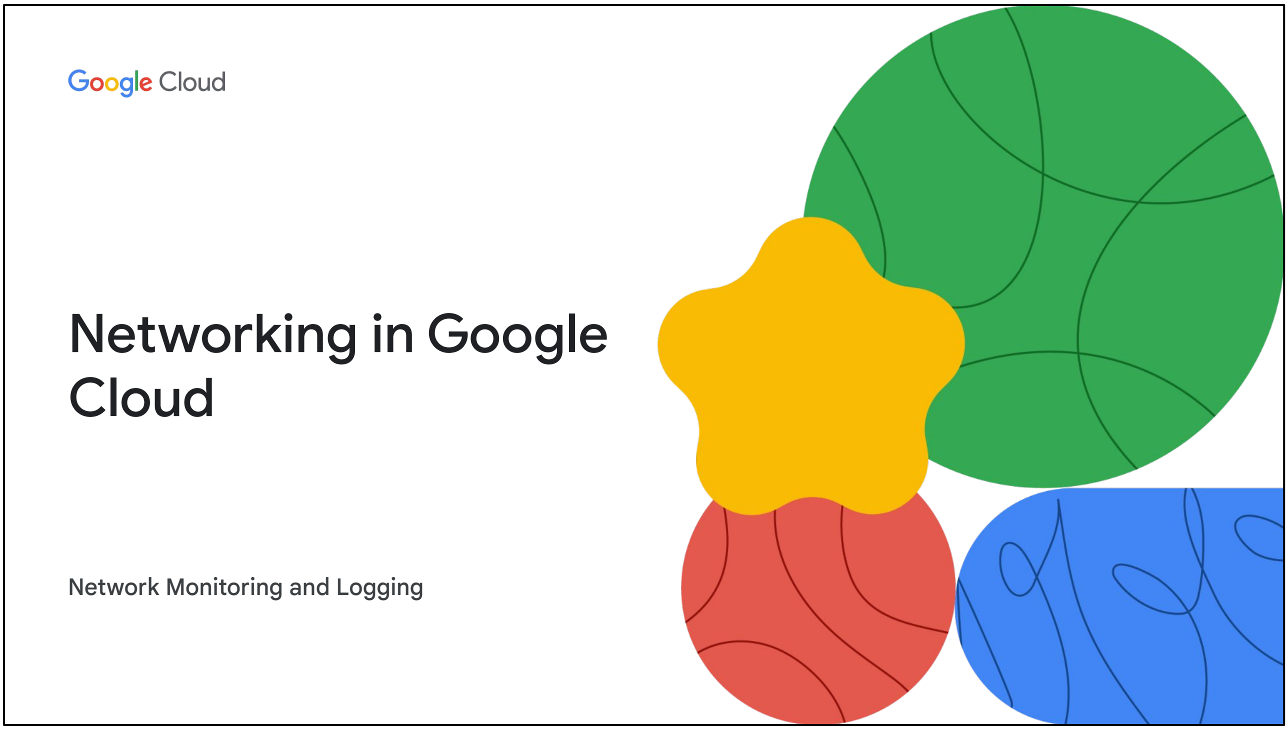
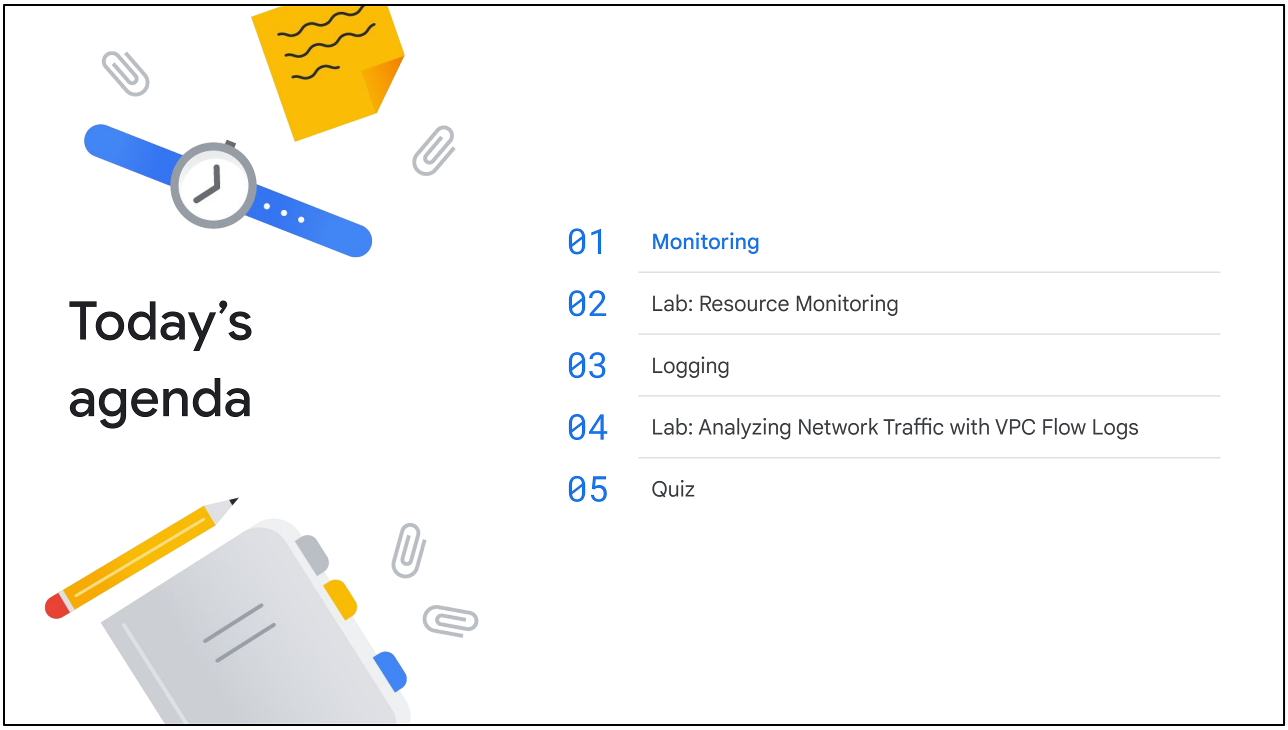


Google Cloud

Networking in Google Cloud

Network Monitoring and Logging

Welcome to the Network Monitoring and Logging module.



Today's agenda

01 Monitoring

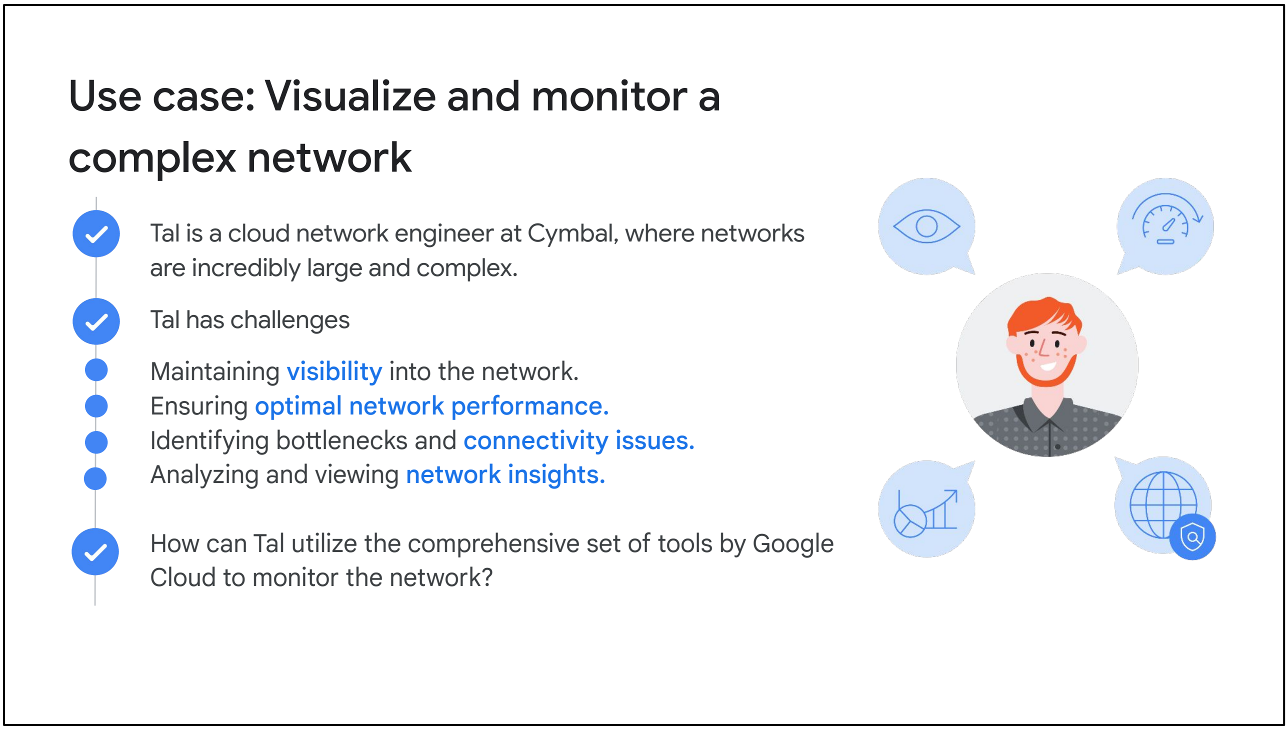
02 Lab: Resource Monitoring

03 Logging

04 Lab: Analyzing Network Traffic with VPC Flow Logs

05 Quiz

In this module, we will cover Google Cloud network monitoring and logging features that can help you troubleshoot your Google Cloud networking services. You implement monitoring and logging in two separate lab exercises. At the end of the module, you will test your knowledge by taking a brief quiz.



Use case: Visualize and monitor a complex network

- ✓ Tal is a cloud network engineer at Cymbal, where networks are incredibly large and complex.
- ✓ Tal has challenges
  - Maintaining **visibility** into the network.
  - Ensuring **optimal network performance.**
  - Identifying bottlenecks and **connectivity issues.**
  - Analyzing and viewing **network insights.**
- ✓ How can Tal utilize the comprehensive set of tools by Google Cloud to monitor the network?

Before we dive deep into monitoring, let us take a look at a scenario.

Tal is a cloud network engineer at Cymbal, where networks are incredibly large and complex. There are multiple VPCs and multiple interconnections used and monitored by various team.

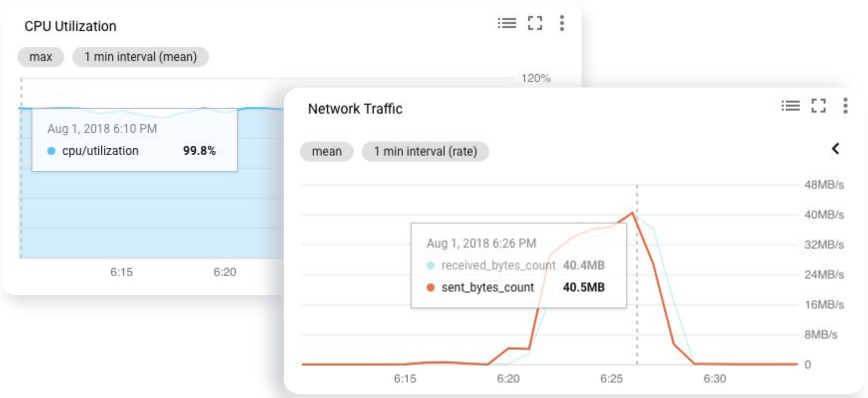
Tal faces challenges with

1. Maintaining visibility into the network.
2. Ensuring optimal network performance.
3. Identifying bottlenecks and connectivity issues.
4. Analyzing and viewing network insights.

With growing complexity, Tal can benefit with a solution to streamline network monitoring and gain actionable insights.

Let’s explore the comprehensive set of tools that Tal can utilize to monitor the network.

Dashboards can show utilization and network traffic

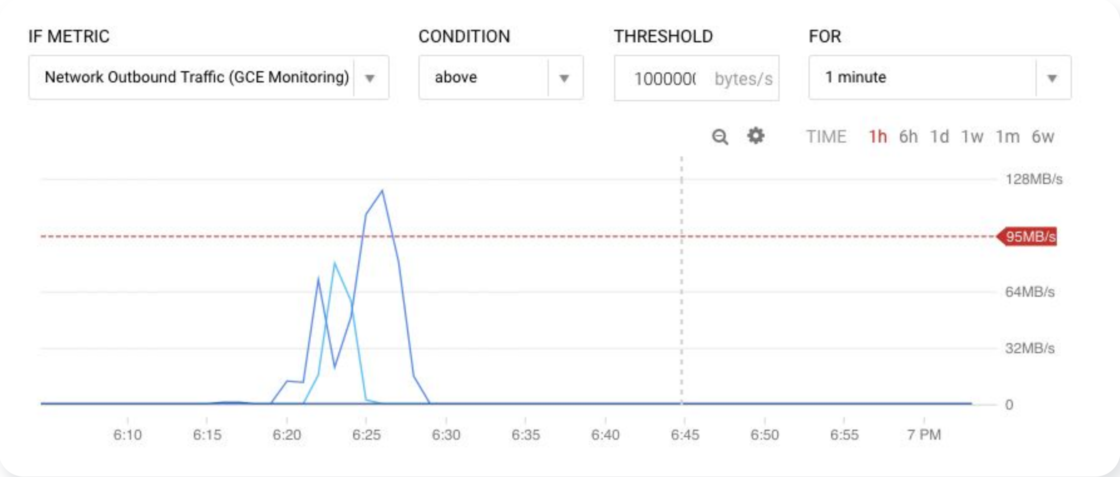


To have visibility into the network, Tal can use Google Cloud monitoring to create custom dashboards that contain charts of the metrics that he wants to monitor. For example, Tal can create charts that display instances' CPU utilization, the packets or bytes sent and received by those instances, and the packets or bytes dropped by the firewall of those instances.

In other words, charts provide **visibility into the utilization and network traffic** of your VM instances, as shown on this slide. These charts can be customized with filters to remove noise, groups to reduce the number of time series, and aggregates to group multiple time series together.

For a full list of supported metrics, please refer to the documentation: https://cloud.google.com/monitoring/api/metrics_Google Cloud.

Alerting policies can notify you of certain conditions



IF METRIC: Network Outbound Traffic (GCE Monitoring)

CONDITION: above

THRESHOLD: 100000(bytes/s

FOR: 1 minute

Now, although charts are extremely useful, they can only provide insight while someone is looking at them.

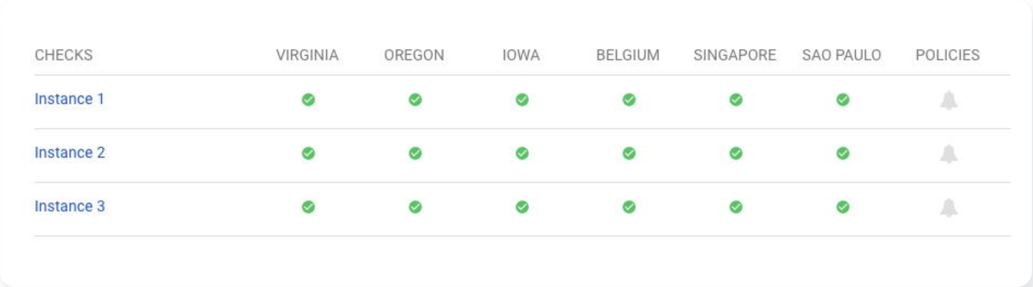
But what if Tal's server goes down in the middle of the night or over the weekend? Tal is not always available to look at dashboards and determine whether the servers are available or have enough capacity or bandwidth.

To solve that, Tal can create alerting policies that **notify when specific conditions are met**. An alerting policy, which describes the circumstances under which you want to be alerted and how you want to be notified about an incident. The alerting policy can monitor time-series data stored by Cloud Monitoring or logs stored by Cloud Logging. When that data meets the alerting policy condition, Cloud Monitoring creates an incident and sends the notifications.

For example, as shown on this slide, Tal can create an alerting policy when the network egress of your VM instance goes above a certain threshold for a specific timeframe.

When this condition is met, you or someone else can be automatically notified through email, SMS, or other channels in order to troubleshoot this issue.

Uptime checks test the availability of your public services



CHECKS	VIRGINIA	OREGON	IOWA	BELGIUM	SINGAPORE	SAO PAULO	POLICIES
Instance 1	✓	✓	✓	✓	✓	✓	🔔
Instance 2	✓	✓	✓	✓	✓	✓	🔔
Instance 3	✓	✓	✓	✓	✓	✓	🔔

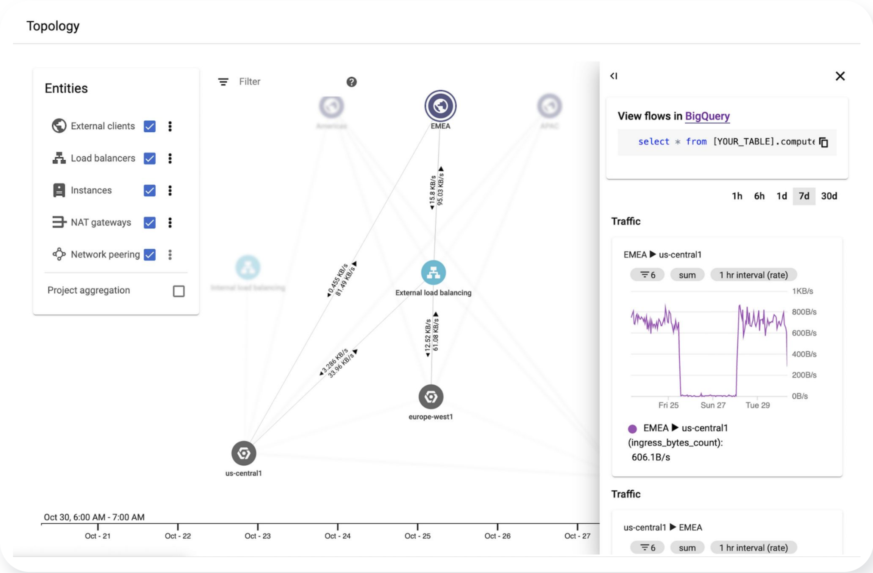
There are also uptime checks that Tal can configure to **test the availability** of public services from locations around the world, as you can see on this slide.

The type of uptime check can be set to HTTP, HTTPS, or TCP.

The resource to be checked can be an App Engine application, a Compute Engine instance, a URL of a host, or an AWS instance or load balancer.

For each uptime check, you can create an alerting policy and view the latency of each global location. Checking uptime time helps in monitoring and maintaining Service Level Indicator, Service Level Agreement, and Service Level Objective for availability.

Network Intelligence Center



```
select * from [YOUR_TABLE].compute
```

Seventy five percent of network outages happen due to misconfiguration. More often than not, these misconfigurations are discovered in production.

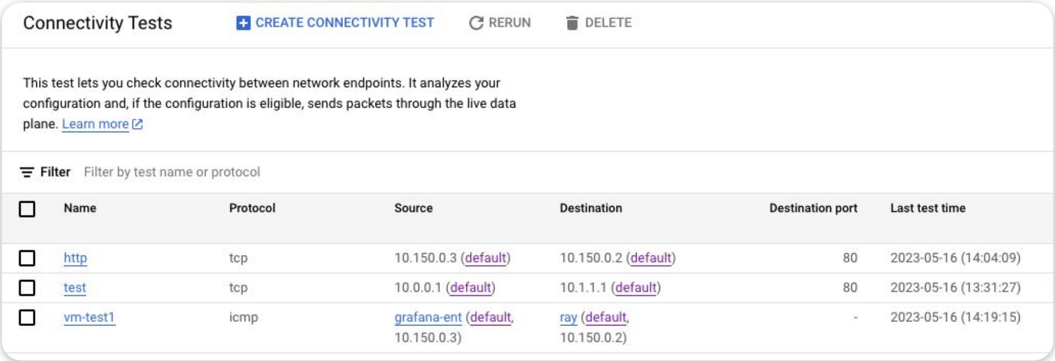
Not knowing the impact of making a configuration change in firewall rules or routing rules makes network monitoring reactive rather than proactive, introducing risk and extending mean time to resolution.

Network Intelligence Center enables Tal to **prevent networking outages and performance issues** before they happen.

Centralized monitoring cuts down troubleshooting time and effort, increases network security, and improves the overall user experience.

Network Intelligence Center modules offer **network topology visualization, network connectivity tests, a performance dashboard and firewall insights.**

Diagnose issues using Connectivity Tests



This test lets you check connectivity between network endpoints. It analyzes your configuration and, if the configuration is eligible, sends packets through the live data plane. Learn more

□	Name	Protocol	Source	Destination	Destination port	Last test time
□	http	tcp	10.150.0.3 (default)	10.150.0.2 (default)	80	2023-05-16 (14:04:09)
□	test	tcp	10.0.0.1 (default)	10.1.1.1 (default)	80	2023-05-16 (13:31:27)
□	vm-test1	icmp	grafana-ent (default, 10.150.0.3)	ray (default, 10.150.0.2)	-	2023-05-16 (14:19:15)

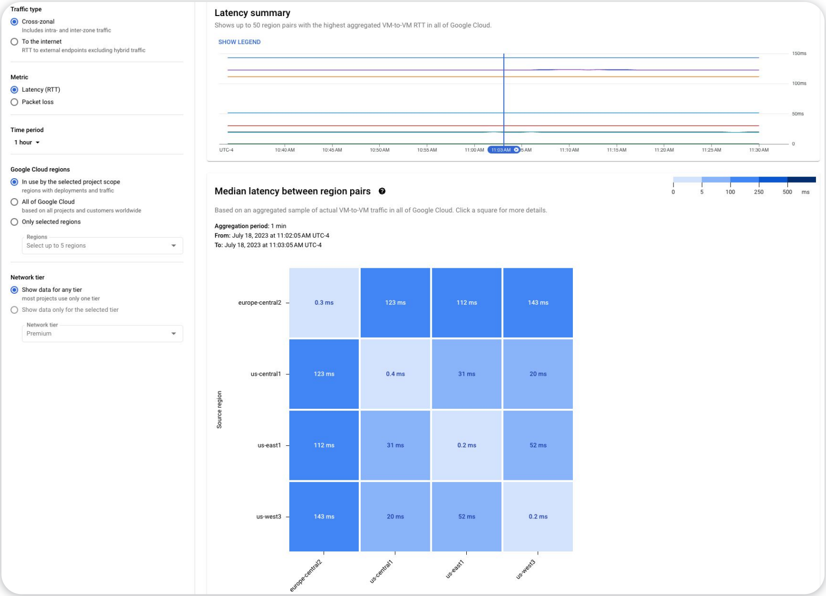
When a virtual machine is unreachable, Tal may need to diagnose the connectivity issue quickly to prevent any issues. For example, there may be an issue between source and destination endpoints in your VPC network.

Using the Network Intelligence Center Connectivity Tests, Tal can **self-diagnose connectivity issues** within Google Cloud or Google Cloud to an external IP address which could be on-premises or on another cloud, helping to isolate whether the issue is in Google Cloud or not.

Tal can create, save and run tests to help verify the impact of configuration changes and ensure that network intent captured by these tests is not violated, proactively preventing network outages.

These tests also help assure network security and compliance. Connectivity Tests has been used internally by the Google Cloud support team to resolve customer issues.

Performance Dashboard



Traffic type

● Cross-zonal
Includes intra- and inter-zone traffic

○ To the internet
RTT to external endpoints excluding hybrid traffic

Metric

● Latency (RTT)

○ Packet loss

Time period

1 hour ▾

Google Cloud regions

● In use by the selected project scope
regions with deployments and traffic

○ All of Google Cloud
based on all projects and customers worldwide

○ Only selected regions

Regions
Select up to 5 regions ▾

Network tier

● Show data for any tier
most projects use only one tier

○ Show data only for the selected tier

Network tier
Premium ▾

Latency summary

Shows up to 50 region pairs with the highest aggregated VM-to-VM RTT in all of Google Cloud.

Median latency between region pairs

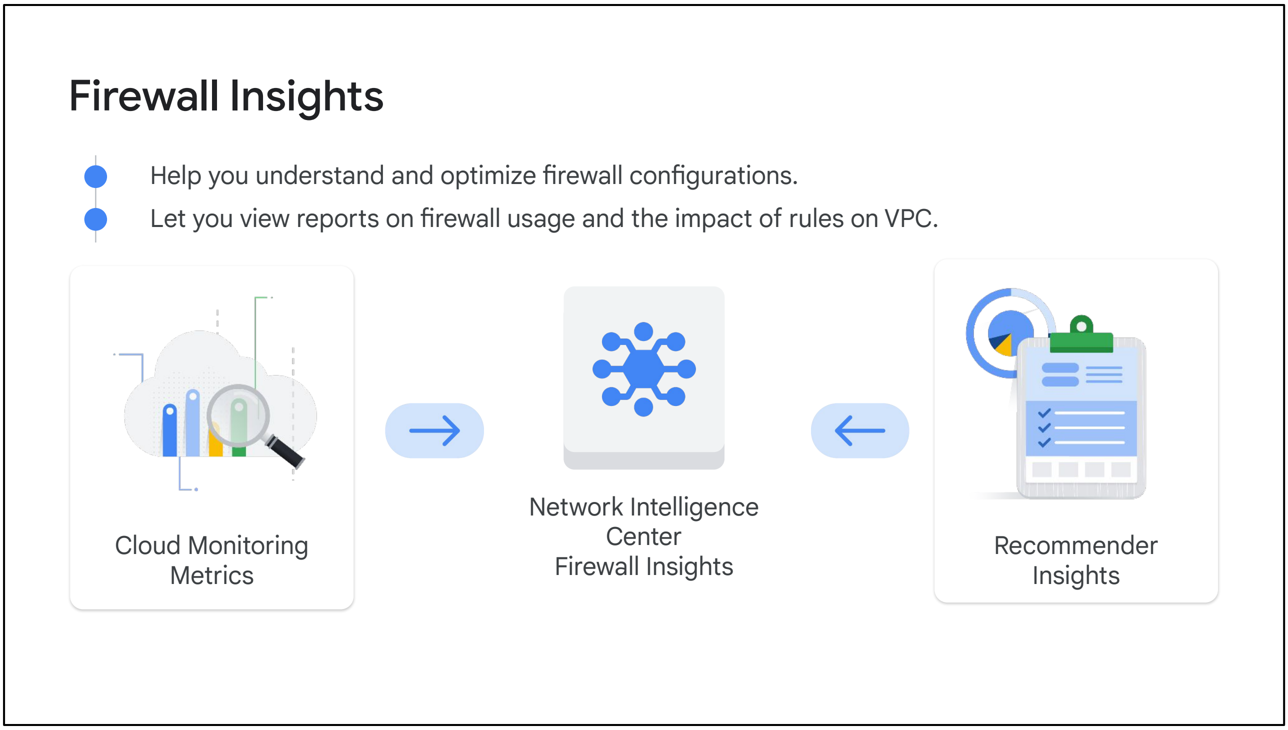
Based on an aggregated sample of actual VM-to-VM traffic in all of Google Cloud. Click a square for more details.

Aggregation period: 1 min
From: July 18, 2023 at 11:02:05 AM UTC-4
To: July 18, 2023 at 11:03:05 AM UTC-4

Source region	europe-central2	us-central1	us-east1	us-west3
europe-central2	0.3 ms	123 ms	112 ms	143 ms
us-central1	123 ms	0.4 ms	31 ms	20 ms
us-east1	112 ms	31 ms	0.2 ms	52 ms
us-west3	143 ms	20 ms	52 ms	0.2 ms

How can Tal diagnose if the application or the underlying network is the root cause of the issues?

Network Intelligence Center’s Performance Dashboard can show you **real-time performance metrics** (latency and packet loss) between the zones where you have VMs, enabling you to quickly troubleshoot where the packet loss is happening, and indeed, if it’s a networking issue at all. Performance Dashboard now shows customer project information and also Google Cloud general information.



Firewall Insights

- Help you understand and optimize firewall configurations.
- Let you view reports on firewall usage and the impact of rules on VPC.

Cloud Monitoring Metrics → Network Intelligence Center Firewall Insights ← Recommender Insights

Firewall configuration can be daunting. How can Tal verify that firewall rules are being used in the intended way?

Firewall Insights enables you to better understand and safely **optimize firewall configurations**.

Firewall Insights provides reports that contain information about firewall usage and the impact of various firewall rules on your Virtual Private Cloud (VPC) network. Make sure to enable Firewall Rules Logging to view the reports.

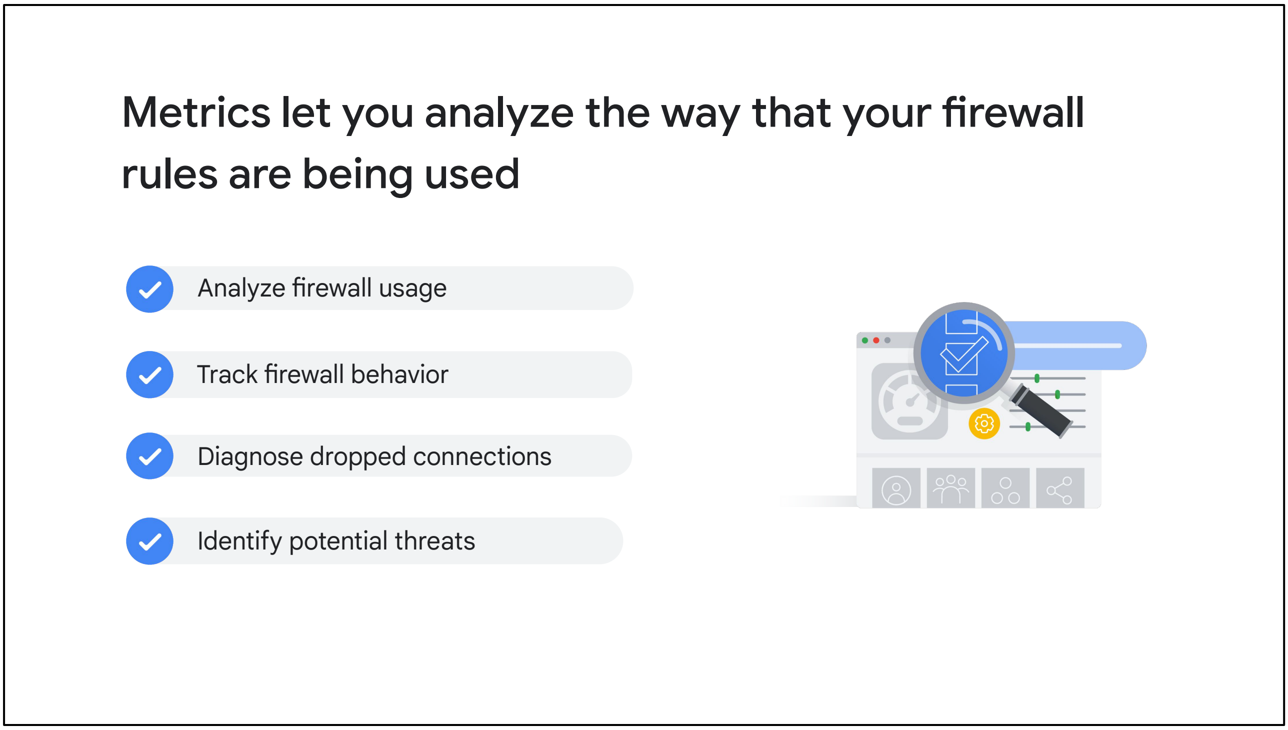
Firewall Insights uses Cloud Monitoring metrics and Recommender insights.

Cloud Monitoring collects measurements to help you understand how your applications and system services are performing. A collection of these measurements is generically called a metric. The applications and system services being monitored are called monitored resources. Measurements might include the latency of requests to a service, the amount of disk space available on a machine, the number of tables in your SQL database, the number of widgets sold, and so forth.

Recommender is a service that provides recommendations and insights for using resources on Google Cloud. These recommendations and insights are per-product or per-service, and are generated based on heuristic methods, machine learning, and current resource usage. You can use insights independently from recommendations. Each insight has a specific insight type. Insight types are specific to a single Google

Cloud product and resource type.

For more information on:
Using Cloud Monitoring for metrics:
https://cloud.google.com/monitoring/api/v3/metrics.
Using Recommender for insights:
https://cloud.google.com/recommender/docs/insights/using-insights.



Metrics let you analyze the way that your firewall rules are being used

- ✓ Analyze firewall usage
- ✓ Track firewall behavior
- ✓ Diagnose dropped connections
- ✓ Identify potential threats

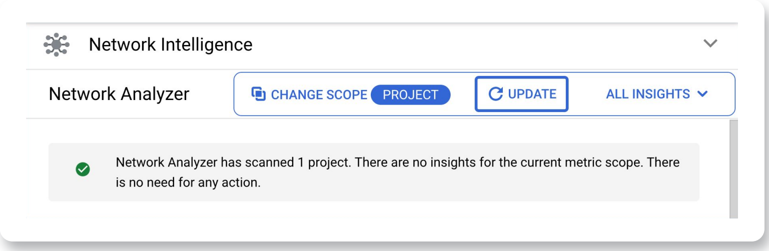
Firewall Insights metrics let Tab **analyze the way firewall rules are being used**. Firewall Insights metrics are available through Cloud Monitoring and Google Cloud Console. Metrics are derived through Firewall Rules Logging.

With Firewall Insights metrics, you can perform the following tasks:

- Analyze firewall rule usage. Determine if firewall rules are functioning as expected.
- Track connection behavior. Verify that firewall rules are permitting or blocking the correct traffic over defined time intervals.
- Diagnose dropped connections. Investigate connections that may be unintentionally blocked by firewall rules.
- Identify potential threats. Detect anomalies in firewall rule hit counts, which could indicate malicious network activity.

Network Analyzer

- Automatically monitors your VPC network configurations and detects misconfigurations and suboptimal configurations.
- Provides insights on network topology, firewall rules, routes, configuration dependencies, and connectivity to services and applications.
- Identifies network failures, provides root cause information, and suggests possible resolutions.

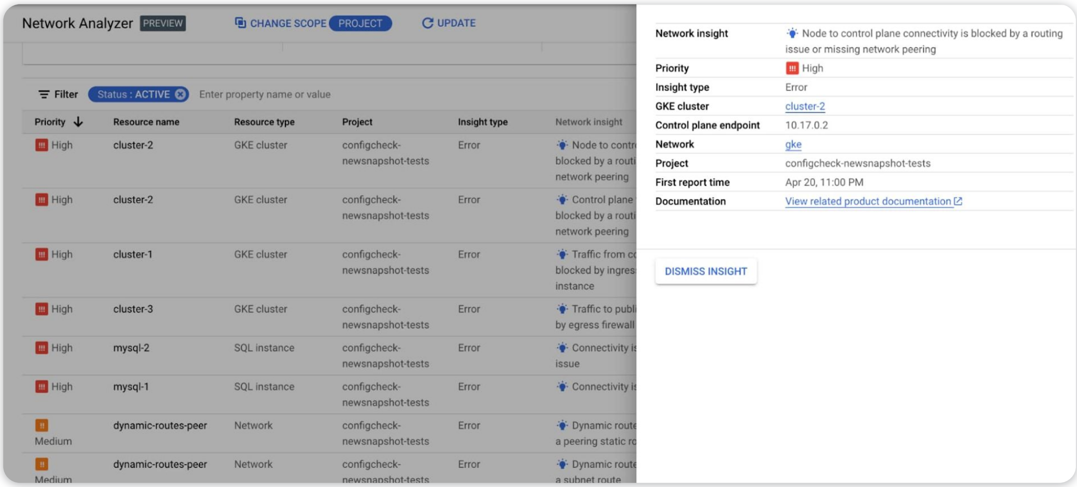


✓ Network Analyzer has scanned 1 project. There are no insights for the current metric scope. There is no need for any action.

Network Analyzer automatically monitors your VPC network configurations and detects misconfigurations and suboptimal configurations. It provides insights on network topology, firewall rules, routes, configuration dependencies, and connectivity to services and applications. It identifies network failures, provides root cause information, and suggests possible resolutions.

Network Analyzer runs continuously and triggers relevant analyses based on near-real-time configuration updates in your network. If a network failure is detected, it tries to correlate the failure with recent configuration changes to identify root causes. Wherever possible, it provides recommendations to fix the issues.

Network Analyzer sample insight

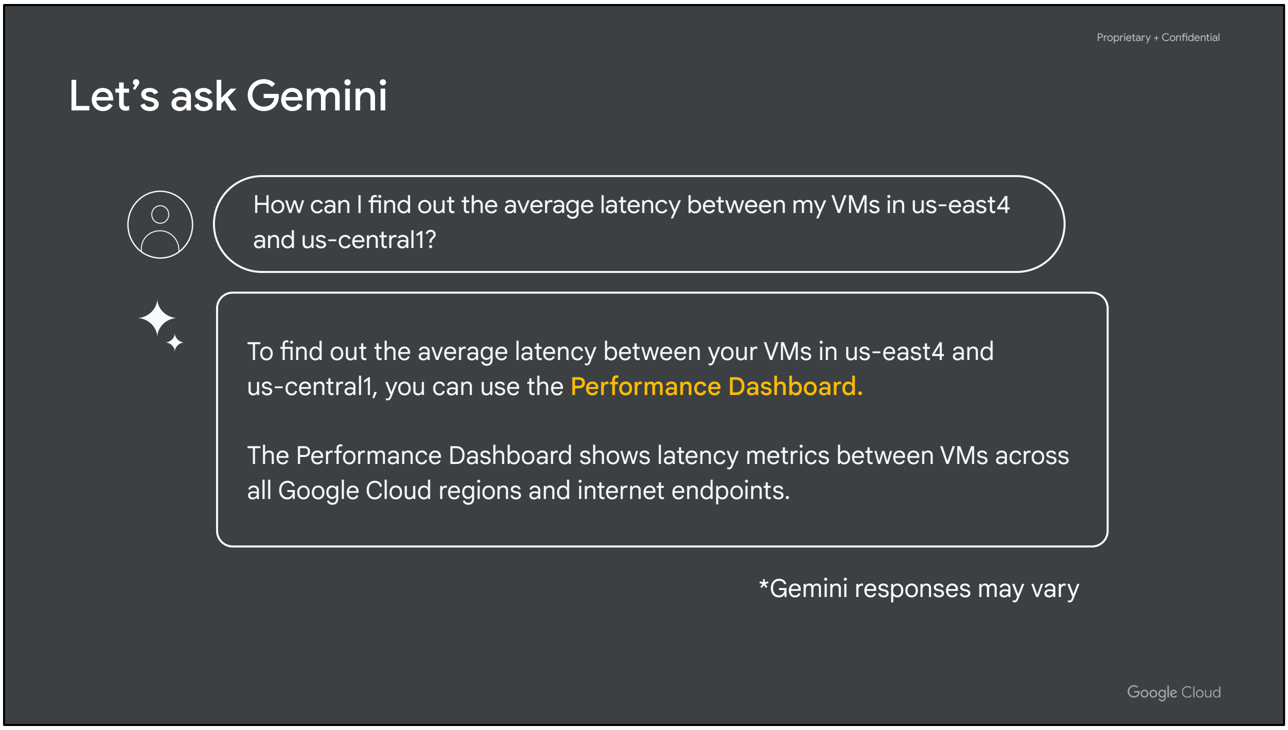


Priority ↓	Resource name	Resource type	Project	Insight type	Network insight
High	cluster-2	GKE cluster	configcheck-newsnapshot-tests	Error	Node to contr blocked by a routi network peering
High	cluster-2	GKE cluster	configcheck-newsnapshot-tests	Error	Control plane blocked by a routi network peering
High	cluster-1	GKE cluster	configcheck-newsnapshot-tests	Error	Traffic from co blocked by ingres instance
High	cluster-3	GKE cluster	configcheck-newsnapshot-tests	Error	Traffic to publi by egress firewall
High	mysql-2	SQL instance	configcheck-newsnapshot-tests	Error	Connectivity is issue
High	mysql-1	SQL instance	configcheck-newsnapshot-tests	Error	Connectivity is
Medium	dynamic-routes-peer	Network	configcheck-newsnapshot-tests	Error	Dynamic route a peering static ro
Medium	dynamic-routes-peer	Network	configcheck-newsnapshot-tests	Error	Dynamic route a subnet route

Network insight	Node to control plane connectivity is blocked by a routing issue or missing network peering
Priority	High
Insight type	Error
GKE cluster	cluster-2
Control plane endpoint	10.17.0.2
Network	gke
Project	configcheck-newsnapshot-tests
First report time	Apr 20, 11:00 PM
Documentation	View related product documentation

In the example above, an insight of the type *Error*, a GKE node to control plane connectivity is generated. The insight page also describes the following:

- The root cause: an ingress firewall rule is blocking the connection between the node and the plane. This indicated that the default firewall rules were modified, removed, or shadowed by another firewall rule.
- A solution: if the root of the problem is a deleted firewall, create a new firewall rule. If it's a shadowed firewall rule, then increase the priority.



Let’s ask Gemini

How can I find out the average latency between my VMs in us-east4 and us-central1?

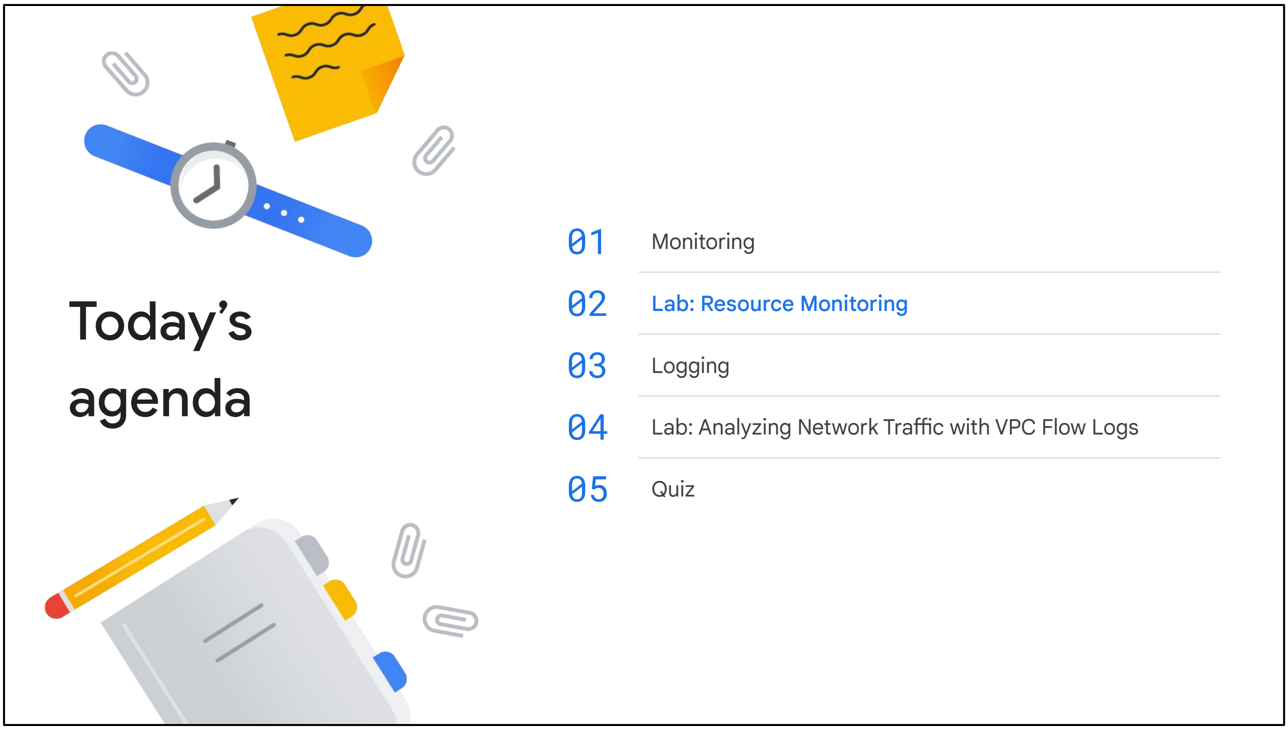
To find out the average latency between your VMs in us-east4 and us-central1, you can use the **Performance Dashboard.**

The Performance Dashboard shows latency metrics between VMs across all Google Cloud regions and internet endpoints.

*Gemini responses may vary

You can use Gemini if you are unsure of where to find a particular performance metric. For example, you can ask Gemini how to find out the average latency between my VMs in us-east4 and us-central1?

Gemini will assist you with the Dashboard name and its purpose.



Today's agenda

01 Monitoring

02 **Lab: Resource Monitoring**

03 Logging

04 Lab: Analyzing Network Traffic with VPC Flow Logs

05 Quiz

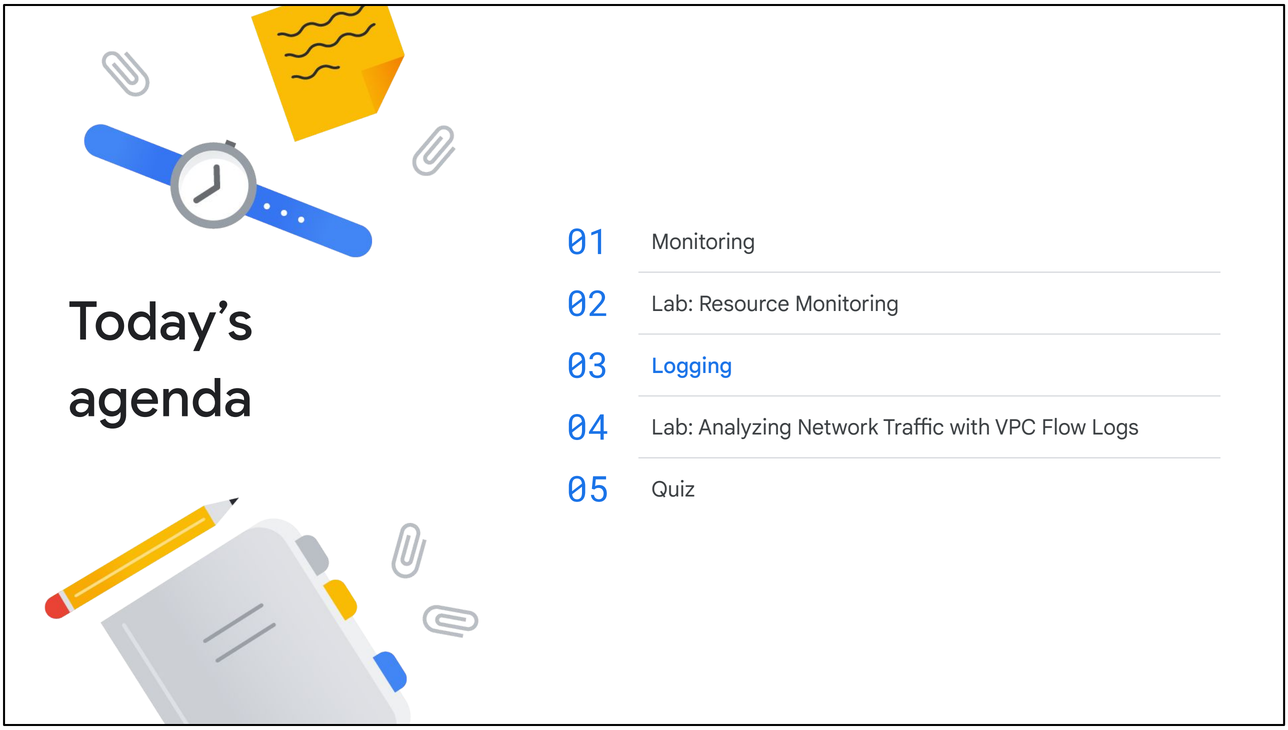
Now, it’s your turn to monitor resources in Google Cloud.

Lab intro

Resource Monitoring

In this lab, you learn how to:

- Explore Cloud Monitoring.
- Add charts to dashboards.
- Create alerts with multiple conditions.
- Create resource groups.
- Create uptime checks.



Today's agenda

01 Monitoring

02 Lab: Resource Monitoring

03 **Logging**

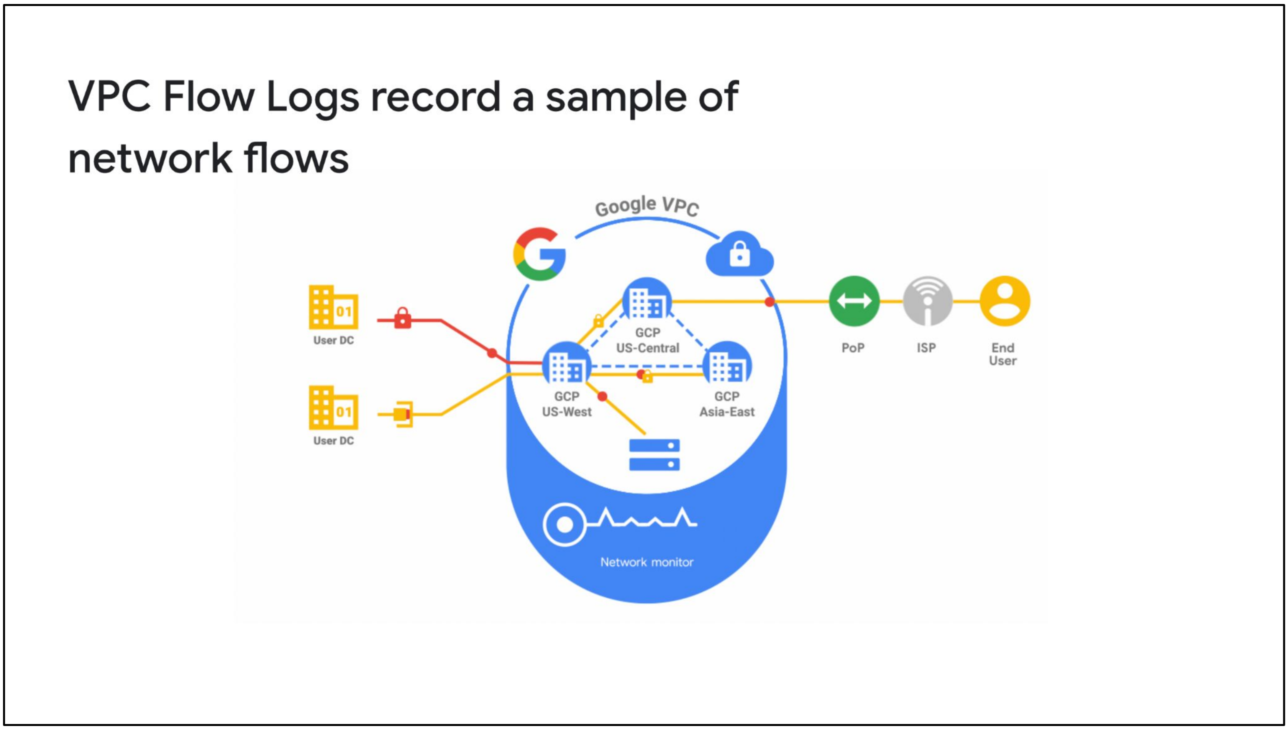
04 Lab: Analyzing Network Traffic with VPC Flow Logs

05 Quiz

Next, let's talk about Logging.

Now, you have already been exposed to Cloud Logging throughout this course.

In this module, we'll focus on VPC Flow Logs and exporting your logs to BigQuery and Looker Studio so that you can analyze and visualize your logs.



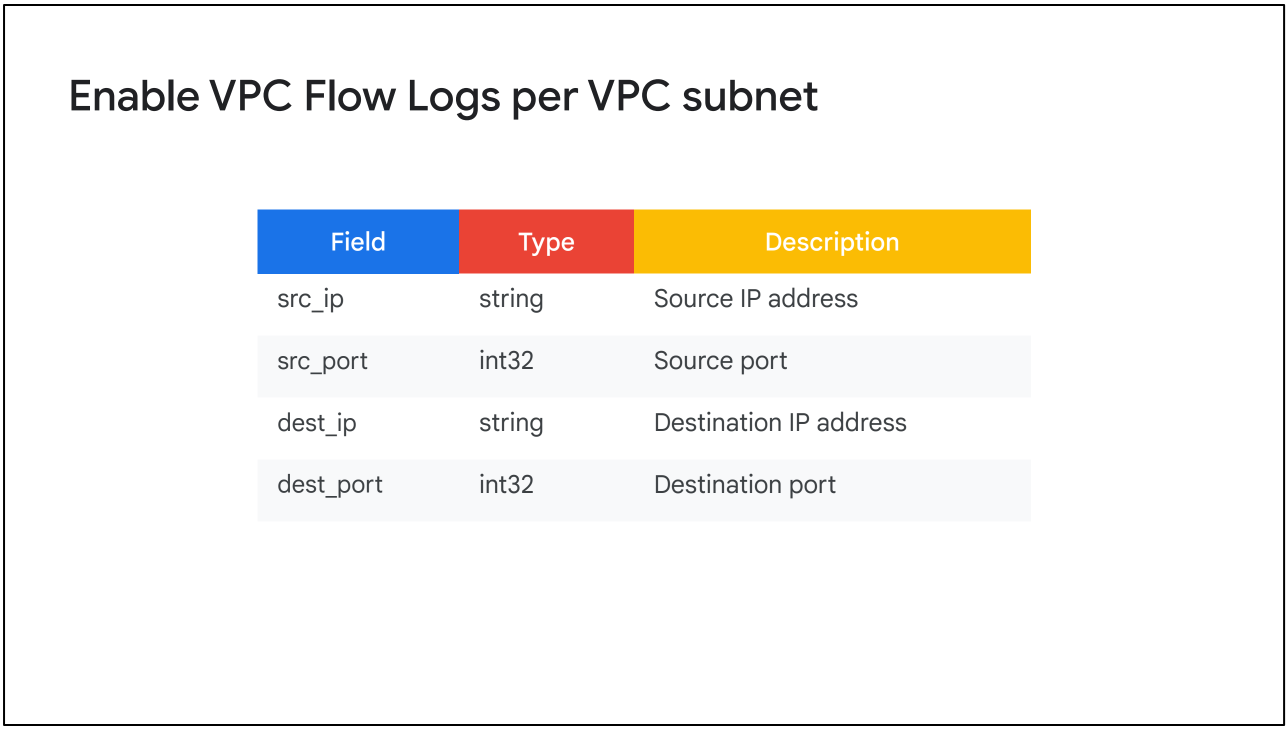
VPC Flow Logs record a sample of network flows

VPC Flow Logs records a sample of network flows sent from and received by VM instances, as you can see in this animation.

These logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization.

Google Cloud is unique for its near-real-time visibility, providing log updates every 5 seconds. Also, there is no extra delay and no performance penalty in routing the logged IP packets to their destination.
DNS provides a lookup for sites on the internet. You can think of it as a phone book, but instead of using the name of an organization to look up its phone number, you use the name of an organization to find an IP address. A DNS service is provided by your ISP (internet service provider).

For example, suppose a request comes from a client computer to access cymbal.com. To direct the client computer to the cymbal.com site, the internet service provider needs the IP address of cymbal.com. The ISP connects to get this information from its DNS service. The DNS service recursive resolver issues a request to look up the IP address of cymbal.com from one of its name servers. The name server responds with the ISP.



Enable VPC Flow Logs per VPC subnet

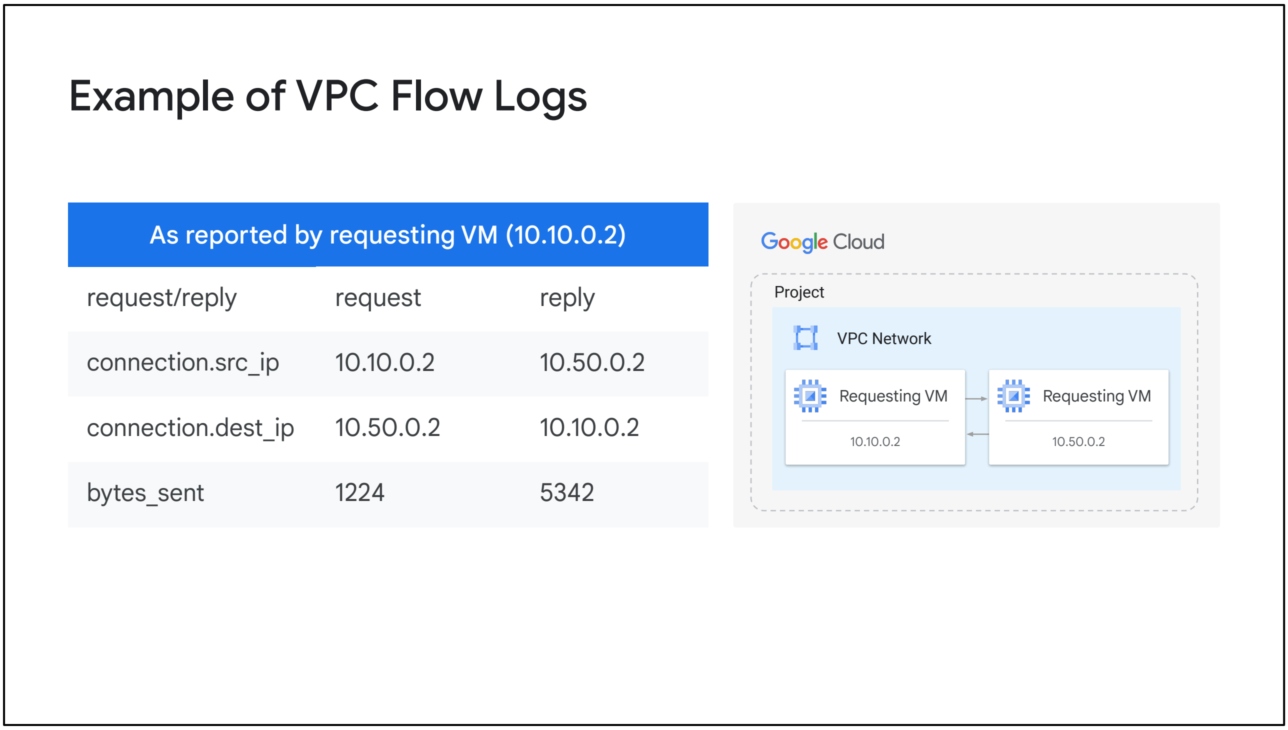
Field	Type	Description
src_ip	string	Source IP address
src_port	int32	Source port
dest_ip	string	Destination IP address
dest_port	int32	Destination port

You can enable or disable VPC Flow Logs per VPC subnet. Once enabled for a subnet, VPC Flow Logs collect data from all VM instances in that subnet.

Each log entry contains a record of different fields. For example, this table illustrates the IP connection information that is recorded. This consists of the source IP address and port, the destination IP address and port, and the protocol number. This set is commonly referred to as 5-tuple.

Other fields include the start and end time of the first and last observed packet, the bytes and packets sent, instance details, VPC details, and geographic details.

For more information on all data recorded by VPC Flow Logs, please refer to https://cloud.google.com/vpc/docs/using-flow-logs#logs_collection.



Example of VPC Flow Logs

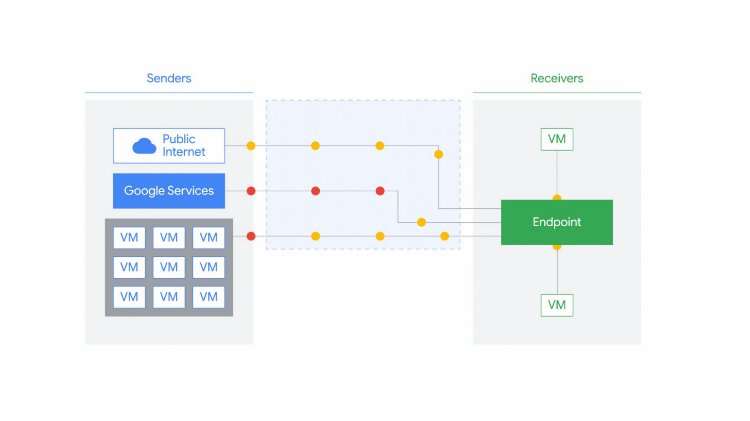
As reported by requesting VM (10.10.0.2)		
request/reply	request	reply
connection.src_ip	10.10.0.2	10.50.0.2
connection.dest_ip	10.50.0.2	10.10.0.2
bytes_sent	1224	5342

Google Cloud
Project
VPC Network
Requesting VM
10.10.0.2
Requesting VM
10.50.0.2

VPC Flow Logs capture traffic from both ends of a VM-to-VM conversation within the same VPC network. To use this feature, ensure both the communicating VMs reside in subnets with VPC Flow Logs enabled.

In this example, VM 10.10.0.2 sends a request with 1,224 bytes to VM 10.50.0.2, which is also in a subnet that has logging enabled. In turn, 10.50.0.2 responds to the request with a reply containing 5,342 bytes. Both the request and reply are recorded from both the requesting and responding VMs.

Packet Mirroring clones the traffic of specified instances in your VPC network



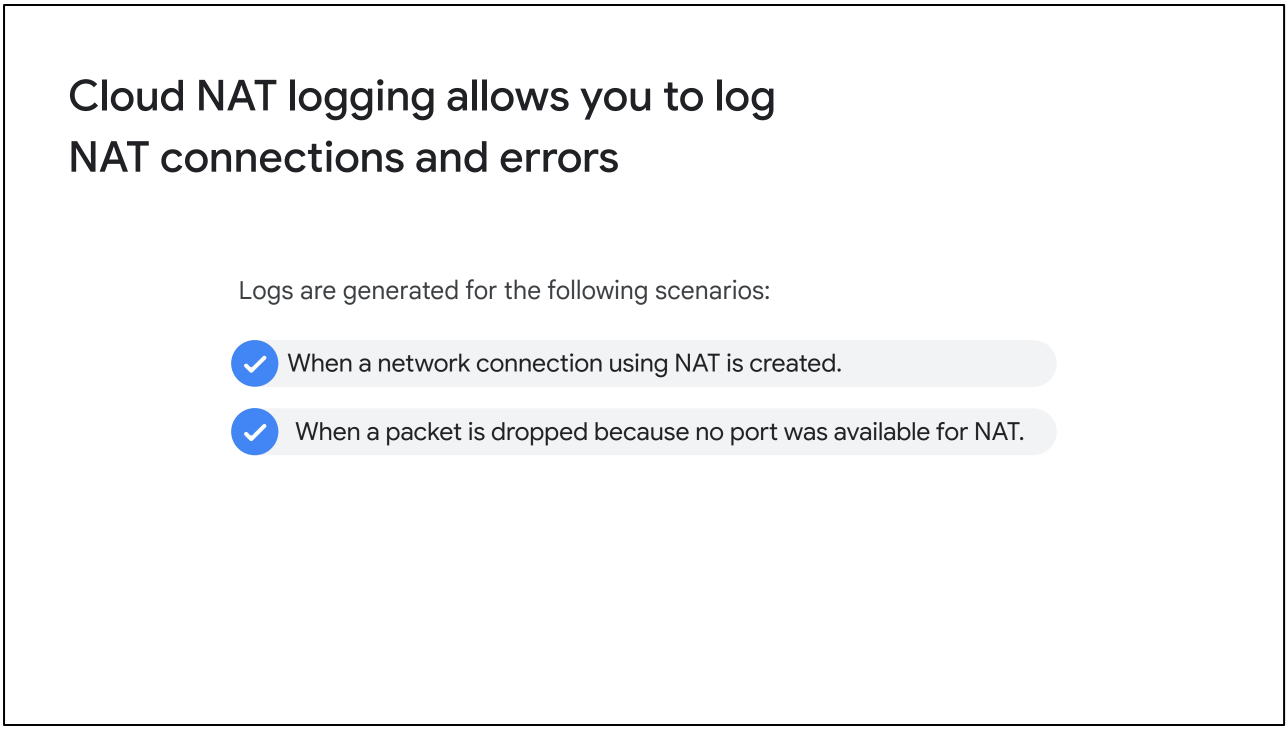
Packet Mirroring clones the traffic of specific instances in your Virtual Private Cloud (VPC) network and forwards it for examination. It also captures all ingress and egress traffic and packet data, such as payloads and headers.

The mirroring happens on the virtual machine (VM) instances, not on the network. Consequently, Packet Mirroring consumes additional bandwidth on the hosts.

Packet Mirroring is useful when you need to monitor and analyze your security status. It exports all traffic, not only the traffic between sampling periods.

For example, you can use security software that analyzes mirrored traffic to detect all threats or anomalies.

Additionally, you can inspect the full traffic flow to detect application performance issues.



Cloud NAT logging allows you to log NAT connections and errors

Logs are generated for the following scenarios:

✓ When a network connection using NAT is created.

✓ When a packet is dropped because no port was available for NAT.

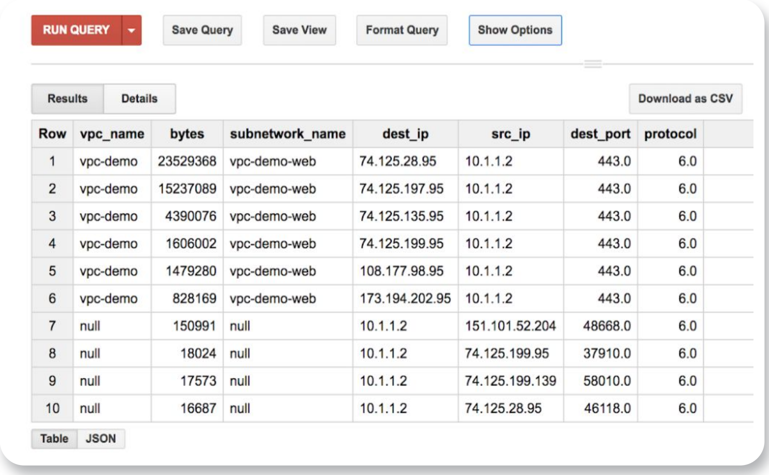
Cloud NAT logging allows you to log NAT connections and errors. When Cloud NAT logging is enabled, one log entry can be generated for each of the following scenarios:

- When a network connection using NAT is created.
- When a packet is dropped because no port was available for NAT.

You can choose to log both kinds of events, or only one.

Created logs are sent to Cloud Logging. Cloud NAT logging handles TCP and UDP traffic only. Cloud NAT logging only logs dropped packets if they are egress (outbound) TCP and UDP packets. It does not log dropped incoming packets, for example, if an inbound response to an outbound request is dropped for any reason, no error is logged.

Analyze logs in BigQuery and visualize in Looker Studio



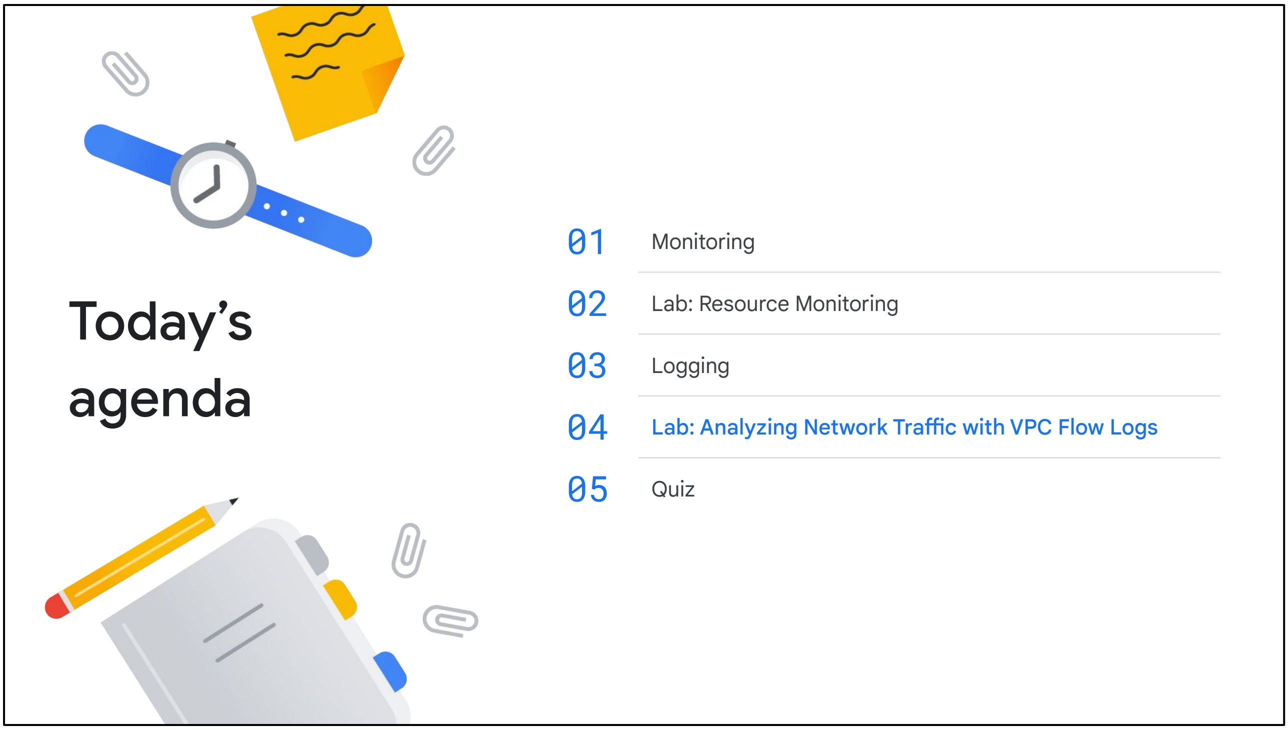
Row	vpc_name	bytes	subnetwork_name	dest_ip	src_ip	dest_port	protocol
1	vpc-demo	23529368	vpc-demo-web	74.125.28.95	10.1.1.2	443.0	6.0
2	vpc-demo	15237089	vpc-demo-web	74.125.197.95	10.1.1.2	443.0	6.0
3	vpc-demo	4390076	vpc-demo-web	74.125.135.95	10.1.1.2	443.0	6.0
4	vpc-demo	1606002	vpc-demo-web	74.125.199.95	10.1.1.2	443.0	6.0
5	vpc-demo	1479280	vpc-demo-web	108.177.98.95	10.1.1.2	443.0	6.0
6	vpc-demo	828169	vpc-demo-web	173.194.202.95	10.1.1.2	443.0	6.0
7	null	150991	null	10.1.1.2	151.101.52.204	48668.0	6.0
8	null	18024	null	10.1.1.2	74.125.199.95	37910.0	6.0
9	null	17573	null	10.1.1.2	74.125.199.139	58010.0	6.0
10	null	16687	null	10.1.1.2	74.125.28.95	46118.0	6.0

Although Tal can explore each log entry within Google Cloud Logging, we recommend exporting logs to BigQuery.

BigQuery runs blazing-fast SQL queries on gigabytes to petabytes of data. This allows Tal to **analyze network traffic** to better understand traffic growth to forecast capacity, analyze network usage to optimize network traffic expenses, or analyze network forensics to examine incidents.

For example, in this screenshot we queried my logs to identify the top IP addresses that have exchanged traffic with the web server. Depending on where these IP addresses are and who they belong to, we could relocate part of my infrastructure to save on networking costs or deny some of these IP addresses if we don’t want them to access my web server.

If Tal wants to visualize logs, we recommend connecting BigQuery tables to Looker Studio. Looker Studio transforms raw data into the metrics and dimensions that Tal can use to create easy-to-understand reports and dashboards.



Today's agenda

01 Monitoring

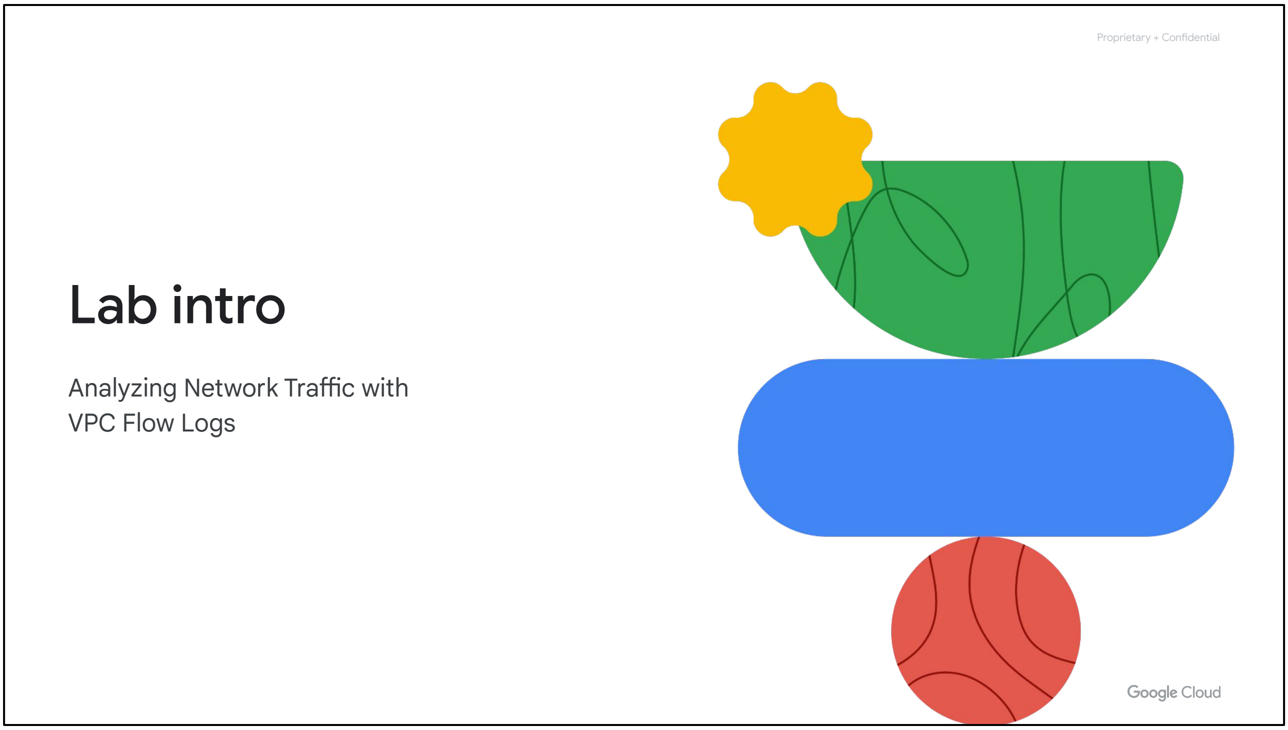
02 Lab: Resource Monitoring

03 Logging

04 **Lab: Analyzing Network Traffic with VPC Flow Logs**

05 Quiz

Let's apply what we just covered to analyze network traffic with VPC Flow Logs.

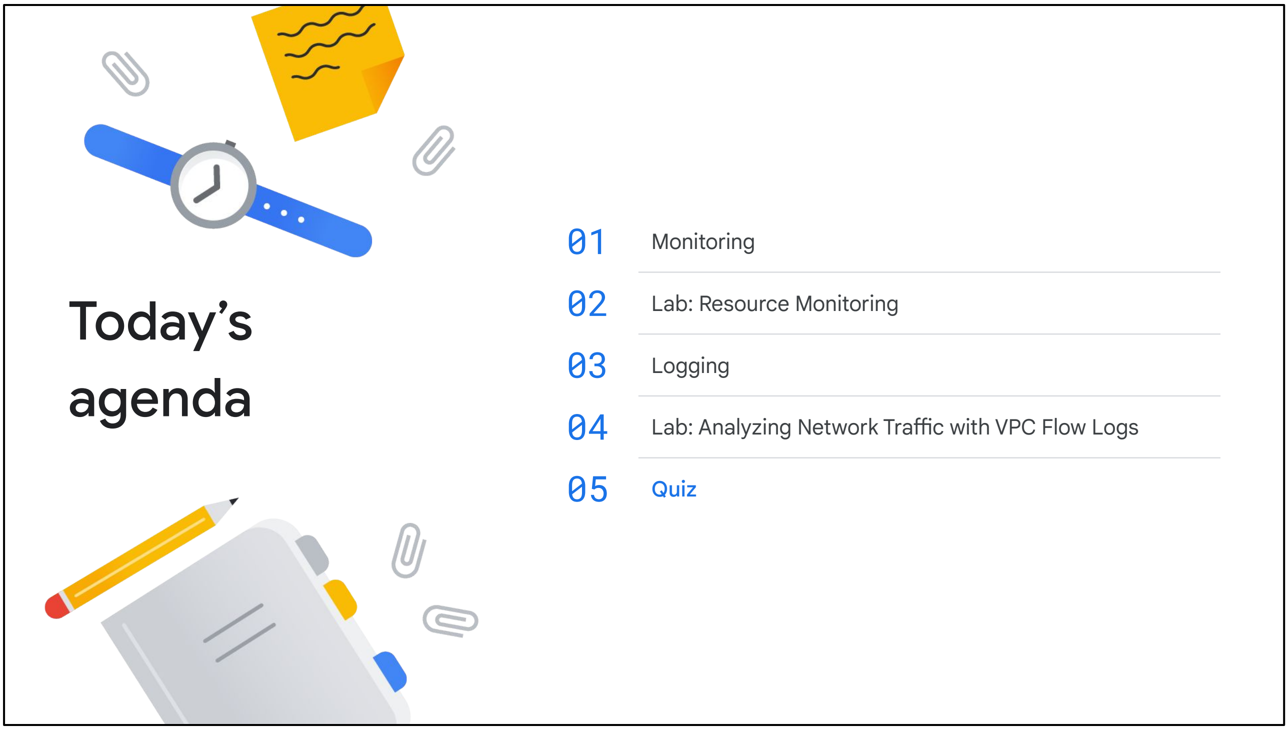


Lab intro

Analyzing Network Traffic with
VPC Flow Logs

In this lab, you learn how to:

- Configure a custom network with VPC Flow Logs.
- Create an Apache web server.
- Verify that network traffic is logged.
- Export the network traffic to BigQuery to further analyze the logs.
- Setup VPC Flow Logs aggregation.



Today's agenda

01 Monitoring

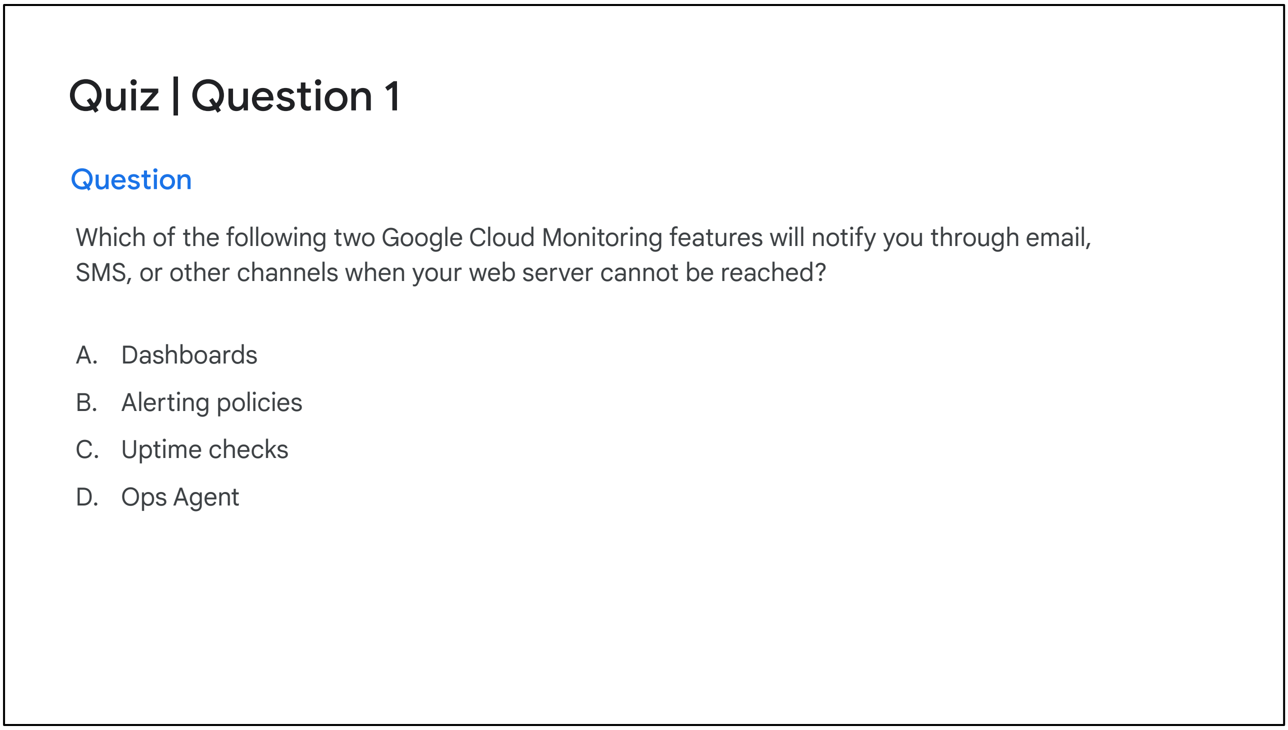
02 Lab: Resource Monitoring

03 Logging

04 Lab: Analyzing Network Traffic with VPC Flow Logs

05 Quiz

Let's test your knowledge.



Quiz | Question 1

Question

Which of the following two Google Cloud Monitoring features will notify you through email, SMS, or other channels when your web server cannot be reached?

A. Dashboards

B. Alerting policies

C. Uptime checks

D. Ops Agent

Quiz | Question 2

Question

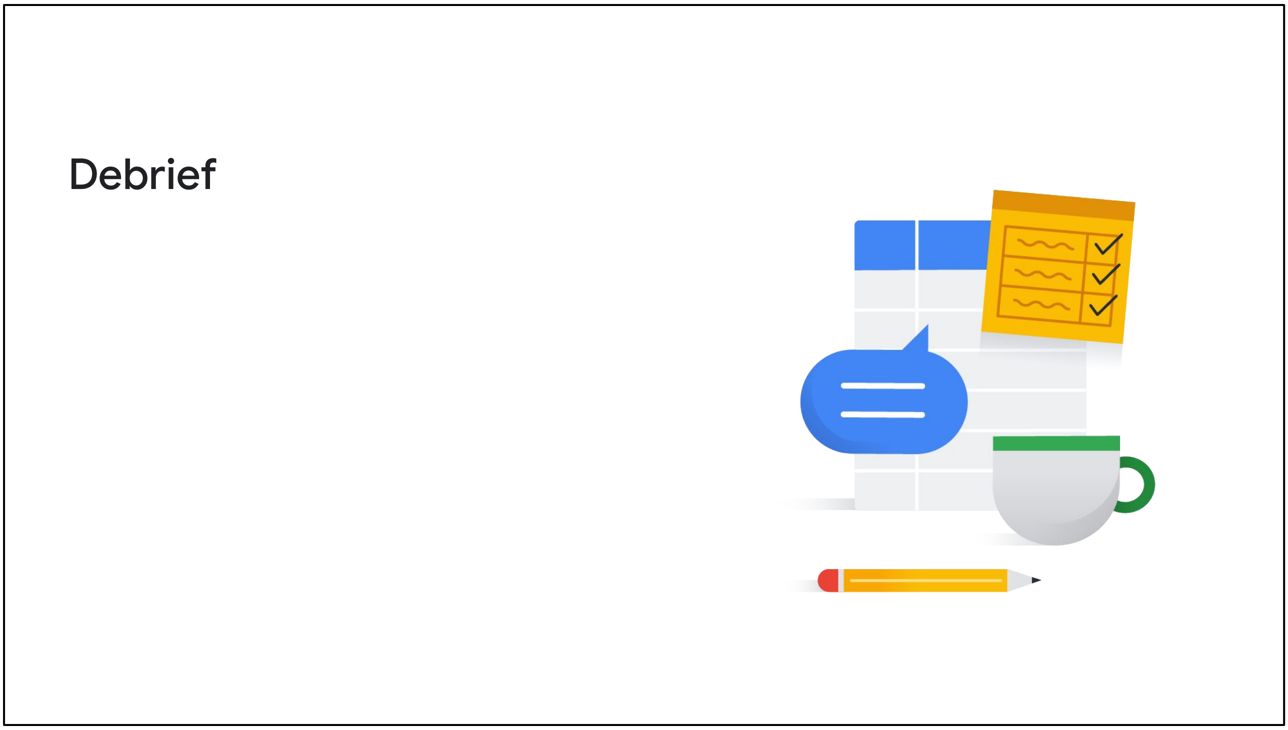
In regards to VPC Flow Logs, which of the following statements is correct?

A. There is a delay and performance penalty in routing logged IP packets.

B. Log updates are provided every 5 minutes.

C. Logs cannot be analyzed in BigQuery or visualized in Looker Studio.

D. Logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization.



Debrief

In this module, we covered Google Cloud network monitoring and logging features that can help you troubleshoot your Google Cloud networking services.

Monitoring is important to Google because it is at the base of site reliability engineering, or SRE. SRE is a discipline that incorporates aspects of software engineering and applies that to operations whose goals are to create ultra-scalable and highly reliable software systems.

This discipline has enabled Google to build, deploy, monitor, and maintain some of the largest software systems in the world.

Thank you.

THANK YOU