Troubleshoot network connectivity by sending Google Cloud VPC Flow Logs to New Relic

Google Cloud Virtual Private Cloud (VPC) Flow Logs supports frictionless transmission of logs to New Relic. With VPC Flow Logs from across your Google Cloud estates, you can quickly understand key insights for performance analytics and troubleshooting network connectivity

Customers today are increasingly deploying cloud-based applications built using microservices and distributed architectures. With such applications, customers need systematic and actionable observability to track the behavior and interactions of their microservices, and to optimize and troubleshoot in a consistent, frictionless manner.

Flow logs provide valuable information about network traffic, helping organizations understand how data flows within their infrastructure. Using New Relic, customers now have enhanced visibility and detailed information about network traffic within their Google Cloud environment, so they can organize their network entities, monitor their performance, and discover how the network is affecting their systems

2X ROI

Using observability solutions

VPC Flow Logs in New Relic eliminates one more blind spot for engineers

New Relic provides observability enabling users to debug and optimize across the entire stack. Flow logs play an integral role in full stack monitoring by providing valuable information on network traffic. Alongside application and infrastructure telemetry, customers can now get insights for performance analytics and pinpoint whether an issue is related to the network.

Customers can now easily send Google Cloud VPC Flow Logs to New Relic to 1) monitor and issue alerts on network traffic between VM instances regardless of the underlying account or region, 2) monitor performance metrics like the number of bytes and packets exchanged across TCP or UDP ports, 3) explore flow log deviations that indicate changes or degradation of network health, and 4) perform security analysis and intrusion detection by analysing unauthorized activity or any compromised IPs.

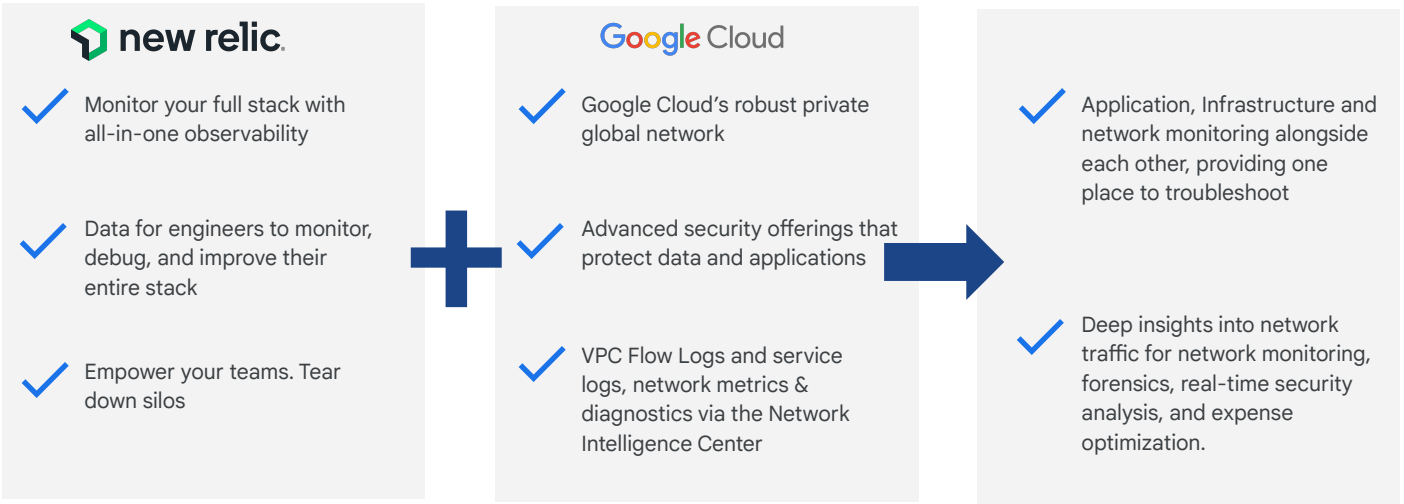
By being able to visualize and analyse network traffic via New Relic, teams have one place to troubleshoot and resolve performance issues in their Google Cloud environment. This is one more step in eliminating blind spots for developers, operators and SRE teams

To unlock cloud-scale observability, engineers need to explore VPC performance and connectivity across multiple accounts and regions, rapidly pivoting on both facets and context, before diving into analyzing related endpoints to answer “Is it the network?”

To solve this, we’ve streamlined the delivery of VPC flow logs by allowing you to send them to New Relic, which can reduce costs and pipeline complexity. With our simple Add Data interface, it only takes moments to configure VPC flow logs.

Instead of digging through raw logs across multiple accounts, engineers can begin with and explore the data that matters, regardless of account or region.

new relic. Google Cloud



Explore changes in network performance

New Relic will capture and list changes in flow logs in the "deviating attributes" sidebar. You can visualize all facets of your network traffic like bytes, packets per second, accepts and reject per second across known applications for TCP and UDP ports.

Using our curated views in "New Relic Explorer", you can quickly narrow in on the VMs where there is an unexpected change in traffic volume or health.

Using our "Lookout" view you can identify variances by egress/ingress bytes and unique sources/destinations.

Visualize across Google Cloud

Our New Relic "Navigator" gives you a high density overview of your entire system, which helps detect any issues and health patterns at a glance.

Group networks by health and other metadata to find where alerts were triggered and see overlaid performance metrics.

Know the state of your system in real time and find issues fast with Navigator's stoplight style shading to indicate each entity's health.

Explore VMs across regions, availability zones, and accounts. The network monitoring experience provides curated insights into traffic patterns and changes in packet loss in a single view.

Monitor and issue alerts

See details of communications between hosts and other services through source and destination IP address and port, metadata that describes both endpoints, key network performance telemetry, and the state of a specific communication attempt.

Detect and diagnose incidents and prioritize them for immediate action.

Our Sankey diagram view automatically links to known hosts monitored through the New Relic infrastructure agent. With facets including instanceId and IP address, a single click will show an overview of the host, including triggered alerts and events, tags, golden metrics, and other critical data points.

Monitor network performance, narrow down network issues, easily troubleshoot and identify malicious activity using the New Relic and Google Cloud VPC Flow Logs integration