendations are scoped to either Single-AZ or Multi-AZ RIs. Cost Explorer updates your recommendations at least once every 24 hours.

> **Note**
>
> Cost Explorer doesn't forecast your usage or take forecasts into account when recommending RIs. Instead, Cost Explorer assumes that your historical usage reflects your future usage when determining which RIs to recommend.

Linked accounts can see recommendations only if they have the relevant permissions. Linked accounts need permissions to view Cost Explorer and permissions to view recommendations. For more information, see Viewing the Cost Explorer Reservation Recommendations.

Topics

- RI Recommendations for Size-Flexible RIs
- Viewing the Cost Explorer Reservation Recommendations
- Reading the Cost Explorer RI Recommendations
- Modifying Your RI Recommendations
- Saving Your RI Recommendations
- Using Your RI Recommendations

RI Recommendations for Size-Flexible RIs

Cost Explorer also considers the benefits of size-flexible regional RIs when generating your RI purchase recommendations. Size-flexible regional RIs help maximize your estimated savings across eligible instance families in your recommendations. AWS uses the concept of normalized units to compare the various sizes within an instance family. Cost Explorer uses the smallest normalization factor to represent the instance type that it recommends. For more information, see Instance Size Flexibility for EC2 Reserved Instances.

For example, let’s say you own an EC2 RI for a `c4.8xlarge`. This RI applies to any usage of a `Linux/Unix c4` instance with shared tenancy in the same region as the RI, such as the following instances:

- One `c4.8xlarge` instance
- Two `c4.4xlarge` instances
- Four `c4.2xlarge` instances
- Sixteen `c4.large` instances

It also includes combinations of EC2 usage, such as one `c4.4xlarge` and eight `c4.large` instances.

If you own an RI that is smaller than the instance that you're running, you are charged the prorated, On-Demand price for the excess. This means that you could buy an RI for a `c4.4xlarge`, use a `c4.4xlarge` instance most of the time, but occasionally scale up to a `c4.8xlarge` instance. Some of your `c4.8xlarge` usage is covered by the purchased RI, and the rest is charged at On-Demand prices. For more information, see How Reserved Instances Are Applied in the *Amazon Elastic Compute Cloud User Guide*.

Viewing the Cost Explorer Reservation Recommendations

Linked accounts need the following permissions to view recommendations:

- `ViewBilling`
- `ViewAccount`

For more information, see Using identity-based policies (IAM policies) for AWS Cost Management.

To view your RI recommendations

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. In the navigation pane, under **Reservations**, choose **Recommendations**.
3. For **Select recommendation type**, choose the service that you want recommendations for.

Reading the Cost Explorer RI Recommendations

The RI recommendation page shows you your estimated potential savings, your RI purchase recommendations, and the parameters that Cost Explorer used to create your recommendations. You can change the parameters to get recommendations that might match your use case more closely.

The top of the RI recommendations page show you three numbers:

- **Estimated Annual Savings** – Your **Estimated Annual Savings** is how much Cost Explorer calculates that you could save by purchasing all the recommended RIs.

- **Savings vs. On-Demand** – Your **Savings vs. On-Demand** is your estimated savings as a percentage of your current costs.
- **Purchase Recommendations** – Your **Purchase Recommendations** is how many different RI purchase options that Cost Explorer found for you.

These numbers enable you to see a rough estimate of how much you could potentially save by buying more RIs. You can recalculate these numbers for a different use case by using the parameters in the pane on the right. The pane allows you to change the following parameters:

- **RI term** – The length of the RI reservation that you want recommendations for.
- **Offering class** – Whether you want recommendations for a standard RI or a convertible RI.
- **Payment option** – Whether you want to pay for recommended RIs upfront.
- **Based on the past** – How many days of your previous instance usage that you want your recommendations to take into account.

At the bottom of the page are tabs with some of your savings estimates. The **All accounts** tab enables you to see the recommendations based on the combined usage across your entire organization, and the **Individual accounts** tab enables you to see recommendations that Cost Explorer generated on a per-linked-account basis. The table on each tab shows the different purchase recommendations and details about the recommendations. If you want to see the usage that Cost Explorer based a recommendation on, choose the **View associated usage** link in the recommendation details. This takes you to a report that shows the exact parameters that Cost Explorer used to generate your recommendation. The report also shows your costs and associated usage grouped by **Purchase option**, so that you can view the On-Demand Instance usage that your recommendation is based on.

> **Note**
>
> Recommendations that Cost Explorer bases on an individual linked account consider all usage by that linked account, including any RIs used by that linked account. This includes RIs shared by another linked account. The recommendations don't assume that an RI will be shared with the linked account in the future.

You can sort your recommendations by **Monthly estimated savings**, **Upfront RI cost**, **Purchase recommendation**, or **Instance type**.

Modifying Your RI Recommendations

You can change the information that Cost Explorer uses when it creates your recommendations, and you can also change the types of recommendations that you want. This allows you to see recommendations for the RIs that work best for you, such as All UpFront RIs with a one-year term, based on your last 30 days of usage.

> **Note**
>
> Instead of forecasting your future usage, Cost Explorer assumes that your future usage is the same as your previous usage. Cost Explorer also assumes that you are renewing any expiring RIs.

To modify your RI recommendations

1. Sign in to the AWS Management Console and open the AWS Cost Management console at https://console.aws.amazon.com/cost-management/home.
2. On the navigation bar, choose the menu, choose **RI Recommendations** and then under **Select a service** choose the service that you want to modify the recommendations for.
3. In the **RI Recommendation Parameters** pane, change the parameters that you want to change. Your estimated savings update automatically.

   a. For **RI term**, select the RI term that you want.

   b. For **Offering class**, select the RI class that you want.

   c. For **Payment option**, select the purchase option that you want.

   d. For **Recommendation type**, select the logic that you want your recommendations based on.

   e. For **Based on the past**, select how many days of usage that you want your RI recommendations to be based on.
4. Choose either **All accounts** or **Individual accounts** to see recommendations based either on your organization-wide usage or on all of your linked accounts based on their individual account usage.

Saving Your RI Recommendations

You can save your RI recommendations as a CSV file.

To save your RI recommendations

1. On the **Reserved Instance Recommendations** page, in the RI parameter pane, change any parameters that you want to change. Your estimated savings update automatically.
2. Above the recommendation table, choose **Download CSV**.

The CSV file contains the following columns.

RI Recommendation CSV Columns

Column Name	Service	Column Explanation
Account ID	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The account associated with your recommendation.
Availability zone	Amazon RDS	The availability zone of the instances used to generate a recommendation.
Average hourly normalized unit usage in historical period	Amazon EC2, RDS, MemoryDB	The average number of normalized units used per hour over the period chosen for generating recommendations.
Average hourly usage in historical period	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The average number of instance hours used per hour over the period chosen for generating recommendations.

Column Name	Service	Column Explanation
Break even months	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The estimated length of time before you recoup your upfront costs for this set of recommended reservations.
Cache engine	Amazon ElastiCache	The kind of engine that the recommended ElastiCache reserved node runs, such as Redis or Memcheched.
Database edition	Amazon RDS	The edition of the database engine that the recommended RDS reserved instance runs.
Database engine	Amazon RDS	The kind of engine that the recommended RDS RI runs, such as Aurora MySQL or MariaDB.
Deployment option	Amazon RDS	Whether your RI is for an RDS instance in a single Availability Zone or an RDS instance with a backup in another Availability Zone.
Estimated savings	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The estimated savings of the recommended reservations.

Column Name	Service	Column Explanation
Expected utilization	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	How much of the recommended RI Cost Explorer estimates you will use.
Instance type	Amazon EC2, RDS, OpenSearch Service	The type of instance that the recommendation is generated for (for example, `m4.large` or `t2.nano`). For size-flexible recommendations, Cost Explorer aggregates all usage in a organization (for example, the m4 family) and shows a recommendation for the smallest instance type RI that is available for purchase (for example, `m4.large`).
Max hourly normalized unit usage in historical period	Amazon EC2, RDS, MemoryDB	The maximum number of normalized units used in an hour over the period chosen for generating recommendations.
Max hourly usage in historical period	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The maximum number of instance hours used in an hour over the period chosen for generating recommendations.
Min hourly normalized unit usage in historical period	Amazon EC2, RDS, MemoryDB	The minimum number of normalized units used in an hour over the period chosen for generating recommendations.

Column Name	Service	Column Explanation
Min hourly usage in historical period	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The minimum number of instance hours used in an hour over the period chosen for generating recommendations.
Node type	Amazon ElastiCache, Redshift, MemoryDB	The type of node that the recommendation is generated for, such as `ds2.xlarge` .
Normalized hours to purchase	Amazon EC2, RDS, MemoryDB	How many normalized units that Cost Explorer recommends that you buy.
Number of instances to purchase	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	How many reservations Cost Explorer recommends that you buy.
Offering class	Amazon EC2	The offering class associated with your recommendation.
Payment option	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The recommended payment option for the recommendation.
Platform	Amazon EC2	The operating system and license model for the recommended RI instance type.

Column Name	Service	Column Explanation
Recommendation date	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The date that Cost Explorer generated your recommendation.
Recurring monthly cost	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The recurring monthly cost of the recommended reservations.
Region	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The region of the instances used to generate a recommendation. You must purchase the recommended RIs in the recommended region to see potential savings.
Size flexible	Amazon EC2, RDS, MemoryDB	Whether a recommended RI is size-flexible.
Tenancy	Amazon EC2	The tenancy for the recommended RI purchase. Valid values are **shared** or **dedicated**.
Term	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The recommended term length for the recommendation.

Using Your RI Recommendations

To purchase the recommended reservations, go to the purchase page on a service console. You can also save a CSV file of your recommendations and purchase the reservations at a later date.

To use Amazon Elastic Compute Cloud recommendations

1. On the **Reserved Instance Recommendations** page, choose Amazon EC2 RI Purchase Console to go to the Amazon EC2 Purchase Console.
2. Purchase your RIs by following the instructions at Buying Reserved Instances in the *Amazon EC2 User Guide*.

To use Amazon Relational Database Service recommendations

1. On the **Reserved instances** page in the Amazon RDS console, choose **Purchase Reserved DB Instance**.
2. Purchase your reservations by following the instructions at Working with reserved DB instances in the *Amazon RDS User Guide*.

To use Amazon Redshift recommendations

1. On the **Reserved nodes** page in the Amazon Redshift console, choose **Purchase reserved nodes**.
2. Purchase your reservations by following the instructions at Purchasing a reserved node offering with the Amazon Redshift console in the *Amazon Redshift Management Guide*.

To use Amazon OpenSearch Service recommendations

1. On the **Reserved Instance Leases** page in the OpenSearch Service console, choose **Order Reserved Instance**.
2. Purchase your reservations by following the instructions at Reserved Instances in Amazon OpenSearch Service in the *Amazon OpenSearch Service Developer Guide*.

To use Amazon ElastiCache recommendations

1. On the **Reserved Nodes** page in the ElastiCache console, choose **Purchase reserved nodes**.

2. Purchase your reservations by following the instructions at Purchasing a Reserved Node in the *Amazon ElastiCache User Guide*.

To use Amazon MemoryDB recommendations

1. On the **Reserved nodes** page in the MemoryDB console, choose **Purchase reserved nodes**.
2. Purchase your reservations by following the instructions at Working with reserved nodes in the *Amazon MemoryDB Developer Guide*.

Manage your costs with Savings Plans

Savings Plans offers a flexible pricing model that provides savings on AWS usage. Savings Plans provide savings beyond On-Demand rates in exchange for a commitment of using a specified amount of compute power (measured every hour) for a one or three year period. You can manage your plans by using recommendations, performance reporting, and budget alerts in AWS Cost Explorer.

For more information, see What is Savings Plans in the *Savings Plans User Guide*.

Security in AWS Cost Management

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to AWS Cost Management, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Billing and Cost Management. The following topics show you how to configure Billing and Cost Management to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Billing and Cost Management resources.

Topics

- Data protection in AWS Cost Management
- Identity and Access Management for AWS Cost Management
- Logging and monitoring in AWS Cost Management
- Compliance validation for AWS Cost Management
- Resilience in AWS Cost Management
- Infrastructure security in AWS Cost Management

Data protection in AWS Cost Management

The AWS shared responsibility model applies to data protection in AWS Cost Management. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with AWS Cost Management or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Identity and Access Management for AWS Cost Management

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use AWS Cost Management resources. IAM is an AWS service that you can use with no additional charge.

Topics

- User types and billing permissions
- Audience
- Authenticating with identities
- Managing access using policies
- Overview of managing access permissions
- How AWS Cost Management works with IAM
- Identity-based policy examples for AWS Cost Management
- Using identity-based policies (IAM policies) for AWS Cost Management
- AWS Cost Management policy examples
- Migrating access control for AWS Cost Management
- Cross-service confused deputy prevention
- Troubleshooting AWS Cost Management identity and access
- Service-linked roles for AWS Cost Management
- Using service-linked roles

User types and billing permissions

This table summarizes the default actions that are permitted in AWS Cost Management for each type of billing user.

User types and billing permissions

User type	Description	Billing permissions
Account owner	The person or entity in whose name your account is set up as.	• Has full control of all Billing and Cost Management resources.

User type	Description	Billing permissions
		- Receives a monthly invoice of AWS charges.
User	A person or application defined as a user in an account by an account owner or administrative user. Accounts can contain multiple users.	- Has permissions explicitly granted to the user or a group that includes the user. - Can be granted permission to view Billing and Cost Management console pages. For more information, see Overview of managing access permissions. - Can't close accounts.
Organization management account owner	The person or entity associated with an AWS Organizations management account. The management account pays for AWS usage that is incurred by a member account in an organization.	- Has full control of all Billing and Cost Management resources for the management account only. - Receives a monthly invoice of AWS charges for the management account and member accounts. - Views the activity of member accounts in the billing reports for the management account.

User type	Description	Billing permissions
Organization member account owner	The person or entity associated with an AWS Organizations member account. The management account pays for AWS usage that is incurred by a member account in an organization.	• Doesn't have permission to review any usage reports or account activity except for its own. Doesn't have access to usage reports or account activity for other member accounts in the organization or for the management account. • Doesn't have permission to view billing reports. • Has permission to update account information only for its own account. Can't access other member accounts or the management account.

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in AWS Cost Management.

Service user – If you use the AWS Cost Management service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more AWS Cost Management features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in AWS Cost Management, see Troubleshooting AWS Cost Management identity and access.

Service administrator – If you're in charge of AWS Cost Management resources at your company, you probably have full access to AWS Cost Management. It's your job to determine which AWS Cost Management features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with AWS Cost Management, see How AWS Cost Management works with IAM.

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to AWS Cost Management. To view example AWS Cost Management identity-based policies that you can use in IAM, see Identity-based policy examples for AWS Cost Management.

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see Signing AWS API requests in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Multi-factor authentication in the *AWS IAM Identity Center User Guide* and Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access AWS services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the AWS Directory Service, the Identity Center directory, or any user that accesses AWS services by using credentials provided through an identity source. When federated identities access AWS accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use AWS IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your AWS accounts and applications. For information about IAM Identity Center, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the *IAM User Guide*.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Creating a role for a third-party Identity Provider in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the

  principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.

  - **Service role –** A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.
  - **Service-linked role –** A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

- **Applications running on Amazon EC2 –** You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM role to grant permissions to applications running on Amazon EC2 instances in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see When to create an IAM role (instead of a user) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access control list (ACL) overview in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries –** A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs) –** SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see Service control policies in the *AWS Organizations User Guide*.
- **Session policies –** Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

Overview of managing access permissions

Granting access to your billing information and tools

The AWS account owner can access billing information and tools by signing in to the AWS Management Console using the account credentials. We recommend that you don't use the account credentials for everyday access to the account, and especially that you don't share account credentials with others to give them access to your account.

For your daily administrative tasks, create an administrative user to securely control access to AWS resources. By default, users don't have access to the AWS Cost Management console. As an administrator, you can create roles under your AWS account that your users can assume. After you create roles, you can attach your IAM policy to them, based on the access needed. For example, you can grant some users limited access to some of your billing information and tools, and grant others complete access to all of the information and tools.

> **Note**
>
> IAM is a feature of your AWS account. If you are already signed up for a product that is integrated with IAM, you don't need to do anything else to sign up for IAM, nor will you be charged for using it.
> Permissions for Cost Explorer apply to all accounts and member accounts, regardless of IAM policies. For more information about Cost Explorer access, see Controlling access to Cost Explorer.

Activating access to the Billing and Cost Management console

IAM roles within an AWS account can't access the Billing and Cost Management console pages by default. This is true even if the role has IAM policies that grant access to certain Billing and Cost Management features. The AWS account administrator can allow roles access to Billing and Cost Management console pages by using the **Activate IAM Access** setting.

On the AWS Cost Management console, the **Activate IAM Access** setting controls access to the following pages:

- Home
- Cost Explorer
- Reports
- Rightsizing recommendations
- Savings Plans recommendations
- Savings Plans utilization report
- Savings Plans coverage report
- Reservations overview
- Reservations recommendations
- Reservations utilization report
- Reservations coverage report
- Preferences

For a list of pages the **Activate IAM Access** setting controls for the Billing console, see Activating access to the Billing console in the *Billing User Guide*.

⚠ **Important**

Activating IAM access alone doesn't grant roles the necessary permissions for these Billing and Cost Management console pages. In addition to activating IAM access, you must also attach the required IAM policies to those roles. For more information, see Using identity-based policies (IAM policies) for AWS Cost Management.

The **Activate IAM Access** setting doesn't control access to the following pages and resources:

- The console pages for AWS Cost Anomaly Detection, Savings Plans overview, Savings Plans inventory, Purchase Savings Plans, and Savings Plans cart
- The Cost Management view in the AWS Console Mobile Application
- The Billing and Cost Management SDK APIs (AWS Cost Explorer, AWS Budgets, and AWS Cost and Usage Reports APIs)
- AWS Systems Manager Application Manager

By default, the **Activate IAM Access** setting is deactivated. To activate this setting, you must log in to your AWS account using the root user credentials, and then select the setting in the **Account** page. Activate this setting in each account where you want to allow IAM role access to the Billing and Cost Management console pages. If you use AWS Organizations, then activate this setting in each management or member account where you want to allow IAM role access to the console pages.

> **Note**
>
> The **Activate IAM Access** setting isn't available to users with administrator access. This setting is available only to the root user of the account.

If the **Activate IAM Access** setting is deactivated, then IAM roles in the account can't access the Billing and Cost Management console pages. This is true even if they have administrator access or the required IAM policies.

To activate IAM user and role access to the Billing and Cost Management console

1. Sign in to the AWS Management Console with your root account credentials (specifically, the email address and password that you used to create your AWS account).
2. On the navigation bar, choose your account name, and then choose My Account.
3. Next to **IAM User and Role Access to Billing Information**, choose **Edit**.
4. Select the **Activate IAM Access** check box to activate access to the Billing and Cost Management console pages.
5. Choose **Update**.

After you activate IAM access, you must also attach the required IAM policies to the IAM roles. The IAM policies can grant or deny access to specific Billing and Cost Management features. For more information, see Using identity-based policies (IAM policies) for AWS Cost Management.

How AWS Cost Management works with IAM

AWS Cost Management integrates with the AWS Identity and Access Management (IAM) service so that you can control who in your organization has access to specific pages on the AWS Cost Management console. You can control access to invoices and detailed information about charges and account activity, budgets, payment methods, and credits.

For more information about how to activate access to the Billing and Cost Management Console, see Tutorial: Delegate Access to the Billing Console in the *IAM User Guide*.

Before you use IAM to manage access to AWS Cost Management, learn what IAM features are available to use with AWS Cost Management.

IAM features you can use with AWS Cost Management

IAM feature	AWS Cost Management support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Partial
Policy condition keys	Yes
ACLs	No
ABAC (tags in policies)	Partial
Temporary credentials	Yes
Forward access sessions (FAS)	Yes
Service roles	Yes
Service-linked roles	No

To get a high-level view of how AWS Cost Management and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for AWS Cost Management

Supports identity-based policies: Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Identity-based policy examples for AWS Cost Management

To view examples of AWS Cost Management identity-based policies, see Identity-based policy examples for AWS Cost Management.

Resource-based policies within AWS Cost Management

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different AWS accounts, an IAM administrator in the trusted account must also grant the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for AWS Cost Management

Supports policy actions: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

To see a list of AWS Cost Management actions, see Actions defined by AWS Cost Management in the *Service Authorization Reference*.

Policy actions in AWS Cost Management use the following prefix before the action:

```
ce
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "ce:action1",
      "ce:action2"
         ]
```

To view examples of AWS Cost Management identity-based policies, see Identity-based policy examples for AWS Cost Management.

Policy resources for AWS Cost Management

Supports policy resources: Partial

Policy resources are only supported for monitors, subscriptions, and cost categories.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of AWS Cost Explorer resource types, see Actions, resources, and condition keys for AWS Cost Explorer in the *Service Authorization Reference*.

To view examples of AWS Cost Management identity-based policies, see Identity-based policy examples for AWS Cost Management.

Policy condition keys for AWS Cost Management

Supports service-specific policy condition keys: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of AWS Cost Management condition keys, actions, and resources, see Condition keys for AWS Cost Management in the *Service Authorization Reference*.

To view examples of AWS Cost Management identity-based policies, see Identity-based policy examples for AWS Cost Management.

Access control lists (ACLs) in AWS Cost Management

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Attribute-based access control (ABAC) with AWS Cost Management

Supports ABAC (tags in policies): Partial

ABAC (tags in policies) are only supported for monitors, subscriptions, and cost categories.

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see What is ABAC? in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

Using Temporary credentials with AWS Cost Management

Supports temporary credentials: Yes

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see AWS services that work with IAM in the *IAM User Guide*.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see Switching to a role (console) in the *IAM User Guide*.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM.

Forward access sessions for AWS Cost Management

Supports forward access sessions (FAS): Yes

When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.

Service roles for AWS Cost Management

Supports service roles: Yes

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.

⚠ **Warning**

Changing the permissions for a service role might break AWS Cost Management functionality. Edit service roles only when AWS Cost Management provides guidance to do so.

Identity-based policy examples for AWS Cost Management

By default, users and roles don't have permission to create or modify AWS Cost Management resources. They also can't perform tasks by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS API. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Creating IAM policies in the *IAM User Guide*.

For details about actions and resource types defined by AWS Cost Management, including the format of the ARNs for each of the resource types, see Actions, resources, and condition keys for AWS Cost Management in the *Service Authorization Reference*.

Topics

- Policy best practices
- Using the AWS Cost Management console
- Allow users to view their own permissions

Policy best practices

Identity-based policies determine whether someone can create, access, or delete AWS Cost Management resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.

- **Apply least-privilege permissions –** When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access –** You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions –** IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see IAM Access Analyzer policy validation in the *IAM User Guide*.
- **Require multi-factor authentication (MFA) –** If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Configuring MFA-protected API access in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Using the AWS Cost Management console

To access the AWS Cost Management console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the AWS Cost Management resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the AWS Cost Management console, also attach the AWS Cost Management `ConsoleAccess` or `ReadOnly` AWS managed policy to the entities. For more information, see [Adding permissions to a user]() in the *IAM User Guide*.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Using identity-based policies (IAM policies) for AWS Cost Management

Note

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- `aws-portal` namespace
- `purchase-orders:ViewPurchaseOrders`
- `purchase-orders:ModifyPurchaseOrders`

If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

This topic provides examples of identity-based policies that demonstrate how an account administrator can attach permissions policies to IAM identities (roles and groups) and thereby grant permissions to perform operations on Billing and Cost Management resources.

For a full discussion of AWS accounts and users, see What Is IAM? in the *IAM User Guide*.

For information on how you can update customer managed policies, see Editing customer managed policies (console) in the *IAM User Guide*.

Topics

- Billing and Cost Management actions policies
- Managed policies
- AWS Cost Management updates to AWS managed policies

Billing and Cost Management actions policies

This table summarizes the permissions that allow or deny users access to your billing information and tools. For examples of policies that use these permissions, see AWS Cost Management policy examples.

For a list of actions policies for the Billing console, see Billing actions policies in the *Billing user guide*.

Permission name	Description
`aws-portal:ViewBilling`	Allow or deny users permission to view the Billing and Cost Management console pages. For an example policy, see Allow IAM users to view your billing information in the *Billing User Guide*.
`aws-portal:ViewUsage`	Allow or deny users permission to view AWS usage Reports. To allow users to view usage reports, you must allow both `ViewUsage` and `ViewBilling` . For an example policy, see Allow IAM users to access the reports console page in the *Billing User Guide*.
`aws-portal:ModifyBilling`	Allow or deny users permission to modify the following Billing and Cost Management console pages: • Budgets • Consolidated Billing • Billing preferences • Credits • Tax settings • Payment methods • Purchase orders

Permission name	Description
	- Cost Allocation Tags To allow users to modify these console pages, you must allow both `ModifyBilling` and `ViewBilling` . For an example policy, see Allow users to modify billing information.
`aws-portal:ViewAccount`	Allow or deny users permission to view the following Billing and Cost Management console pages: - Billing Dashboard - Account Settings
`aws-portal:ModifyAccount`	Allow or deny users permission to modify Account Settings. To allow users to modify account settings, you must allow both `ModifyAccount` and `ViewAccount` . For an example of a policy that explicitly denies a user access to the **Account Settings** console page, see Deny access to account settings, but allow full access to all other billing and usage information.
`budgets:ViewBudget`	Allow or deny users permission to view Budgets. To allow users to view budgets, you must also allow `ViewBilling` .

Permission name	Description
`budgets:ModifyBudget`	Allow or deny users permission to modify Budgets. To allow users to view and modify budgets, you must also allow `ViewBilling` .
`ce:GetPreferences`	Allow or deny users permissions to view the Cost Explorer preferences page. For an example policy, see View and update the Cost Explorer preferences page.
`ce:UpdatePreferences`	Allow or deny users permissions to update the Cost Explorer preferences page. For an example policy, see View and update the Cost Explorer preferences page.
`ce:DescribeReport`	Allow or deny users permissions to view the Cost Explorer reports page. For an example policy, see View, create, update, and delete using the Cost Explorer reports page.
`ce:CreateReport`	Allow or deny users permissions to create reports using the Cost Explorer reports page. For an example policy, see View, create, update, and delete using the Cost Explorer reports page.
`ce:UpdateReport`	Allow or deny users permissions to update using the Cost Explorer reports page. For an example policy, see View, create, update, and delete using the Cost Explorer reports page.

Permission name	Description
`ce:DeleteReport`	Allow or deny users permissions to delete reports using the Cost Explorer reports page. For an example policy, see View, create, update, and delete using the Cost Explorer reports page.
`ce:DescribeNotificationSubscription`	Allow or deny users permissions to view Cost Explorer reservation expiration alerts in the reservation overview page. For an example policy, see View, create, update, and delete reservation and Savings Plans alerts.
`ce:CreateNotificationSubscription`	Allow or deny users permissions to create Cost Explorer reservation expiration alerts in the reservation overview page. For an example policy, see View, create, update, and delete reservation and Savings Plans alerts.
`ce:UpdateNotificationSubscription`	Allow or deny users permissions to update Cost Explorer reservation expiration alerts in the reservation overview page. For an example policy, see View, create, update, and delete reservation and Savings Plans alerts.

Permission name	Description
`ce:DeleteNotificationSubscription`	Allow or deny users permissions to delete Cost Explorer reservation expiration alerts in the reservation overview page. For an example policy, see View, create, update, and delete reservation and Savings Plans alerts.
`ce:CreateCostCategoryDefinition`	Allow or deny users permissions to create cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*. You can add resource tags to monitors during `Create`. In order to create monitors with resource tags, you need the `ce:TagResource` permission.
`ce:DeleteCostCategoryDefinition`	Allow or deny users permissions to delete cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*.
`ce:DescribeCostCategoryDefinition`	Allow or deny users permissions to view cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*.
`ce:ListCostCategoryDefinitions`	Allow or deny users permissions to list cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*.

Permission name	Description
`ce:ListTagsForResource`	Allow or deny users permissions to list all resource tags for a given resource. For a list of supported resources, see ResourceTag in the *AWS Billing and Cost Management API Reference*.
`ce:UpdateCostCategoryDefinition`	Allow or deny users permissions to update cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*.
`ce:CreateAnomalyMonitor`	Allow or deny users permissions to create a single AWS Cost Anomaly Detection monitor. You can add resource tags to monitors during `Create`. In order to create monitors with resource tags, you need the `ce:TagResource` permission.
`ce:GetAnomalyMonitors`	Allow or deny users permissions to view all AWS Cost Anomaly Detection monitors.
`ce:UpdateAnomalyMonitor`	Allow or deny users permissions to update AWS Cost Anomaly Detection monitors.
`ce:DeleteAnomalyMonitor`	Allow or deny users permissions to delete AWS Cost Anomaly Detection monitors.
`ce:CreateAnomalySubscription`	Allow or deny users permissions to create a single subscription for AWS Cost Anomaly Detection. You can add resource tags to subscriptions during `Create`. In order to create subscriptions with resource tags, you need the `ce:TagResource` permission.

Permission name	Description
`ce:GetAnomalySubscriptions`	Allow or deny users permissions to view all subscriptions for AWS Cost Anomaly Detection .
`ce:UpdateAnomalySubscription`	Allow or deny users permissions to update AWS Cost Anomaly Detection subscriptions.
`ce:DeleteAnomalySubscription`	Allow or deny users permissions to delete AWS Cost Anomaly Detection subscriptions.
`ce:GetAnomalies`	Allow or deny users permissions to view all anomalies in AWS Cost Anomaly Detection.
`ce:ProvideAnomalyFeedback`	Allow or deny users permissions to provide feedback on a detected AWS Cost Anomaly Detection.
`ce:TagResource`	Allow or deny users permissions to add resource tag key-value pairs to a resource. For a list of supported resources, see ResourceTag in the *AWS Billing and Cost Management API Reference*.
`ce:UntagResource`	Allow or deny users permissions to delete resource tags from a resource. For a list of supported resources, see ResourceTag in the *AWS Billing and Cost Management API Reference*.

Managed policies

Note

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- *aws-portal* namespace
- *purchase-orders:ViewPurchaseOrders*
- *purchase-orders:ModifyPurchaseOrders*

If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

Managed policies are standalone identity-based policies that you can attach to multiple users, groups, and roles in your AWS account. You can use AWS managed policies to control access in Billing and Cost Management.

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases. AWS managed policies make it easier for you to assign appropriate permissions to users, groups, and roles than if you had to write the policies yourself.

You can't change the permissions defined in AWS managed policies. AWS occasionally updates the permissions defined in an AWS managed policy. When this occurs, the update affects all principal entities (users, groups, and roles) that the policy is attached to.

Billing and Cost Management provides several AWS managed policies for common use cases.

Topics

- Allows full access to AWS Budgets including budgets actions
- Allows read only access to AWS Budgets
- Allows permission to control AWS resources
- Allows Cost Optimization Hub to call services required to make the service work
- Allows read-only access to Cost Optimization Hub
- Allows admin access to Cost Optimization Hub

- Allows split cost allocation data to call services required to make the service work
- Allows Data Exports to access other AWS services

Allows full access to AWS Budgets including budgets actions

Managed policy name: `AWSBudgetsActionsWithAWSResourceControlAccess`

This managed policy is focused on the user, ensuring that you have the proper permissions to grant permission to AWS Budgets to run the defined actions. This policy provides full access to AWS Budgets, including budgets actions, to retrieve the status of your policies and run AWS resources using the AWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "budgets:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "budgets.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ModifyBilling",
                "ec2:DescribeInstances",
                "iam:ListGroups",
                "iam:ListPolicies",
                "iam:ListRoles",
                "iam:ListUsers",
                "organizations:ListAccounts",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListPolicies",
                "organizations:ListRoots",
                "rds:DescribeDBInstances",
                "sns:ListTopics"
            ],
            "Resource": "*"
        }
    ]
}
```

Allows read only access to AWS Budgets

Managed policy name: `AWSBudgetsReadOnlyAccess`

This managed policy allows read only access to AWS Budgets through the AWS Management Console. The policy can be attached to your users, groups, and roles.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid": "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Allows permission to control AWS resources

Managed policy name: `AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

This managed policy is focused on specific actions that AWS Budgets takes on your behalf when completing a specific action. This policy gives permission to control AWS resources. For example, starts and stops Amazon EC2 or Amazon RDS instances by running AWS Systems Manager (SSM) scripts.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstanceStatus",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "rds:DescribeDBInstances",
                "rds:StartDBInstance",
                "rds:StopDBInstance"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
                "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
                "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
                "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
            ]
        }
    ]
}
```

Allows Cost Optimization Hub to call services required to make the service work

Managed policy name: `CostOptimizationHubServiceRolePolicy`

Allows Cost Optimization Hub to retrieve organization information and collect optimization-related data and metadata.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AwsOrgsAccess",
            "Effect": "Allow",
            "Action":  [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource":  [
                "*"
            ]
        },
        {
            "Sid": "AwsOrgsScopedAccess",
            "Effect": "Allow",
            "Action":  [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "cost-optimization-
hub.bcm.amazonaws.com" ]
                }
            }
        },
        {
            "Sid": "CostExplorerAccess",
            "Effect": "Allow",
            "Action": [
                "ce:ListCostAllocationTags",
                "ce:GetCostAndUsage"
            ],
            "Resource":  [
                "*"
            ]
        }
    ]
}
```

For more information, see Service-linked roles for Cost Optimization Hub.

Allows read-only access to Cost Optimization Hub

Managed policy name: `CostOptimizationHubReadOnlyAccess`

This managed policy provides read-only access to Cost Optimization Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CostOptimizationHubReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:GetPreferences",
                "cost-optimization-hub:GetRecommendation",
                "cost-optimization-hub:ListRecommendations",
                "cost-optimization-hub:ListRecommendationSummaries"
            ],
            "Resource": "*"
        }
    ]
}
```

Allows admin access to Cost Optimization Hub

Managed policy name: `CostOptimizationHubAdminAccess`

This managed policy provides admin access to Cost Optimization Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CostOptimizationHubAdminAccess",
            "Effect": "Allow",
            "Action": [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:UpdateEnrollmentStatus",
                "cost-optimization-hub:GetPreferences",
                "cost-optimization-hub:UpdatePreferences",
                "cost-optimization-hub:GetRecommendation",
                "cost-optimization-hub:ListRecommendations",
                "cost-optimization-hub:ListRecommendationSummaries",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub"
            ],
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "cost-optimization-hub.bcm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowAWSServiceAccessForCostOptimizationHub",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "cost-optimization-hub.bcm.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Allows split cost allocation data to call services required to make the service work

Managed policy name: `SplitCostAllocationDataServiceRolePolicy`

Allows split cost allocation data to retrieve AWS Organizations information, if applicable, and collect telemetry data for the split cost allocation data services that the customer has opted in to.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AwsOrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AmazonManagedServiceForPrometheusAccess",
            "Effect": "Allow",
            "Action": [
                "aps:ListWorkspaces",
                "aps:QueryMetrics"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information, see Service-linked roles for split cost allocation data.

Allows Data Exports to access other AWS services

Managed policy name: `AWSBCMDataExportsServiceRolePolicy`

Allows Data Exports to access other AWS services such as Cost Optimization Hub on your behalf.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CostOptimizationRecommendationAccess",
            "Effect": "Allow",
            "Action":  [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:ListRecommendations"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information, see Service-linked roles for Data Exports.

AWS Cost Management updates to AWS managed policies

View details about updates to AWS managed policies for AWS Cost Management since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Cost Management Document history page.

Change	Description	Date
Update to existing policy CostOptimizationHubServiceRolePolicy	We updated the policy to add the `organizations:ListDelegatedAdministrators` and `ce:GetCostAndUsage` actions.	07/05/2024

Change	Description	Date
Update to existing policy AWSBudgetsReadOnlyAccess	We updated the policy to add the `budgets:ListTagsForResource` action.	06/17/2024
Addition of a new policy AWSBCMDataExportsServiceRolePolicy	Data Exports added a new policy to be used with service-linked roles, which enables access to other AWS services such as Cost Optimization Hub.	06/10/2024
Addition of a new policy SplitCostAllocationDataServiceRolePolicy	Split cost allocation data added a new policy to be used with service-linked roles, which enables access to AWS services and resources used or managed by split cost allocation data.	04/16/2024
Update to existing policy AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	We updated the policy with scoped down permissions. The `ssm:StartAutomationExecution` action is only allowed for specific resources used by Budget actions.	12/14/2023

Change	Description	Date
Update to existing policies CostOptimizationHubReadOnlyAccess CostOptimizationHubAdminAccess	Cost Optimization Hub updated the following two managed policies: - `CostOptimizationHubReadOnlyAccess` : Fixed typo in "GetRecommendation"; removed permissions covered by the SLR policy. - `CostOptimizationHubAdminAccess` : Fixed typo in "GetRecommendation"; removed permissions covered by the SLR policy; added permissions to enable service access and to create the SLR, so that the policy provides all necessary permissions to opt in and use Cost Optimization Hub.	12/14/2023
Addition of a new policy CostOptimizationHubServiceRolePolicy	Cost Optimization Hub added a new policy to be used with service-linked roles, which enables access to AWS services and resources used or managed by Cost Optimization Hub.	11/02/2023
AWS Cost Management started tracking changes	AWS Cost Management started tracking changes for its AWS managed policies	11/02/2023

AWS Cost Management policy examples

Note

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- *aws-portal* namespace
- *purchase-orders:ViewPurchaseOrders*
- *purchase-orders:ModifyPurchaseOrders*

If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

This topic contains example policies that you can attach to your IAM role or group to control access to your account's billing information and tools. The following basic rules apply to IAM policies for Billing and Cost Management:

- `Version` is always `2012-10-17`.
- `Effect` is always `Allow` or `Deny`.
- `Action` is the name of the action or a wildcard (`*`).

  The action prefix is `budgets` for AWS Budgets, `cur` for AWS Cost and Usage Reports, `aws-portal` for AWS Billing, or `ce` for Cost Explorer.
- `Resource` is always `*` for AWS Billing.

  For actions performed on a `budget` resource, specify the budget Amazon Resource Name (ARN).
- It's possible to have multiple statements in one policy.

For a list of policy examples for the Billing console, see Billing policy examples in the *Billing user guide*.

Note

These policies require that you activate user access to the Billing and Cost Management console on the Account Settings console page. For more information, see Activating access to the Billing and Cost Management console.

Topics

- Deny users access to the Billing and Cost Management console
- Deny AWS Console cost and usage widget access for member accounts
- Deny AWS Console cost and usage widget access for specific users and roles
- Allow full access to AWS services but deny users access to the Billing and Cost Management console
- Allow users to view the Billing and Cost Management console except for account settings
- Allow users to modify billing information
- Allow users to create budgets
- Deny access to account settings, but allow full access to all other billing and usage information
- Deposit reports into an Amazon S3 bucket
- View costs and usage
- Enable and disable AWS Regions
- View and update the Cost Explorer preferences page
- View, create, update, and delete using the Cost Explorer reports page
- View, create, update, and delete reservation and Savings Plans alerts
- Allow read-only access to AWS Cost Anomaly Detection
- Allow AWS Budgets to apply IAM policies and SCPs
- Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances

Deny users access to the Billing and Cost Management console

To explicitly deny a user access to the all Billing and Cost Management console pages, use a policy similar to this example policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "aws-portal:*",
            "Resource": "*"
        }
    ]
}
```

Deny AWS Console cost and usage widget access for member accounts

To restrict member (linked) account access to cost and usage data, use your management (payer) account to access the Cost Explorer preferences tab and uncheck **Linked Account Access**. This will deny access to cost and usage data from the Cost Explorer (AWS Cost Management) console, Cost Explorer API, and AWS Console Home page's cost and usage widget regardless of the IAM actions a member account’s user or role has.

Deny AWS Console cost and usage widget access for specific users and roles

To deny AWS Console cost and usage widget access for specific users and roles, use the permissions policy below.

> **Note**
>
> Adding this policy to a user or role will deny users access to Cost Explorer (AWS Cost Management) console and Cost Explorer APIs as well.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ce:*",
            "Resource": "*"
        }
    ]
}
```

Allow full access to AWS services but deny users access to the Billing and Cost Management console

To deny users access to everything on the Billing and Cost Management console, use the following policy. In this case, you should also deny user access to AWS Identity and Access Management (IAM) so that the users can't access the policies that control access to billing information and tools.

> ⚠ **Important**
>
> This policy doesn't allow any actions. Use this policy in combination with other policies that allow specific actions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aws-portal:*",
                "iam:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to view the Billing and Cost Management console except for account settings

This policy allows read-only access to all of the Billing and Cost Management console, including the **Payments Method** and **Reports** console pages, but denies access to the **Account Settings** page, thus protecting the account password, contact information, and security questions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "aws-portal:View*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "aws-portal:*Account",
            "Resource": "*"
        }
    ]
}
```

Allow users to modify billing information

To allow users to modify account billing information in the Billing and Cost Management console, you must also allow users to view your billing information. The following policy example allows a user to modify the **Consolidated Billing**, **Preferences**, and **Credits** console pages. It also allows a user to view the following Billing and Cost Management console pages:

- **Dashboard**
- **Cost Explorer**
- **Bills**
- **Orders and invoices**
- **Advance Payment**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "aws-portal:*Billing",
            "Resource": "*"
        }
    ]
}
```

Allow users to create budgets

To allow users to create budgets in the Billing and Cost Management console, you must also allow users to view your billing information, create CloudWatch alarms, and create Amazon SNS notifications. The following policy example allows a user to modify the **Budget** console page.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1435216493000",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling",
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "Stmt1435216514000",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "Stmt1435216552000",
            "Effect": "Allow",
            "Action": [
                "sns:*"
            ],
            "Resource": [
                "arn:aws:sns:us-east-1::"
            ]
        }
    ]
}
```

Deny access to account settings, but allow full access to all other billing and usage information

To protect your account password, contact information, and security questions, you can deny user access to **Account Settings** while still enabling full access to the rest of the functionality in the Billing and Cost Management console, as shown in the following example.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:*Billing",
                "aws-portal:*Usage",
                "aws-portal:*PaymentMethods"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "aws-portal:*Account",
            "Resource": "*"
        }
    ]
}
```

Deposit reports into an Amazon S3 bucket

The following policy allows Billing and Cost Management to save your detailed AWS bills to an Amazon S3 bucket, as long as you own both the AWS account and the Amazon S3 bucket. Note that this policy must be applied to the Amazon S3 bucket, instead of to a user. That is, it's a resource-based policy, not a user-based policy. You should deny user access to the bucket for users who don't need access to your bills.

Replace *bucketname* with the name of your bucket.

For more information, see Using Bucket Policies and User Policies in the *Amazon Simple Storage Service User Guide*.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "billingreports.amazonaws.com"
    },
    "Action": [
      "s3:GetBucketAcl",
      "s3:GetBucketPolicy"
    ],
    "Resource": "arn:aws:s3:::bucketname"
  },
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "billingreports.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::bucketname/*"
  }
  ]
}
```

View costs and usage

To allow users to use the AWS Cost Explorer API, use the following policy to grant them access.

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

Enable and disable AWS Regions

For an example IAM policy that allows users to enable and disable Regions, see AWS: Allows Enabling and Disabling AWS Regions in the *IAM User Guide*.

View and update the Cost Explorer preferences page

This policy allows a user to view and update using the **Cost Explorer preferences page**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "ce:UpdatePreferences"
       ],
      "Resource": "*"
    }
  ]
}
```

The following policy allows users to view Cost Explorer, but deny permission to view or edit the **Preferences** page.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:GetPreferences",
                "ce:UpdatePreferences"
            ],
            "Resource": "*"
        }
    ]
}
```

The following policy allows users to view Cost Explorer, but deny permission to edit the **Preferences** page.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:UpdatePreferences"
            ],
            "Resource": "*"
        }
    ]
}
```

View, create, update, and delete using the Cost Explorer reports page

This policy allows a user to view, create, update, and delete using the **Cost Explorer reports page**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "ce:CreateReport",
        "ce:UpdateReport",
        "ce:DeleteReport"
       ],
      "Resource": "*"
    }
  ]
}
```

The following policy allows users to view Cost Explorer, but deny permission to view or edit the **Reports** page.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:DescribeReport",
                "ce:CreateReport",
                "ce:UpdateReport",
                "ce:DeleteReport"
            ],
            "Resource": "*"
        }
    ]
}
```

The following policy allows users to view Cost Explorer, but deny permission to edit the **Reports** page.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action":
                "ce:CreateReport",
                "ce:UpdateReport",
                "ce:DeleteReport"
            ],
            "Resource": "*"
        }
    ]
}
```

View, create, update, and delete reservation and Savings Plans alerts

This policy allows a user to view, create, update, and delete reservation expiration alerts and Savings Plans alerts. To edit reservation expiration alerts or Savings Plans alerts, a user needs all three granular actions: `ce:CreateNotificationSubscription`, `ce:UpdateNotificationSubscription`, and `ce:DeleteNotificationSubscription`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "ce:CreateNotificationSubscription",
        "ce:UpdateNotificationSubscription",
        "ce:DeleteNotificationSubscription"
       ],
      "Resource": "*"
    }
  ]
}
```

The following policy allows users to view Cost Explorer, but denies permission to view or edit the **Reservation Expiration Alerts** and **Savings Plans alert** pages.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:DescribeNotificationSubscription",
                "ce:CreateNotificationSubscription",
                "ce:UpdateNotificationSubscription",
                "ce:DeleteNotificationSubscription"
            ],
            "Resource": "*"
        }
    ]
}
```

The following policy allows users to view Cost Explorer, but denies permission to edit the **Reservation Expiration Alerts** and **Savings Plans alert** pages.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:CreateNotificationSubscription",
                "ce:UpdateNotificationSubscription",
                "ce:DeleteNotificationSubscription"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow read-only access to AWS Cost Anomaly Detection

To allow users read-only access to AWS Cost Anomaly Detection, use the following policy to grant them access. `ce:ProvideAnomalyFeedback` is optional as a part of the read-only access.

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

Allow AWS Budgets to apply IAM policies and SCPs

This policy allows AWS Budgets to apply IAM policies and service control policies (SCPs) on behalf of the user.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:DetachGroupPolicy",
        "iam:DetachRolePolicy",
        "iam:DetachUserPolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances

This policy allows AWS Budgets to apply IAM policies and service control policies (SCPs), and to target Amazon EC2 and Amazon RDS instances on behalf of the user.

Trust policy

Note

This trust policy allows AWS Budgets to assume a role that can call other services on your behalf. For more information on the best practices for cross-service permissions like this, see Cross-service confused deputy prevention.

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "budgets.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:budgets::123456789012:budget/*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
]
}
```

Permissions policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:DetachGroupPolicy",
        "iam:DetachRolePolicy",
        "iam:DetachUserPolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance",
        "ssm:StartAutomationExecution"
      ],
      "Resource": "*"
    }
  ]
}
```

Migrating access control for AWS Cost Management

Note

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- *`aws-portal`* namespace
- *`purchase-orders:ViewPurchaseOrders`*
- *`purchase-orders:ModifyPurchaseOrders`*

If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

You can use fine-grained access controls to provide individuals in your organization access to AWS Billing and Cost Management services. For example, you can provide access to Cost Explorer without providing access to the AWS Billing console.

To use the fine-grained access controls, you'll need to migrate your policies from under `aws-portal` to the new IAM actions.

The following IAM actions in your permission policies or service control policies (SCP) require updating with this migration:

- `aws-portal:ViewAccount`
- `aws-portal:ViewBilling`
- `aws-portal:ViewPaymentMethods`
- `aws-portal:ViewUsage`
- `aws-portal:ModifyAccount`

- `aws-portal:ModifyBilling`
- `aws-portal:ModifyPaymentMethods`
- `purchase-orders:ViewPurchaseOrders`
- `purchase-orders:ModifyPurchaseOrders`

To learn how to use the **Affected policies** tool to identify your impacted IAM policies, see How to use the affected policies tool.

> **Note**
>
> Programmatic requests to AWS Cost Explorer, AWS Cost and Usage Reports, and AWS Budgets remains unaffected.
> Activating access to the Billing and Cost Management console remain unchanged.

Topics

- Managing access permissions
- How to use the affected policies tool

Managing access permissions

AWS Cost Management integrates with the AWS Identity and Access Management (IAM) service so that you can control who in your organization has access to specific pages on the AWS Cost Management console. You can control access to AWS Cost Management features. For example, AWS Cost Explorer, Savings Plans, and reservation recommendations, Savings Plans and reservations utilization and coverage reports.

Use the following IAM permissions for granular control for the AWS Cost Management console.

Using fine-grained AWS Cost Management actions

This table summarizes the permissions that allow or deny IAM users and roles access to your cost and usage information. For examples of policies that use these permissions, see AWS Cost Management policy examples.

For a list of actions for the AWS Billing console, see AWS Billing actions policies in the *AWS Billing user guide*.

Feature name in the AWS Cost Management console	IAM action	Description

AWS Cost Management Home	`ce:GetCostAndUsage`
	`ce:GetDimensionValues`
	`ce:GetCostForecast`
	`ce:GetReservationUtilization`
	`ce:GetReservationPurchaseRecommendation`
	`ce:DescribeReport`
	`ce:GetDimensionValues`
	`ce:GetReservationUtilization`
		Allow or deny users permission to view the **AWS Cost Management Home** page. All IAM actions are required to view the page.

AWS Cost Explorer	`ce:GetCostCategories`
	`ce:GetDimensionValues`
	`ce:GetCostAndUsageWithResources`
	`ce:GetCostAndUsage`
	`ce:GetCostForecast`
	`ce:GetTags`
	`ce:GetUsageForecast`
		Allow or deny users permission to view the **AWS Cost Explorer** page.

Feature name in the AWS Cost Management console	IAM action	Description
	`ce:DescribeReport`	
	`ce:CreateReport`	Allow or deny users permission to save Cost Explorer reports.
[Reports]()	`ce:DescribeReport`	Allow or deny users permission to view a list of saved reports.
	`ce:DeleteReport`	Allow or deny users permission to delete a saved report.

[AWS Budgets]()	`budgets:ViewBudget`
	`budgets:DescribeBudgetActionsForBudget`
	`budgets:DescribeBudgetAction`
	`budgets:DescribeBudgetActionsForAccount`
	`budgets:DescribeBudgetActionHistories`
		Allow or deny users permission to view the **Budgets** page.

Feature name in the AWS Cost Management console	IAM action	Description

	`budgets:CreateBudgetAction`
	`budgets:ExecuteBudgetAction`
	`budgets:DeleteBudgetAction`
	`budgets:UpdateBudgetAction`
	`budgets:ModifyBudget`
		Allow or deny users permission to create, delete, and modify Budgets and Budgets actions.

Feature name in the AWS Cost Management console	IAM action	Description

AWS Cost Anomaly Detection	`ce:GetDimensionValues`
	`ce:GetCostAndUsage`
	`ce:CreateAnomalyMonitor`
	`ce:GetAnomalyMonitors`
	`ce:UpdateAnomalyMonitor`
	`ce:DeleteAnomalyMonitor`
	`ce:CreateAnomalySubscription`
	`ce:GetAnomalySubscriptions`
	`ce:UpdateAnomalySubscription`
	`ce:DeleteAnomalySubscription`
	`ce:GetAnomalies`
	`ce:ProvideAnomalyFeedback`
		Allow or deny users permission to view, create, delete, and update on the **Cost Anomaly Detection** page.

Feature name in the AWS Cost Management console	IAM action	Description

[Rightsizing recommendations]()	`ce:GetDimensionValues`
	`ce:GetTags`
	`ce:GetRightsizingRecommendation`
		Allow or deny users permission to view the **Savings Plans Overview** page.

[Savings Plans overview]()	`ce:GetSavingsPlansUtilizationDetails` `ce:GetSavingsPlansPurchaseRecommendation`	
	`ce:DescribeNotificationSubscription`	Allow or deny users permission to view the existing notification settings for expiring and queued Savings Plans alerts.

	`ce:CreateNotificationSubscription`
	`ce:UpdateNotificationSubscription`
	`ce:DeleteNotificationSubscription`
		Allow or deny users permission to update the existing notification settings for expiring and queued Savings Plans alerts.

[Savings Plans inventory]()	`savingsplans:DescribeSavingsPlans` `ce:GetSavingsPlansUtilizationDetails`	Allow or deny users permissions to view purchased Savings Plans.

Feature name in the AWS Cost Management console	IAM action	Description
	`savingsplans:DescribeSavingsPlansOfferings`	Allow or deny users permissions to add the Savings Plans they wish to renew to the cart.
Savings Plans recommendations	`ce:GetSavingsPlansPurchaseRecommendation` `ce:ListSavingsPlansPurchaseRecommendationGeneration`	Allow or deny users permission to view generated Savings Plans recommendations.
	`ce:StartSavingsPlansPurchaseRecommendationGeneration`	Allow or deny users permission to calculate a new set of recommendations based on the latest usage and Savings Plans inventory.
Purchase Savings Plans	`savingsplans:DescribeSavingsPlansOfferings`	Allow or deny users permission to add Savings Plans to the cart.

Savings Plans utilization report	`ce:DescribeReport`
	`ce:GetSavingsPlansUtilization`
	`ce:GetSavingsPlansUtilizationDetails`
	`ce:GetDimensionValues`
		Allow or deny users permission to view utilization of your existing Savings Plans.

Feature name in the AWS Cost Management console	IAM action	Description
	`savingsplans:DescribeSavingsPlanRates`	Allow or deny users permission to view the Savings Plans rate.

Savings Plans coverage report	`ce:GetDimensionValues`
	`ce:GetSavingsPlansCoverage`
	`ce:GetCostCategories`
	`ce:DescribeReport`
	`ce:GetSavingsPlansPurchaseRecommendation`
		Allow or deny users permission to view the eligible spends covered by Savings Plans.

Savings Plans cart	`savingsplans:DescribeSavingsPlansOfferings` `savingsplans:DescribeSavingsPlans`	Allow or deny users permission to purchase Savings Plans.
	`savingsplans:CreateSavingsPlan`	

Feature name in the AWS Cost Management console	IAM action	Description
Reservations overview	ce:GetReservationUtilization ce:GetReservationCoverage ce:GetReservationPurchaseRecommendation ce:DescribeReport	Allow or deny users permission to view the **Reservations Overview** page.
	ce:DescribeNotificationSubscription	Allow or deny users permission to view existing notification settings for expiring reserved instances (RI) alerts.
	ce:CreateNotificationSubscription ce:UpdateNotificationSubscription ce:DeleteNotificationSubscription	Allow or deny users permission to update notification settings for expiring RI alerts.
Reservations recommendations	ce:GetReservationPurchaseRecommendation ce:GetDimensionValues	Allow or deny users permission to view reservations recommendations.

Feature name in the AWS Cost Management console	IAM action	Description

Reservations utilization reports	`ce:GetDimensionValues`
	`ce:GetReservationUtilization`
	`ce:DescribeReport`
		Allow or deny users permission to view utilization of your existing RI.

	`ce:CreateReport`	Allow or deny users permission to save RI reports.

Reservations coverage report	`ce:GetReservationCoverage`
	`ce:GetReservationPurchaseRecommendation`
	`ce:DescribeReport`
	`ce:GetDimensionValues`
	`ce:GetCostCategories`
		Allow or deny users permission to view eligible spends covered by Reservations (RIs).

	`ce:CreateReport`	Allow or deny users permission to save RI coverage reports.
Preferences	`ce:GetPreferences`	Allow or deny users permission to view AWS Cost Management preferences.
	`ce:UpdatePreferences`	Allow or deny users permission to update AWS Cost Management preferences.

How to use the affected policies tool

Note

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- *aws-portal* namespace
- *purchase-orders:ViewPurchaseOrders*
- *purchase-orders:ModifyPurchaseOrders*

If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

You can use the **Affected policies** tool in the Billing console to identify IAM policies (excluding SCPs), and reference the IAM actions affected by this migration. Use the **Affected policies** tool to do the following tasks:

- Identify IAM policies and reference the IAM actions affected by this migration
- Copy the updated policy to your clipboard
- Open the affected policy in IAM policy editor
- Save the updated policy for your account
- Turn on the fine-grained permissions and disable the old actions

This tool operates within the boundaries of the AWS account you're signed into, and information regarding other AWS Organizations accounts are not disclosed.

To use the Affected policies tool

1. Sign in to the AWS Management Console and open the AWS Billing console at https://console.aws.amazon.com/billing/.
2. Paste the following URL into your browser to access the **Affected policies** tool: https://console.aws.amazon.com/poliden/home?region=us-east-1#/.

   > **Note**
   >
   > You must have the `iam:GetAccountAuthorizationDetails` permission to view this page.

3. Review the table that lists the affected IAM policies. Use the **Deprecated IAM actions** column to review specific IAM actions referenced in a policy.
4. Under the **Copy updated policy** column, choose **Copy** to copy the updated policy to your clipboard. The updated policy contains the existing policy and the suggested fine-grained actions appended to it as a separate `Sid` block. This block has the prefix `AffectedPoliciesMigrator` at the end of the policy.
5. Under the **Edit Policy in IAM Console** column, choose **Edit** to go to IAM policy editor. You will see the JSON of your existing policy.
6. Replace the entire existing policy with the updated policy that you copied in step 4. You can make any other changes as needed.
7. Choose **Next** and then choose **Save changes**.
8. Repeat steps 3 to 7 for all affected policies.
9. After you update your policies, refresh the **Affected policies** tool to confirm there are no affected policies listed. The **New IAM Actions Found** column should have **Yes** for all policies and the **Copy** and **Edit** buttons will be disabled. Your affected policies are updated.

To enable fine-grained actions for your account

After you update your policies, follow this procedure to enable the fine-grained actions for your account.

Only the management account (payer) of an organization or individual accounts can use the **Manage New IAM Actions** section. An individual account can enable the new actions for itself. A management account can enable new actions for the entire organization or a subset of member accounts. If you're a management account, update the affected policies for all member accounts and enable the new actions for your organization. For more information, see the How to toggle accounts between new fine-grained actions or existing IAM actions? section in the AWS blog post.

> **Note**
>
> To do this, you must have the following permissions:
>
> - `aws-portal:GetConsoleActionSetEnforced`
> - `aws-portal:UpdateConsoleActionSetEnforced`
> - `ce:GetConsoleActionSetEnforced`
> - `ce:UpdateConsoleActionSetEnforced`
> - `purchase-orders:GetConsoleActionSetEnforced`
> - `purchase-orders:UpdateConsoleActionSetEnforced`

If you don't see the **Manage New IAM Actions** section, this means your account has already enabled the fine-grained IAM actions.

1. Under **Manage New IAM Actions**, the **Current Action Set Enforced** setting will have the **Existing** status.

   Choose **Enable New actions (Fine Grained)** and then choose **Apply changes**.
2. In the dialog box, choose **Yes**. The **Current Action Set Enforced** status will change to **Fine Grained**. This means the new actions are enforced for your AWS account or for your organization.
3. (Optional) You can then update your existing policies to remove any of the old actions.

Example Example: Before and after IAM policy

The following IAM policy has the old `aws-portal:ViewPaymentMethods` action.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewPaymentMethods"
            ],
            "Resource": "*"
        }
    ]
}
```

After you copy the updated policy, the following example has the new `Sid` block with the fine-grained actions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewPaymentMethods"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AffectedPoliciesMigrator0",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "invoicing:GetInvoicePDF",
                "payments:GetPaymentInstrument",
                "payments:GetPaymentStatus",
                "payments:ListPaymentPreferences"
            ],
            "Resource": "*"
        }
    ]
}
```

Related resources

For more information, see Sid in the *IAM User Guide*.

For more information about the new fine-grained actions, see the Mapping fine-grained IAM actions reference and Using fine-grained AWS Cost Management actions.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies to limit the permissions to the resource that AWS Cost Management features can give another service. If you use both global condition context keys, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcards (`*`) for the unknown portions of the ARN. For example, `arn:aws:`*`servicename`*`::`*`123456789012`*`:*`. For AWS Budgets, the value of `aws:SourceArn` must be `arn:aws:budgets::`*`123456789012`*`:budget/*`.

The following example shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in AWS Budgets to prevent the confused deputy problem.

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "budgets.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:budgets::123456789012:budget/*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
]
}
```

Troubleshooting AWS Cost Management identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with AWS Cost Management and IAM.

Topics

- I am not authorized to perform an action in AWS Cost Management
- I am not authorized to perform iam:PassRole
- I want to view my access keys
- I'm an administrator and want to allow others to access AWS Cost Management
- I want to allow people outside of my AWS account to access my AWS Cost Management resources

I am not authorized to perform an action in AWS Cost Management

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person who provided you with your sign-in credentials.

The following example error occurs when the `mateojackson` user tries to use the console to view details about a fictional *`my-example-widget`* resource but does not have the fictional `ce:`*`GetWidget`* permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ce:GetWidget on resource: my-example-widget
```

In this case, Mateo asks his administrator to update his policies to allow him to access the *`my-example-widget`* resource using the `ce:`*`GetWidget`* action.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to AWS Cost Management.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in AWS Cost Management. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

Important

Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your AWS account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing access keys in the *IAM User Guide*.

I'm an administrator and want to allow others to access AWS Cost Management

To allow others to access AWS Cost Management, you must grant permission to the people or applications that need access. If you are using AWS IAM Identity Center to manage people and applications, you assign permission sets to users or groups to define their level of access. Permission sets automatically create and assign IAM policies to IAM roles that are associated with the person or application. For more information, see Permission sets in the *AWS IAM Identity Center User Guide*.

If you are not using IAM Identity Center, you must create IAM entities (users or roles) for the people or applications that need access. You must then attach a policy to the entity that grants them the correct permissions in AWS Cost Management. After the permissions are granted, provide the credentials to the user or application developer. They will use those credentials to access AWS. To learn more about creating IAM users, groups, policies, and permissions, see IAM Identities and Policies and permissions in IAM in the *IAM User Guide*.

I want to allow people outside of my AWS account to access my AWS Cost Management resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether AWS Cost Management supports these features, see How AWS Cost Management works with IAM.
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.

- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Service-linked roles for AWS Cost Management

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing service-linked roles, see AWS services that work with IAM. Find a service in the table that includes a `Yes` in the **Service-linked role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

Using service-linked roles

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

Topics

- Service-linked roles for Cost Optimization Hub
- Service-linked roles for split cost allocation data
- Service-linked roles for Data Exports

Service-linked roles for Cost Optimization Hub

Cost Optimization Hub uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Cost Optimization Hub. Service-linked roles are predefined by Cost Optimization Hub and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Cost Optimization Hub easier because you don't have to manually add the necessary permissions. Cost Optimization Hub defines the permissions of its service-linked roles, and unless defined otherwise, only Cost Optimization Hub can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Cost Optimization Hub

Cost Optimization Hub uses the service-linked role named `AWSServiceRoleForCostOptimizationHub`, which enables access to AWS services and resources used or managed by Cost Optimization Hub.

The `AWSServiceRoleForCostOptimizationHub` service-linked role trusts the `cost-optimization-hub.bcm.amazonaws.com` service to assume the role.

The role permissions policy, `CostOptimizationHubServiceRolePolicy`, allows Cost Optimization Hub to complete the following actions on the specified resources:

- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListParents
- organizations:DescribeOrganizationalUnit
- organizations:ListDelegatedAdministrators
- ce:ListCostAllocationTags
- ce:GetCostAndUsage

For more information, see Allows Cost Optimization Hub to call services required to make the service work.

To view the full permissions details of the service-linked role `CostOptimizationHubServiceRolePolicy`, see CostOptimizationHubServiceRolePolicy in the *AWS Managed Policy Reference Guide*.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating the Cost Optimization Hub service-linked role

You don't need to manually create a service-linked role. When you enable Cost Optimization Hub, the service automatically creates the service-linked role for you. You can enable Cost Optimization Hub through the AWS Cost Management console, or via the API or AWS CLI. For more information, see Enable Cost Optimization Hub in this user guide.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account.

Editing the Cost Optimization Hub service-linked role

You can't edit the name or permissions of the `AWSServiceRoleForCostOptimizationHub` service-linked role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

To allow an IAM entity to edit the description of the `AWSServiceRoleForCostOptimizationHub` service-linked role

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub",
    "Condition": {"StringLike": {"iam:AWSServiceName": "cost-optimization-
hub.bcm.amazonaws.com"}}
}
```

Deleting the Cost Optimization Hub service-linked role

If you no longer need to use Cost Optimization Hub, we recommend that you delete the `AWSServiceRoleForCostOptimizationHub` service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, before you can manually delete the service-linked role, you must opt out of Cost Optimization Hub.

To opt out of Cost Optimization Hub

For information about opting out of Cost Optimization Hub, see Opting out of Cost Optimization Hub.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS Command Line Interface (AWS CLI), or the AWS API to delete the `AWSServiceRoleForCostOptimizationHub` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for Cost Optimization Hub service-linked roles

Cost Optimization Hub supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see AWS service endpoints.

Service-linked roles for split cost allocation data

Split cost allocation data uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to split cost allocation data. Service-linked roles are predefined by split cost allocation data and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up split cost allocation data easier because you don't have to manually add the necessary permissions. Split cost allocation data defines the permissions of its service-linked roles, and unless defined otherwise, only split cost allocation data can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for split cost allocation data

Split cost allocation data uses the service-linked role named `AWSServiceRoleForSplitCostAllocationData`, which enables access to AWS services and resources used or managed by split cost allocation data.

The `AWSServiceRoleForSplitCostAllocationData` service-linked role trusts the `split-cost-allocation-data.bcm.amazonaws.com` service to assume the role.

The role permissions policy, `SplitCostAllocationDataServiceRolePolicy`, allows split cost allocation data to complete the following actions on the specified resources:

- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListParents
- aps:ListWorkspaces
- aps:QueryMetrics

For more information, see Allows split cost allocation data to call services required to make the service work.

To view the full permissions details of the service-linked role `SplitCostAllocationDataServiceRolePolicy`, see `SplitCostAllocationDataServiceRolePolicy` in the *AWS Managed Policy Reference Guide*.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the IAM User Guide.

Creating the split cost allocation data service-linked role

You don't need to manually create a service-linked role. When you opt in to split cost allocation data, the service automatically creates the service-linked role for you. You can enable split cost allocation data through the AWS Cost Management console. For more information, see Enabling split cost allocation data.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account.

Editing the split cost allocation data service-linked role

You can't edit the name or permissions of the `AWSServiceRoleForSplitCostAllocationData` service-linked role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

To allow an IAM entity to edit the description of the `AWSServiceRoleForSplitCostAllocationData` service-linked role

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/split-cost-allocation-
data.bcm.amazonaws.com/AWSServiceRoleForSplitCostAllocationData",
    "Condition": {"StringLike": {"iam:AWSServiceName": "split-cost-allocation-
data.bcm.amazonaws.com"}}
}
```

Deleting the split cost allocation data service-linked role

If you no longer need to use split cost allocation data, we recommend that you delete the `AWSServiceRoleForSplitCostAllocationData` service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, before you can manually delete the service-linked role, you must opt out of split cost allocation data.

To opt out of split cost allocation data

For information about opting out of split cost allocation data, see Enabling split cost allocation data.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS Command Line Interface (AWS CLI), or the AWS API to delete the `AWSServiceRoleForSplitCostAllocationData` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for split cost allocation data service-linked roles

Split cost allocation data supports using service-linked roles in all of the AWS Regions where split cost allocation data is available. For more information, see AWS service endpoints.

Service-linked roles for Data Exports

Data Exports uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Data Exports. Service-linked roles are predefined by Data Exports and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Data Exports easier because you don't have to manually add the necessary permissions. Data Exports defines the permissions of its service-linked role, and unless defined otherwise, only Data Exports can assume that role. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Data Exports

Data Exports uses the service-linked role named `AWSServiceRoleForBCMDataExports`, which enables access to AWS service data for exporting the data to a target location, such as Amazon S3, on behalf of the customer. This service-linked role is used for read-only actions to collect the least amount of AWS service data necessary. The service-linked role is used over time to ensure security and to continue refreshing the export data in the target location.

The `AWSServiceRoleForBCMDataExports` service-linked role trusts the `bcm-data-exports.amazonaws.com` service to assume the role.

The role permissions policy, `AWSBCMDataExportsServiceRolePolicy`, allows Data Exports to complete the following actions on the specified resources:

- cost-optimization-hub:ListEnrollmentStatuses
- cost-optimization-hub:ListRecommendation

For more information, see Allows Data Exports to access other AWS services.

To view the full permissions details of the service-linked role `AWSBCMDataExportsServiceRolePolicy`, see AWSBCMDataExportsServiceRolePolicy in the *AWS Managed Policy Reference Guide*.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see [Service-linked role permissions](#) in the IAM User Guide.

Creating the Data Exports service-linked role

You don't need to manually create the Data Exports service-linked role. On the Data Exports console page, when you attempt to create an export of a table that requires the service-linked role, the service automatically creates the role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account.

Editing the Data Exports service-linked role

You can't edit the name or permissions of the `AWSServiceRoleForBCMDataExports` service-linked role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a service-linked role](#) in the IAM User Guide.

To allow an IAM entity to edit the description of the `AWSServiceRoleForBCMDataExports` service-linked role

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/bcm-data-exports.amazonaws.com/
AWSServiceRoleForBCMDataExports",
    "Condition": {"StringLike": {"iam:AWSServiceName": "bcm-data-
exports.amazonaws.com"}}
}
```

Deleting the Data Exports service-linked role

If you no longer need to use Data Exports, we recommend that you delete the `AWSServiceRoleForBCMDataExports` service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, before you can manually delete the service-linked role, you must first delete any Data Exports that require the service-linked role.

To delete an export

For information about deleting an export, see Editing and deleting exports.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS Command Line Interface (AWS CLI), or the AWS API to delete the `AWSServiceRoleForBCMDataExports` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for Data Exports service-linked roles

Data Exports supports using service-linked roles in all of the AWS Regions where Data Exports is available. For more information, see AWS service endpoints.

Logging and monitoring in AWS Cost Management

Monitoring is an important part of maintaining the reliability, availability, and performance of your AWS account. There are several tools available to monitor your Billing and Cost Management usage.

AWS Cost and Usage Reports

AWS Cost and Usage Reports tracks your AWS usage and provides estimated charges associated with your account. Each report contains line items for each unique combination of AWS products, usage type, and operation that you use in your AWS account. You can customize the AWS Cost and Usage Reports to aggregate the information either by the hour or by the day.

For more information about AWS Cost and Usage Reports, see the *Cost and Usage Report Guide*.

AWS Cost Explorer

Cost Explorer enables you to view and analyze your costs and usage. You can monitor data for up to the last 13 months, forecast how much you're likely to spend for the next three months, and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to identify areas that need further inquiry and see trends that you can use to understand your costs.

For more information about Cost Explorer, see the Analyzing your costs with AWS Cost Explorer.

AWS Budgets

Budgets enables you to track your AWS cost and usage by using the cost visualization provided by Cost Explorer. Budgets shows the status of your budgets, provides forecasts of your estimated costs, and tracks your AWS usage, including Free Tier. You can also receive notifications when your estimated costs exceed your budgets.

For more information about Budgets, see the Managing your costs with AWS Budgets.

AWS CloudTrail

Billing and Cost Management is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Billing and Cost Management. CloudTrail captures all write and modify API calls for Billing and Cost Management as events, including calls from the Billing and Cost Management console and from code calls to the Billing and Cost Management APIs.

For more information about AWS CloudTrail, see the Logging AWS Cost Management API calls with AWS CloudTrail.

Logging AWS Cost Management API calls with AWS CloudTrail

AWS Cost Management is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Cost Management. CloudTrail captures API calls for AWS Cost Management as events. The calls captured include API calls from the AWS Cost Management console and from your applications.

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Cost Management. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS Cost Management, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

AWS Cost Management information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS Cost Management, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for AWS Cost Management, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the CloudTrail console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partitions and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to analyze and act on the event data collected in CloudTrail logs.

For more information, see the following in the *CloudTrail User Guide*:

- Creating a trail for your AWS account (overview)
- CloudTrail supported services and integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail log files from multiple regions
- Receiving CloudTrail log files from multiple accounts

AWS Cost Management actions are logged by CloudTrail and documented in the AWS Billing and Cost Management API Reference. For example, calls to the `GetDimensionValues`, `GetCostCategories`, and `GetCostandUsage` endpoints generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine whether the request was made:

- With root or user role credentials.
- With temporary security credentials for a role or federated user.
- By another AWS service.

For more information, see the CloudTrail userIdentity Element.

Understanding AWS Cost Management log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on.

CloudTrail log files contain one or more log entries. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

The following example shows a CloudTrail log entry for the `GetCostandUsage` endpoint.

```
{
        "eventVersion":"1.08",
        "userIdentity":{
            "accountId":"111122223333",
            "accessKeyId":"AIDACKCEVSQ6C2EXAMPLE"
        },
        "eventTime":"2022-05-24T22:38:51Z",
        "eventSource":"ce.amazonaws.com",
        "eventName":"GetCostandUsage",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.100.10.10",
        "requestParameters":{
           "TimePeriod":{
              "Start":"2022-01-01",
              "End":"2022-01-31"
           },
           "Metrics":[
              "UnblendedCost",
              "UsageQuantity"
           ],
           "Granularity":"MONTHLY",
           "GroupBy":[
              {
                 "Type":"DIMENSION",
                 "Key":"SERVICE"
              }
           ]
        },
        "responseElements":null,
        "requestID":"3295c994-063e-44ac-80fb-b40example9f",
        "eventID":"5923c499-063e-44ac-80fb-b40example9f",
        "readOnly":true,
        "eventType":"AwsApiCall",
        "managementEvent":true,
        "recipientAccountId":"1111-2222-3333",
        "eventCategory":"Management",
        "tlsDetails":{
           "tlsVersion":"TLSv1.2",
           "clientProvidedHostHeader":"ce.us-east-1.amazonaws.com"
        }
}
```

Understanding Cost Optimization Hub log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following examples show CloudTrail log entries that demonstrate API actions and exceptions for Cost Optimization Hub.

Examples

- Exceptions
  - Throttling Exception
  - Access denied exception
- API actions
  - ListEnrollmentStatus
  - ListRecommendations
  - ListRecommendationSummaries
  - GetRecommendation
  - UpdateEnrollmentStatus
  - UpdatePreferences

Throttling Exception

The following example shows a log entry for a throttling exception.

```
    {
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "EXAMPLEAIZ5FYRFP3POCC",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "john-doe": "Admin"
          },
          "attributes": {
            "creationDate": "2023-10-14T00:48:50Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-10-14T01:16:45Z",
      "eventSource": "cost-optimization-hub.amazonaws.com",
      "eventName": "ListEnrollmentStatuses",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "errorCode": "ThrottlingException",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "cc04aa10-7417-4c46-b1eb-EXAMPLE1df2b",
      "eventID": "754a3aad-1b54-456a-ac1f-EXAMPLE0e9c3",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "tlsDetails": {
        "clientProvidedHostHeader": "localhost:8080"
      }
    }
```

Access denied exception

The following example shows a log entry for an `AccessDenied` exception.

```
{
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
    "principalId": "EXAMPLEAIZ5FTKD2BZKUK:john-doe",
    "arn": "arn:aws:sts::111122223333:assumed-role/ReadOnly/john-doe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
     "sessionIssuer": {
      "type": "Role",
      "principalId": "EXAMPLEAIZ5FTKD2BZKUK",
      "arn": "arn:aws:iam::111122223333:role/ReadOnly",
      "accountId": "111122223333",
      "john-doe": "ReadOnly"
     },
     "attributes": {
      "creationDate": "2023-10-16T19:08:36Z",
      "mfaAuthenticated": "false"
     }
    }
   },
   "eventTime": "2023-10-16T19:11:04Z",
   "eventSource": "cost-optimization-hub.amazonaws.com",
   "eventName": "ListEnrollmentStatuses",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "192.0.2.0",
   "userAgent": "PostmanRuntime/7.28.3",
   "errorCode": "AccessDenied",
   "errorMessage": "User: arn:aws:sts::111122223333:assumed-role/ReadOnly/john-
doe is not authorized to perform: cost-optimization-hub:ListEnrollmentStatuses
 on resource: * because no identity-based policy allows the cost-optimization-
hub:ListEnrollmentStatuses action",
   "requestParameters": null,
   "responseElements": null,
   "requestID": "1e02d84a-b04a-4b71-8615-EXAMPLEdcda7",
   "eventID": "71c86695-d4ec-4caa-a106-EXAMPLEe0d94",
   "readOnly": true,
   "eventType": "AwsApiCall",
   "managementEvent": true,
   "recipientAccountId": "111122223333",
   "eventCategory": "Management",
   "tlsDetails": {
    "clientProvidedHostHeader": "localhost:8080"
   }
  }
```

ListEnrollmentStatus

The following example shows a log entry for the `ListEnrollmentStatus` API action.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC",
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "john-doe": "Admin"
      },
      "attributes": {
        "creationDate": "2023-10-14T00:48:50Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-10-14T01:16:43Z",
  "eventSource": "cost-optimization-hub.amazonaws.com",
  "eventName": "ListEnrollmentStatuses",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "PostmanRuntime/7.28.3",
  "requestParameters": {
    "includeOrganizationInfo": false
  },
  "responseElements": null,
  "requestID": "cba87aa3-4678-41b8-a840-EXAMPLEaf3b8",
  "eventID": "57f04d0e-61f7-4c0f-805c-EXAMPLEbbbf5",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "localhost:8080"
  }
}
```

ListRecommendations

The following example shows a log entry for the `ListRecommendations` API action.

```
    {
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "EXAMPLEAIZ5FYRFP3POCC",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "john-doe": "Admin"
          },
          "attributes": {
            "creationDate": "2023-10-16T23:47:55Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-10-17T00:45:29Z",
      "eventSource": "cost-optimization-hub.amazonaws.com",
      "eventName": "ListRecommendations",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "requestParameters": {
        "filter": {
          "resourceIdentifiers": [
            "arn:aws:ecs:us-east-1:111122223333:service/
EXAMPLEAccountsIntegrationService-EcsCluster-ClusterEB0386A7-7fsvP2MMmxZ5/
EXAMPLEAccountsIntegrationService-EcsService-Service9571FDD8-Dqm4mPMLstDn"
          ]
        },
        "includeAllRecommendations": false
      },
      "responseElements": null,
      "requestID": "a5b2df72-2cfd-4628-8a72-EXAMPLE7560a",
      "eventID": "a73bef13-6af7-4c11-a708-EXAMPLE6af5c",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "tlsDetails": {
        "clientProvidedHostHeader": "cost-optimization-hub.us-east-1.amazonaws.com"
      }
    }
```

ListRecommendationSummaries

The following example shows a log entry for the `ListRecommendationSummaries` API action.

```
    {
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "EXAMPLEAIZ5FYRFP3POCC",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "userName": "Admin"
          },
          "attributes": {
            "creationDate": "2023-10-16T23:47:55Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-10-17T00:46:16Z",
      "eventSource": "cost-optimization-hub.amazonaws.com",
      "eventName": "ListRecommendationSummaries",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "requestParameters": {
        "groupBy": "ResourceType"
      },
      "responseElements": null,
      "requestID": "ab54e6ad-72fe-48fe-82e9-EXAMPLEa6d1e",
      "eventID": "9288d9fa-939d-4e5f-a49a-EXAMPLEeb14b",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "tlsDetails": {
        "clientProvidedHostHeader": "cost-optimization-hub.us-east-1.amazonaws.com"
      }
    }
```

GetRecommendation

The following example shows a log entry for the `GetRecommendation` API action.

```
    {
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "EXAMPLEAIZ5FYRFP3POCC",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "john-doe": "Admin"
          },
          "attributes": {
            "creationDate": "2023-10-16T23:47:55Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-10-17T00:47:48Z",
      "eventSource": "cost-optimization-hub.amazonaws.com",
      "eventName": "GetRecommendation",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "requestParameters": {
        "recommendationId":
 "EXAMPLEwMzEwODU5XzQyNTFhNGE4LWZkZDItNDUyZi1hMjY4LWRkOTFkOTA1MTc1MA=="
      },
      "responseElements": null,
      "requestID": "e289a76a-182c-4bc9-8093-EXAMPLEbed0e",
      "eventID": "f1ed7ee6-871c-41fd-bb27-EXAMPLE24b64",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "tlsDetails": {
        "clientProvidedHostHeader": "cost-optimization-hub.us-east-1.amazonaws.com"
      }
    }
```

UpdateEnrollmentStatus

The following example shows a log entry for the `UpdateEnrollmentStatus` API action.

```
{
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "EXAMPLEAIZ5FYRFP3POCC",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "john-doe": "Admin"
          },
          "attributes": {
            "creationDate": "2023-10-16T19:11:30Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-10-16T19:12:35Z",
      "eventSource": "cost-optimization-hub.amazonaws.com",
      "eventName": "UpdateEnrollmentStatus",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "requestParameters": {
        "status": "Inactive"
      },
      "responseElements": {
        "status": "Inactive"
      },
      "requestID": "6bf0c8a3-af53-4c4e-8f50-EXAMPLE477f0",
      "eventID": "d2bfa850-ef3d-4317-8ac4-EXAMPLEc16b1",
      "readOnly": false,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "tlsDetails": {
        "clientProvidedHostHeader": "localhost:8080"
      }
    }
```

UpdatePreferences

The following example shows a log entry for the `UpdatePreferences` API action.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC",
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "john-doe": "Admin"
      },
      "attributes": {
        "creationDate": "2023-10-16T19:11:30Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-10-16T19:16:00Z",
  "eventSource": "cost-optimization-hub.amazonaws.com",
  "eventName": "UpdatePreferences",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "PostmanRuntime/7.28.3",
  "requestParameters": {
    "costMetricsType": "AfterDiscounts"
  },
  "responseElements": {
    "costMetricsType": "AfterDiscounts",
    "memberAccountDiscountVisibility": "None"
  },
  "requestID": "01e56ca3-47af-45f0-85aa-EXAMPLE30b42",
  "eventID": "7350ff23-35f5-4760-98b2-EXAMPLE61f13",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "localhost:8080"
  }
}
```

Compliance validation for AWS Cost Management

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs. AWS Cost Management is not in scope of any AWS compliance programs.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS Cost Management is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in AWS Cost Management

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in AWS Cost Management

As a managed service, AWS Cost Management is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access Billing and Cost Management through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Quotas and restrictions

The following table describes the current quotas, restrictions, and naming constraints within AWS Cost Management features.

For a list of quotas and restrictions for features in the AWS Billing console, see Quotas and restrictions in the *AWS Billing User Guide*.

Topics

- Budgets
- Budget reports
- Cost Explorer
- AWS Cost Anomaly Detection
- Savings Plans

Budgets

Number of free budgets with actions per account	2
Number of actions per budget	10
Number of budget actions per account	100
Total number of budgets per management account	20,000
Characters allowed in a budget name	• `0-9` • `A-Z` and `a-z` • `Space` • The following symbols: `_.:/=+-%@`

Budget reports

Maximum number of budget reports	50
Maximum number of budgets per budget report	50
Maximum email recipients in a budget report	50

Cost Explorer

Maximum number of reports that you can save per account	300
Maximum number of filters in the `GetCostAndUsage` operation (API)	100

AWS Cost Anomaly Detection

Maximum number of anomaly monitors you can create for an AWS services monitor type	1 monitor per account
Maximum number of anomaly monitors you can create for other monitor types (linked account, cost category, cost allocation tag)	500 total monitors per management account
Maximum number of anomaly alert subscriptions you can create	100 subscriptions per account
Unsupported services	• AWS Marketplace • AWS Support • WorkSpaces • Cost Explorer • Budgets

	- AWS Shield - Amazon Route 53 - AWS Certificate Manager - Upfront and recurring reserved fee and Savings Plan fees

Savings Plans

Maximum number of daily refresh requests for Savings Plans recommendations per consolidated billing family	3
Maximum number of purchased Savings Plans you can return per calendar year, as long as within seven days of purchase in the same calender month	10 per management account **Note** The management account used when returning the Savings Plan must be the same as the management account that was used to purchase the plan.

Document history

The following table describes the documentation for this release of the AWS Cost Management console.

Change	Description	Date
Added delegated administrator for Cost Optimization Hub	You can delegate a member account in your organization as an administrator for Cost Optimization Hub.	August 6, 2024
Updated AWS managed policy	Cost Optimization Hub updated the CostOptimizationHubServiceRolePolicy.	July 5, 2024
Updated AWS managed policy	Updated the AWSBudgetsReadOnlyAccess policy.	June 17, 2024
Added AWS managed policy	Data Exports added the AWSBCMDataExportsServiceRolePolicy.	June 10, 2024
Launched cost analysis in Amazon Q (preview)	You can use Amazon Q, the generative AI assistant for AWS, to retrieve and analyze your cost data from AWS Cost Explorer.	April 29, 2024
Added AWS managed policy	Split cost allocation data added the SplitCostAllocationDataServiceRolePolicy.	April 16, 2024
Updated AWS managed policy	Updated the AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM policy.	December 14, 2023

Updated AWS managed policies	Cost Optimization Hub updated the following two managed policies: - CostOptimizationHubReadOnlyAccess - CostOptimizationHubAdminAccess	December 14, 2023
Updated documentation	For an overview of your AWS cloud financial management data, use the AWS Billing and Cost Management widgets on the Billing and Cost Management home page. See the following updates: - Using the AWS Billing and Cost Management home page - Understanding the differences between AWS Billing data and AWS Cost Explorer data	November 26, 2023
New Cost Optimization Hub	Added a new Cost Optimization Hub feature that helps you consolidate and prioritize cost optimization recommendations across your AWS accounts and AWS Regions.	November 26, 2023
Added AWS managed policy	Cost Optimization Hub added the CostOptimizationHubServiceRolePolicy.	November 26, 2023

Updated documentation	Updated information about how to use the affected IAM policies tool.	November 17, 2023
Added multi-year and granular data to Cost Explorer	You can now enable up to 38 months of multi-year data (at monthly granularity) and more granular data (at hourly and daily granularity) for the previous 14 days.	November 16, 2023
New AWS Cost Anomaly Detection anomaly monitors limit	Increased the number of anomaly monitors you can create for other monitor types (linked account, cost category, cost allocation tag).	September 12, 2023
New AWS Cost Anomaly Detection configuration by default	Added automatic configuration of AWS Cost Anomaly Detection for all new AWS Cost Explorer users.	March 27, 2023
New AWS Cost Anomaly Detection percentage-based thresholds	Added support for percentage-based thresholds in AWS Cost Anomaly Detection for anomaly alerting.	December 15, 2022
New AWS Cost Anomaly Detection details in alert notifications	Added important details such as account name, monitor name, and monitor type in alert emails, the console, and notifications sent through SNS to Slack or Chime.	December 8, 2022

New templates and tutorials in AWS Budgets	Added a new feature to create a budget using a template with recommended configurations as well as walk-through tutorials to learn about creating different kinds of budgets.	September 27, 2022
New AWS Cost Anomaly Detection history values	Added information about new values in the AWS Cost Anomaly Detection history tab into the AWS Cost Management guide to align with the console.	August 16, 2022
New split-view panel in AWS Budgets	Added a new feature to enhance the console experience by adding a split-view panel that allows you to view budget details without leaving the Budgets Overview page.	June 15, 2022
New AWS Cost Management guide	Split the Billing and Cost Management user guide and aligned the feature details into the Billing guide and AWS Cost Management guide to align with the console.	October 20, 2021
New AWS Cost Anomaly Detection	Added a new AWS Cost Anomaly Detection feature that uses machine learning to continuously monitor your cost and usage to detect unusual spends.	December 16, 2020

New Purchase Order Management	Added a new purchase order feature to configure how your purchases are reflected on your invoices.	October 15, 2020
New Budget Actions	Added a new AWS Budgets actions feature to run an action on your behalf when a budget exceeds a certain cost or usage threshold.	October 15, 2020
New China bank redirect payment method	Added a new payment method that allows China CNY customers using AWS to pay their overdue payments using China Bank Redirect.	February 20, 2020
New security chapter	Added a new security chapter that provides informati on about various security controls. Former "Controlling Access" chapter contents have been migrated here.	February 6, 2020
New reporting method using AWS Budgets	Added a new reporting functionality using AWS Budgets reports.	June 27, 2019
Added normalized units to AWS Cost Explorer	AWS Cost Explorer reports now include normalized units.	February 5, 2019
New payment behavior	AWS India customers can now enable the auto-charge ability for their payments.	December 20, 2018
Updated the AWS Cost Explorer UI	Updated the AWS Cost Explorer UI.	November 15, 2018

Added budget history	Added the ability to see the history of a budget.	November 13, 2018
Expanded budget services	Expanded RI budgets to Amazon OpenSearch Service.	November 8, 2018
Added a new payment method	Added the SEPA Direct Debit payment method.	October 25, 2018
Redesigned budget experience	Updated the budget UI and workflow.	October 23, 2018
New Reserved Instance recommendation columns	Added new columns to the AWS Cost Explorer RI recommendations.	October 18, 2018
Added a new Reserved Instance report	Expanded RI reports to Amazon OpenSearch Service.	October 10, 2018
AWS Cost Explorer walkthrough	AWS Cost Explorer now provides a walkthrough for the most common functionality.	September 24, 2018
Added a new payment method	Added the ACH Direct Debit payment method.	July 24, 2018
Added RI purchase recommendations for additional services	Added RI purchase recommendations for additional services in AWS Cost Explorer.	July 11, 2018
Added RI purchase recommendations for linked accounts	Added RI purchase recommendations for linked accounts in AWS Cost Explorer.	June 27, 2018
Added AWS CloudFormation for budgets	Added Budgets templates for AWS CloudFormation.	May 22, 2018

Updated RI allocation behavior for linked accounts	Updated the RI allocation behavior size-flexible RI for linked accounts.	May 9, 2018
RI coverage alerts	Added RI coverage alerts.	May 8, 2018
Unblend linked account bills	Linked account bills no longer show the blended rate for the organization.	May 7, 2018
Added Amazon RDS recommendations to AWS Cost Explorer	Added Amazon RDS Recommendations to AWS Cost Explorer.	April 19, 2018
Added a new AWS Cost Explorer dimension and AWS Cost and Usage Reports line item	Added a new AWS Cost Explorer dimension and AWS Cost and Usage Reports line item.	March 27, 2018
Added purchase recommendations to the AWS Cost Explorer API	Added access to the Amazon EC2 Reserved Instance (RI) purchase recommendations via the AWS Cost Explorer API.	March 20, 2018
Added RI coverage for Amazon RDS, Amazon Redshift, and ElastiCache	Reserved Instance (RI) coverage for Amazon RDS, Amazon Redshift, and ElastiCache .	March 13, 2018
Added RI coverage to the AWS Cost Explorer API	Added `GetReservationCoverage` to the AWS Cost Explorer API.	February 22, 2018
RI recommendations	Added RI recommendations based on previous usage.	November 20, 2017
AWS Cost Explorer API	Enabled programmatic access to AWS Cost Explorer via API.	November 20, 2017

RI utilization alerts for additional services	Added notifications for additional services.	November 10, 2017
Added RI reports	Expanded RI reports to Amazon RDS, Redshift, and ElastiCache.	November 10, 2017
Discount sharing preferences	Updated preferences so that AWS credits and RI discount sharing can be turned off.	November 6, 2017
RI utilization alerts	Added notifications for when RI utilization drops below a preset percentage-based threshold.	August 21, 2017
Updated AWS Cost Explorer UI	Released a new AWS Cost Explorer UI.	August 16, 2017
AWS Marketplace data integration	Added AWS Marketplace so that customers can see their data reflected in all billing artifacts, including the Bills page, AWS Cost Explorer, and more.	August 10, 2017
Linked account access and usage type groups in budgets	Added support for creating cost and usage budgets based on specific usage types and usage type groups, and extended budget creation capabilities to all account types.	June 19, 2017

Added AWS Cost Explorer advanced options	You can now filter AWS Cost Explorer reports by additional advanced options, such as refunds, credits, RI upfront fees, RI recurring charges, and support charges.	March 22, 2017
Added a AWS Cost Explorer report	You can now track your Reserved Instance (RI) coverage in AWS Cost Explorer.	March 20, 2017
Added AWS Cost Explorer filters	You can now filter AWS Cost Explorer reports by tenancy, platform, and the Amazon EC2 Spot and Scheduled Reserved Instance purchase options.	March 20, 2017
AWS Cost Explorer and budgets for AWS India	AWS India users can now use AWS Cost Explorer and budgets.	March 6, 2017
Added grouping for AWS Cost Explorer usage types	AWS Cost Explorer supports grouping for both cost and usage data, enabling customers to identify their cost drivers by cross-referencing their cost and usage charts.	February 24, 2017
Added a AWS Cost Explorer report	You can now track your monthly Amazon EC2 Reserved Instance (RI) utilization in AWS Cost Explorer.	December 16, 2016

Added a AWS Cost Explorer report	You can now track your daily Amazon EC2 Reserved Instance (RI) utilization in AWS Cost Explorer.	December 15, 2016
Added AWS Cost Explorer advanced options	You can now exclude tagged resources from your AWS Cost Explorer reports.	November 18, 2016
Expanded budget functiona lity	You can now use budgets to track usage data.	October 20, 2016
Expanded AWS Cost Explorer functionality	You can now use AWS Cost Explorer to visualize your costs by usage type groups.	September 15, 2016
AWS Cost Explorer report manager	You can now save AWS Cost Explorer queries.	November 12, 2015
Budgets and forecasting	You can now manage your AWS usage and costs using budgets and cost forecasts.	June 29, 2015
Amazon Web Services India Private Limited	You can now manage your account settings and payment methods for an Amazon Web Services India Private Limited (AWS India) account.	June 1, 2015
Expanded AWS Cost Explorer functionality	You can now use AWS Cost Explorer to visualize your costs by Availability Zone, API operation, purchase option, or multiple cost allocation tags.	February 19, 2015
Preferred payment currencies	You can now change the currency associated with your credit card.	February 16, 2015

Expanded AWS Cost Explorer functionality	You can now use AWS Cost Explorer to visualize your costs by Amazon EC2 instance type or region.	January 5, 2015
User permissions	You can now enable federated users or roles to access and manage your account settings, view your bills, and perform cost managemen t. For example, you can grant people in your finance department full access to the financial setup and control of your AWS account, without having to give them access to your production AWS environment.	July 7, 2014
AWS Cost Explorer launched	AWS Cost Explorer provides a visualization of your AWS costs that enables you to analyze your costs in multiple ways.	April 8, 2014
Version 2.0 published for the Billing guide	The *AWS Billing User Guide* has been reorganized and rewritten to use the new Billing and Cost Management console.	October 25, 2013

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.