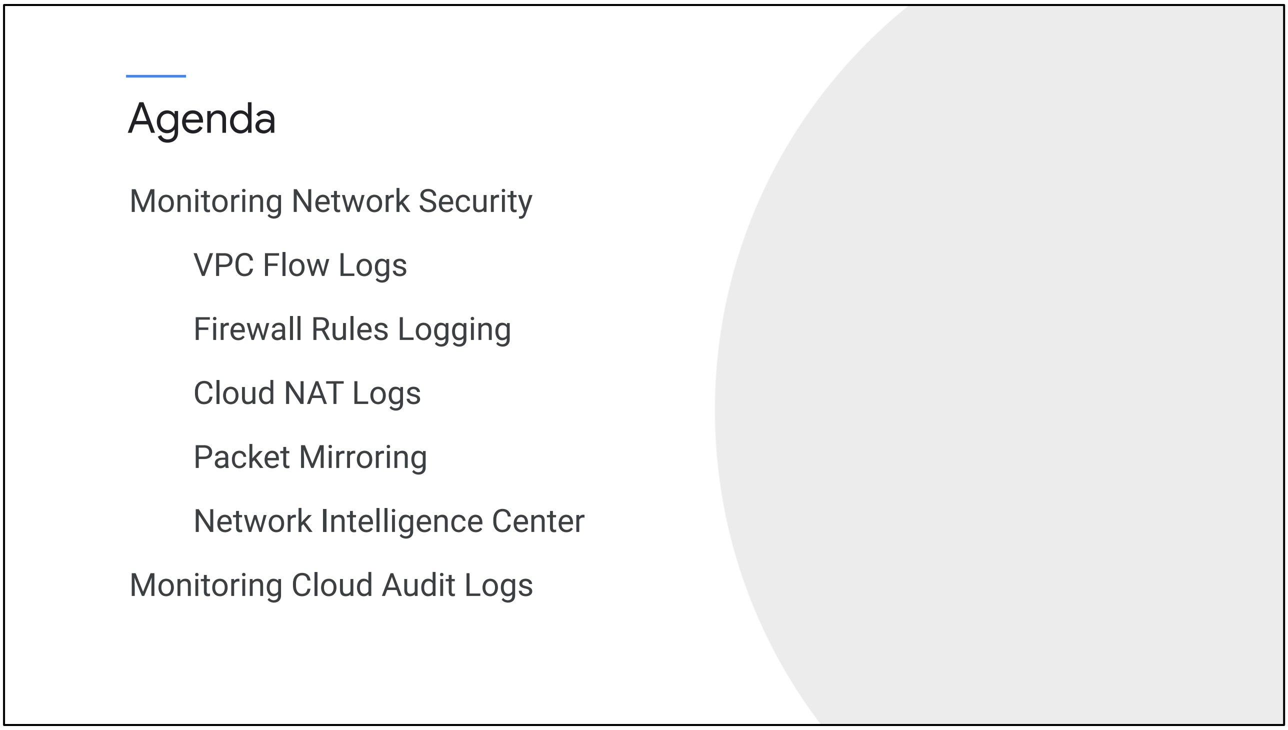
Monitoring Network Security and Audit Logs

In this module, we will examine two key topics: Monitoring as it relates to the VPC network, and Google's Cloud Audit logs.



Agenda

Monitoring Network Security

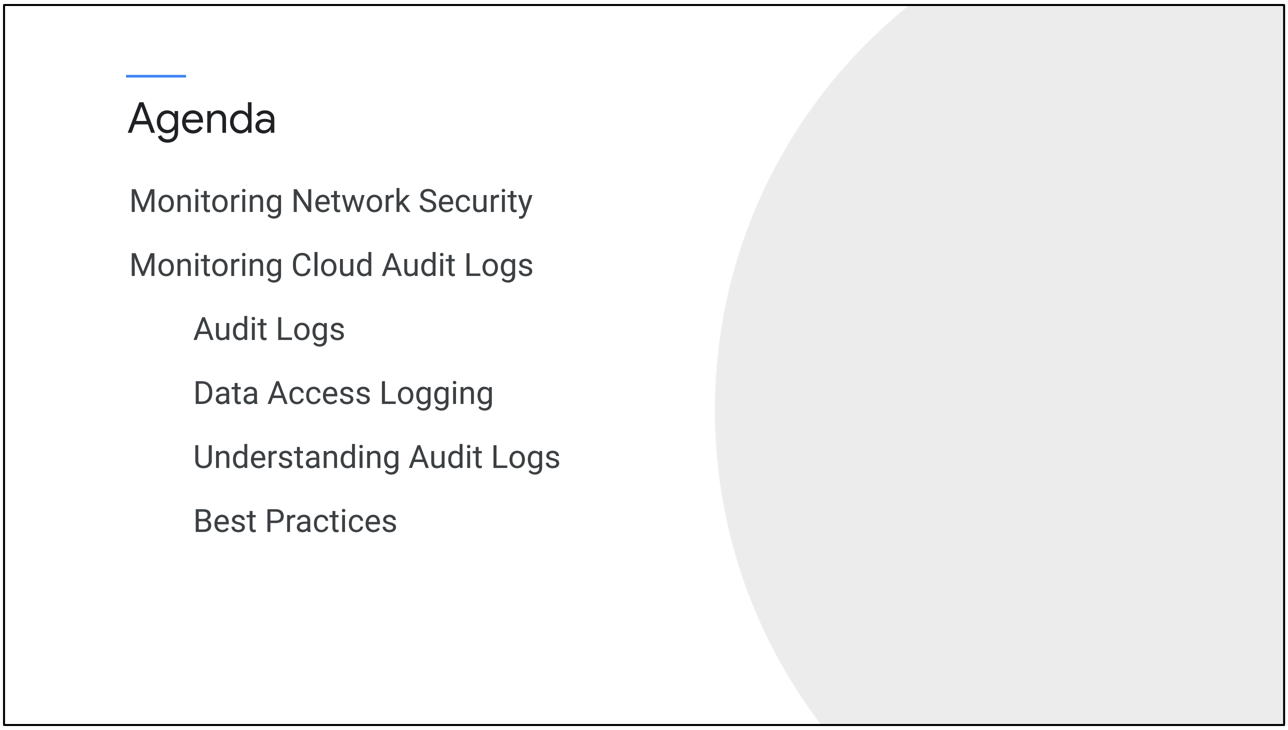
- VPC Flow Logs
- Firewall Rules Logging
- Cloud NAT Logs
- Packet Mirroring
- Network Intelligence Center

Monitoring Cloud Audit Logs

Specifically, you will learn to:

- Collect and analyze VPC Flow, Firewall Rule, and Cloud NAT logs so you can see what's happening to the traffic across your network
- Enable Packet Mirroring so you can replicate packets at the virtual machine network interface, and forward it for further analysis.
- Explain the capabilities of the Network Intelligence Center.

And …



Agenda

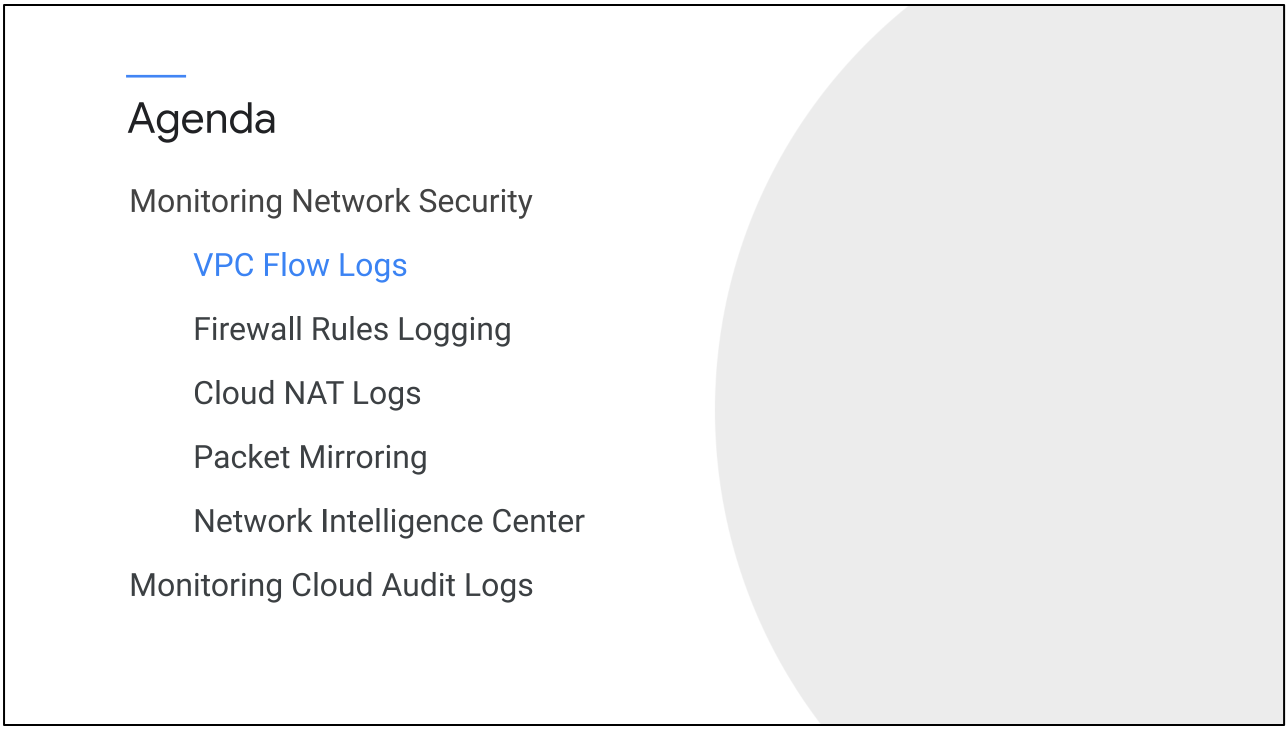
Monitoring Network Security

Monitoring Cloud Audit Logs

- Audit Logs
- Data Access Logging
- Understanding Audit Logs
- Best Practices

Use the Cloud Audit logs: Admin Activity, Data Access, and System Event, to answer the question, “Who, did what, and when?”

We will also cover best practices for Audit Logging.



Agenda

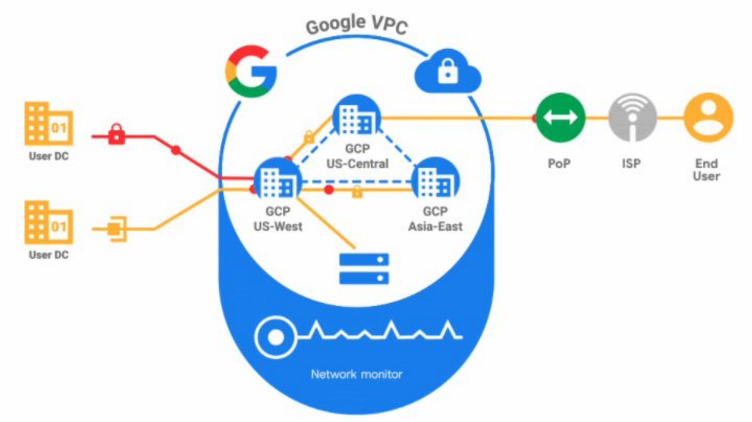
Monitoring Network Security

- VPC Flow Logs
- Firewall Rules Logging
- Cloud NAT Logs
- Packet Mirroring
- Network Intelligence Center

Monitoring Cloud Audit Logs

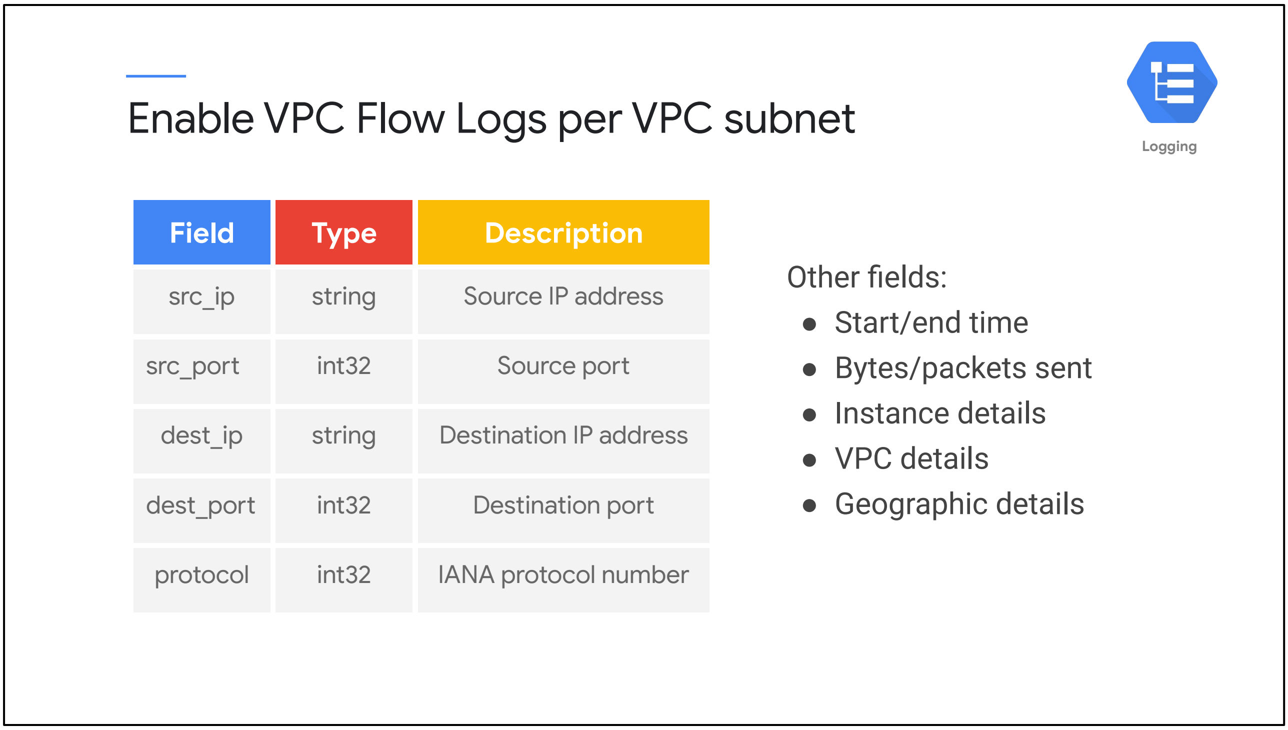
Let’s start with monitoring the network...

VPC Flow Logs record a sample of network flows



VPC Flow Logs record a sample (about 1 out of 10 packets) of network flows sent from and received by VM instances, including Kubernetes Engines nodes. These logs can be used for network monitoring, traffic analysis, forensics, real-time security analysis, and expense optimization.

VPC Flow Logs is part of Andromeda, the software that powers VPC networks. VPC Flow Logs introduces no delay or performance penalty when enabled.



Enable VPC Flow Logs per VPC subnet

Logging

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
protocol	int32	IANA protocol number

Other fields:

- Start/end time
- Bytes/packets sent
- Instance details
- VPC details
- Geographic details

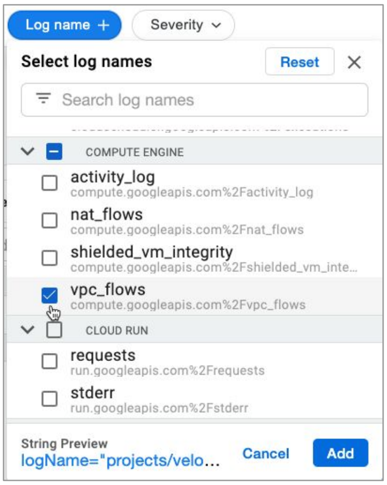
You can enable or disable VPC Flow Logs per VPC subnet. Once enabled for a subnet, VPC Flow Logs collect data from all VM instances in that subnet.

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 including network tags, VPC details, and geographic details. For more information on all data recorded by VPC Flow Logs, please see the documentation.

Use Logging to review your VPC Flow Logs

Logging



COMPUTE ENGINE

- □ activity_log compute.googleapis.com%2Factivity_log
- □ nat_flows compute.googleapis.com%2Fnat_flows
- □ shielded_vm_integrity compute.googleapis.com%2Fshielded_vm_inte…
- ☑ vpc_flows compute.googleapis.com%2Fvpc_flows

□ CLOUD RUN

- □ requests run.googleapis.com%2Frequests
- □ stderr run.googleapis.com%2Fstderr

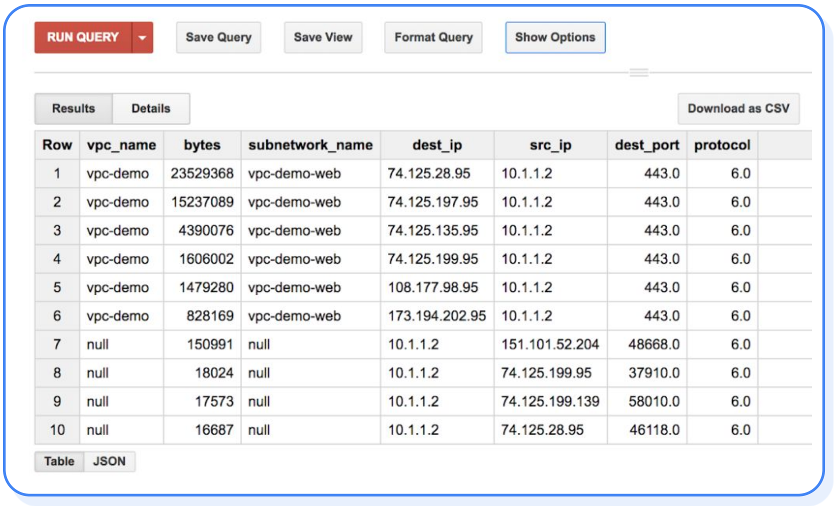
String Preview
logName="projects/velo…

The Google Cloud Logs Viewer can be used to access the VPC Flow Logs. The entries will be vpc_flows under the Compute Engine section. Searching the log names for vpc_flows works well.

Analyze Logs in BigQuery and visualize in Data Studio

BigQuery

Data Studio

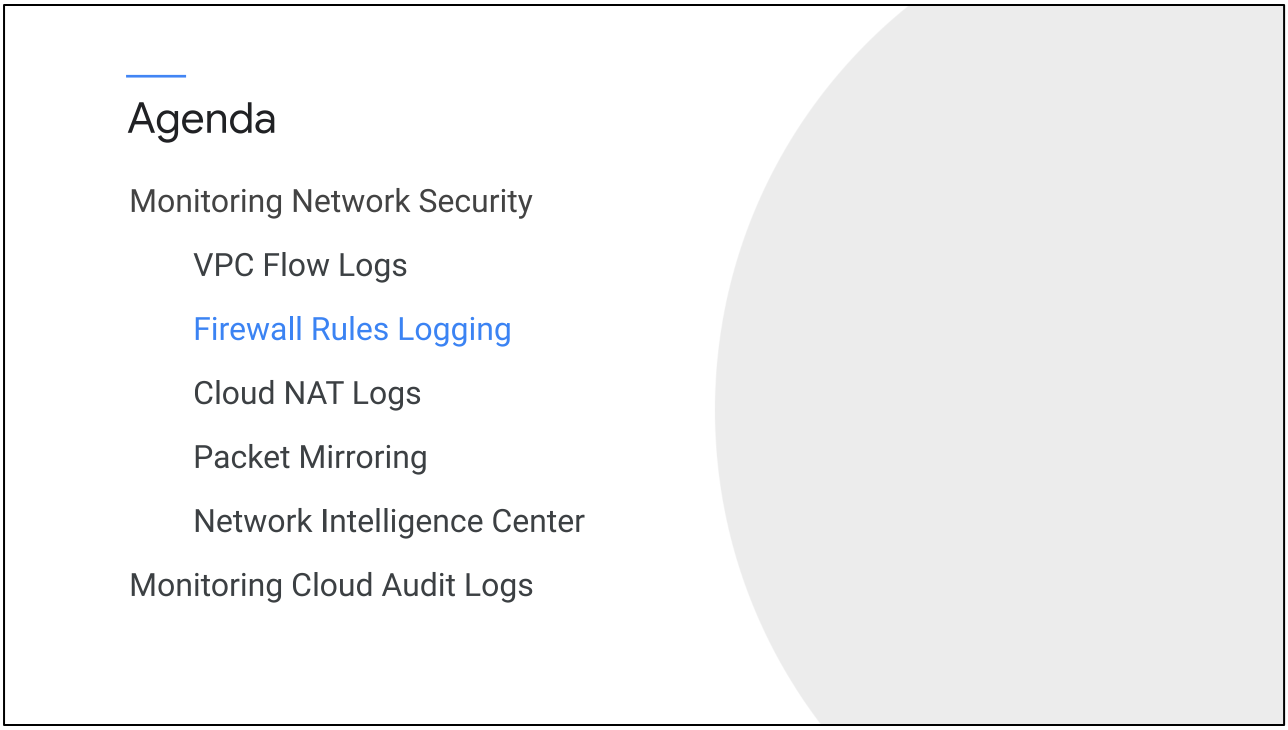


Row	vpc_name	bytes	subnetwork_name	dest_ip	src_ip	dest_port	protocol
1	vpc-demo	23529368	vpc-demo-web	74.125.28.95	10.1.1.2	443.0	6.0
2	vpc-demo	15237089	vpc-demo-web	74.125.197.95	10.1.1.2	443.0	6.0
3	vpc-demo	4390076	vpc-demo-web	74.125.135.95	10.1.1.2	443.0	6.0
4	vpc-demo	1606002	vpc-demo-web	74.125.199.95	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

Exporting VPC Flow logs to BigQuery allows you to analyze your network traffic with SQL, to understand traffic growth patterns and network usage better.

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

For more sophisticated visualizations, connect your BigQuery tables to Data Studio and transform the raw data into the metrics and dimensions needed to create end-user friendly reports and dashboards.



Agenda

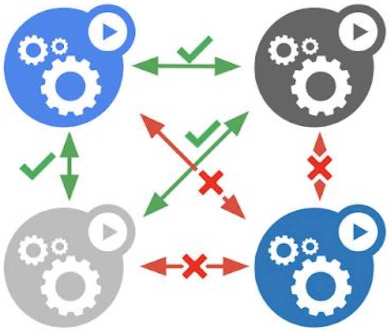
Monitoring Network Security

- VPC Flow Logs
- Firewall Rules Logging
- Cloud NAT Logs
- Packet Mirroring
- Network Intelligence Center

Monitoring Cloud Audit Logs

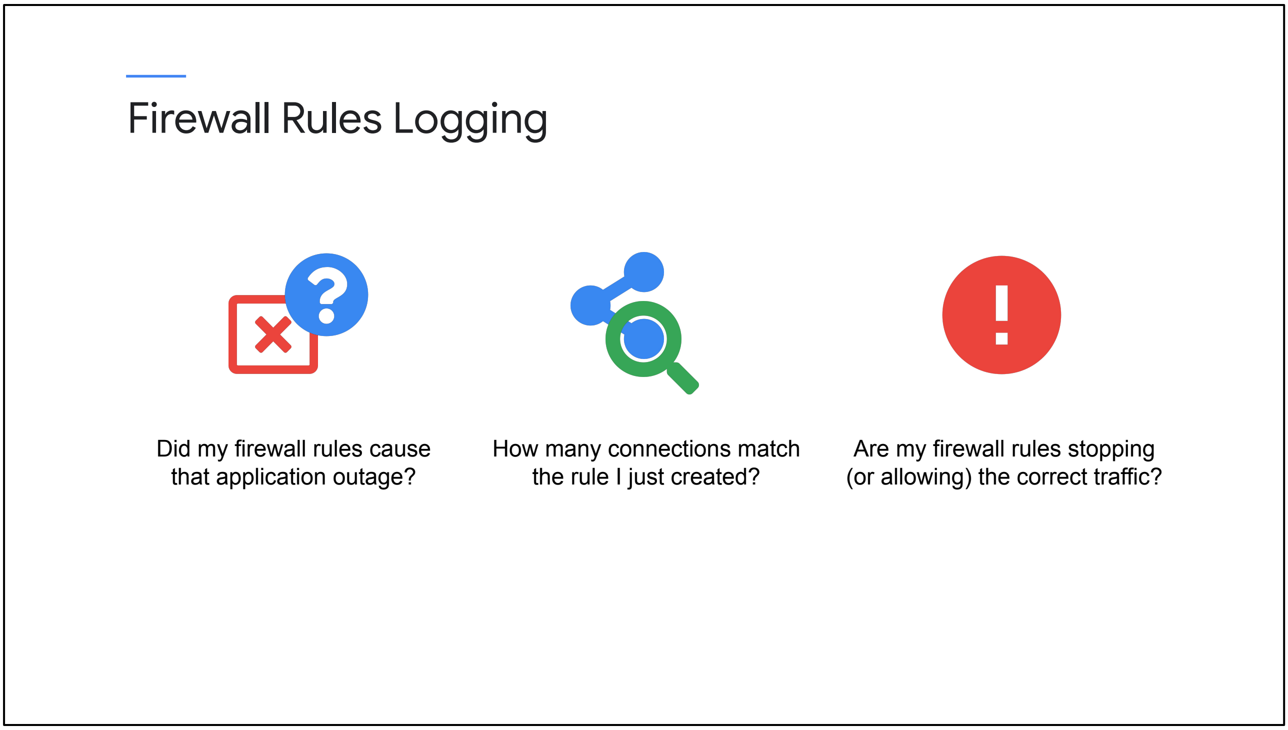
Another essential part of knowing what's happening at the VPC network level is knowing what the firewall rules are doing.

VPC Firewalls



VPC firewall rules let you allow or deny connections to or from your virtual machine (VM) instances based on a configuration that you specify.

Enabled VPC firewall rules are always enforced, protecting your instances regardless of their configuration and operating system, even if they have not started up.



Firewall Rules Logging

Did my firewall rules cause that application outage?

How many connections match the rule I just created?

Are my firewall rules stopping (or allowing) the correct traffic?

Firewall Rules Logging allows you to audit, verify, and analyze the effects of your firewall rules.

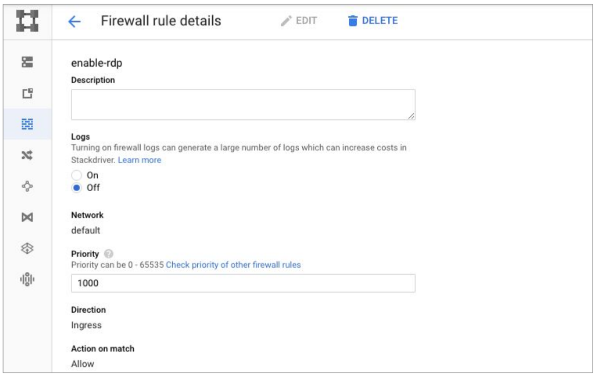
It can help answer questions like:

- Did my firewall rules cause that application outage?
- How many connections match the rule I just created?
- Are my firewall rules stopping (or allowing) the correct traffic?

See the Firewall Rule Logging documentation for details.

Enabling Firewall Rule Logging in the console

- Firewall Rule Logging is **disabled** by default
- You enable it on a per-rule basis



enable-rdp

Description

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more

○ On
● Off

Network

default

Priority

Priority can be 0 - 65535 Check priority of other firewall rules

1000

Direction

Ingress

Action on match

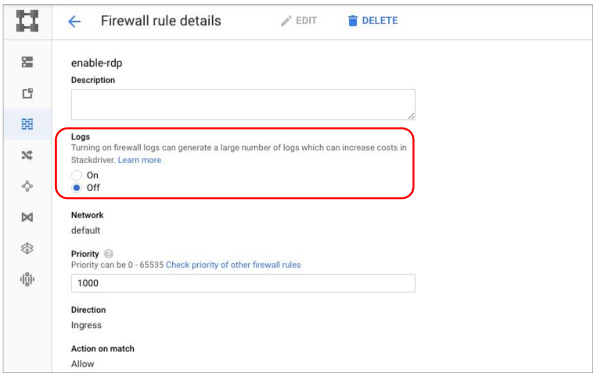
Allow

By default, firewall rule logging is disabled.

You can enable it on a per-rule basis.

Enabling Firewall Rule Logging in the console

- Firewall Rule Logging is **disabled** by default
- You enable it on a per-rule basis



enable-rdp

Description

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more

○ On
● Off

Network
default

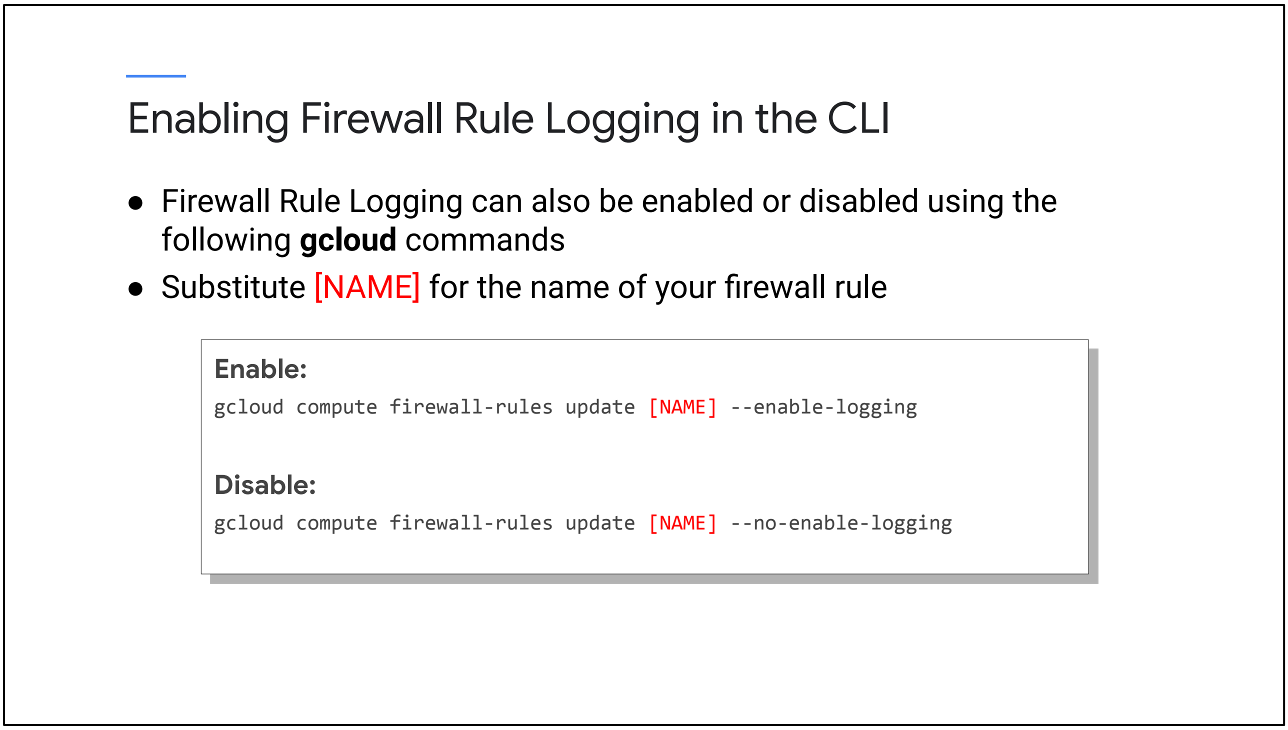
Priority
Priority can be 0 - 65535 Check priority of other firewall rules
1000

Direction
Ingress

Action on match
Allow

In the slide screenshot, the user is editing the firewall rule named *enable-rdp*. Selecting the radio button will enable firewall rules.

Caution. Firewall rule logging can generate a lot of data which may have a cost impact.



Enabling Firewall Rule Logging in the CLI

- Firewall Rule Logging can also be enabled or disabled using the following **gcloud** commands
- Substitute [NAME] for the name of your firewall rule

Enable:

```
gcloud compute firewall-rules update [NAME] --enable-logging
```

Disable:

```
gcloud compute firewall-rules update [NAME] --no-enable-logging
```

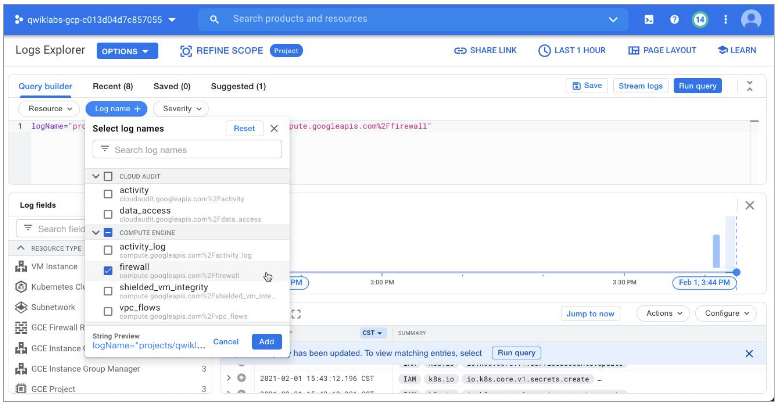
Firewall rule logging can also be enabled on existing firewall rules using the CLI. See these two examples on this slide. In both, [NAME] would be the name of your firewall rule.

Viewing the Firewall Rule Logs

- In Logging, you can view the logs in real time
- Or, export the firewall logs to a BigQuery sink

Logging

BigQuery



```
logName="prc                  pute.googleapis.com%2Ffirewall"
```

☐ CLOUD AUDIT
☐ activity
☐ data_access
▣ COMPUTE ENGINE
☐ activity_log
☑ firewall
☐ shielded_vm_integrity
☐ vpc_flows

String Preview logName="projects/qwikl...

has been updated. To view matching entries, select Run query

```
2021-02-01 15:43:12.196 CST   IAM  k8s.io  io.k8s.core.v1.secrets.create …
```

Like all Google Cloud Logs, use Logs Explorer to view logs in real-time, or to configure exports.

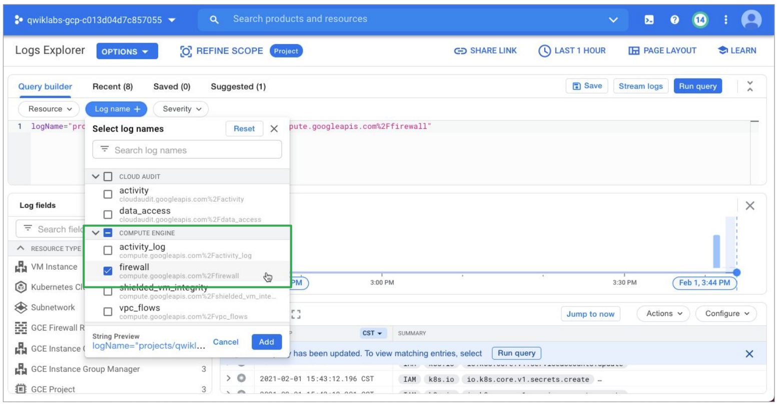
BigQuery is frequently used to simplify firewall rule log analysis.

Viewing the Firewall Rule Logs

- In Logging, you can view the logs in real time
- Or, export the firewall logs to a BigQuery sink

Logging

BigQuery



```
logName="pro   pute.googleapis.com%2Ffirewall"
```

CLOUD AUDIT

☐ activity
cloudaudit.googleapis.com%2Factivity

☐ data_access
cloudaudit.googleapis.com%2Fdata_access

COMPUTE ENGINE

☐ activity_log
compute.googleapis.com%2Factivity_log

☑ firewall
compute.googleapis.com%2Ffirewall

☐ shielded_vm_integrity
compute.googleapis.com%2Fshielded_vm_inte...

☐ vpc_flows
compute.googleapis.com%2Fvpc_flows

String Preview
logName="projects/qwikl...

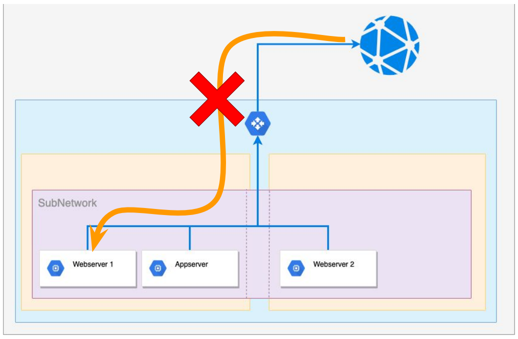
y has been updated. To view matching entries, select Run query

```
2021-02-01 15:43:12.196 CST   IAM   k8s.io   io.k8s.core.v1.secrets.create …
```

To filter for firewall logs, select **firewall** under the Compute Engine resource.

Firewall Rules provide microsegmentation

Segmentation/Gateway-centric

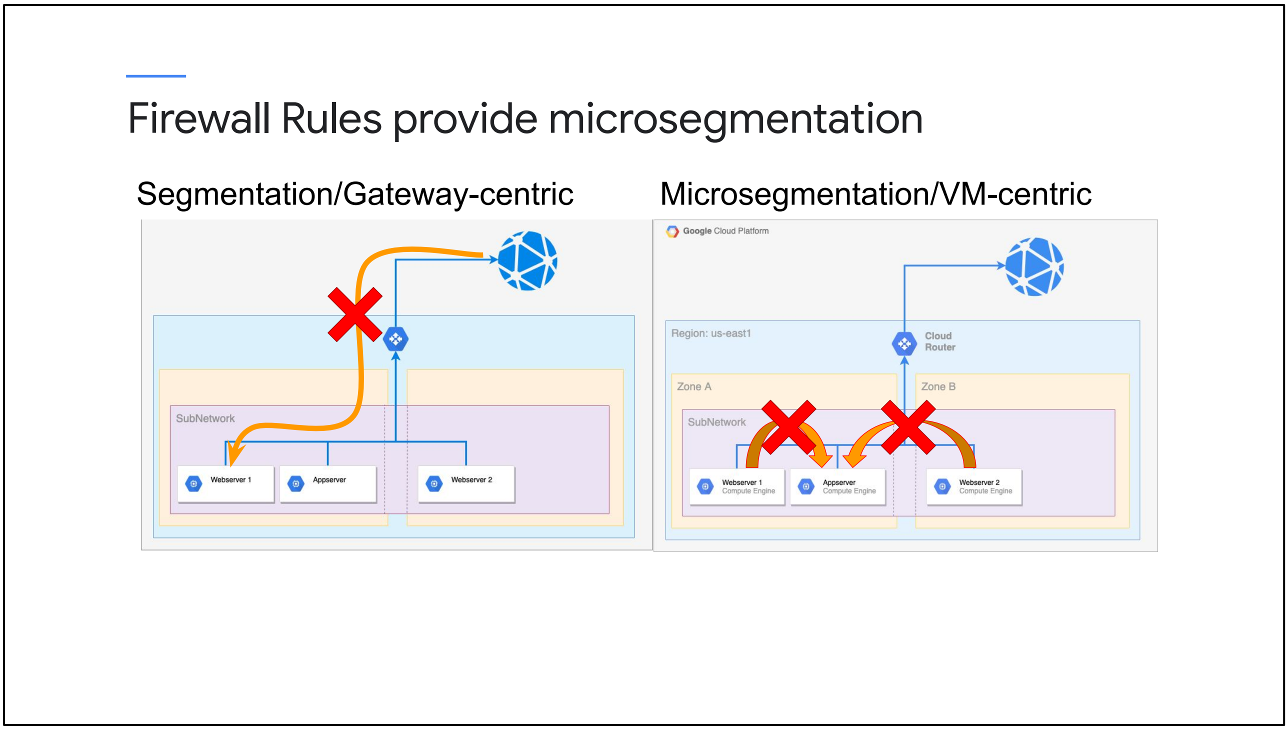


A lot of users are familiar with classic segmentation or gateway centric firewalls.

In this example, you can see a private network, possibly at your office or home.

At the network boundary, where the private network meets the outside internet, sits a firewall.

A segmentation firewall is designed to segment and secure a protected network from an outside insecure network.



Firewall Rules provide microsegmentation

Segmentation/Gateway-centric

Microsegmentation/VM-centric

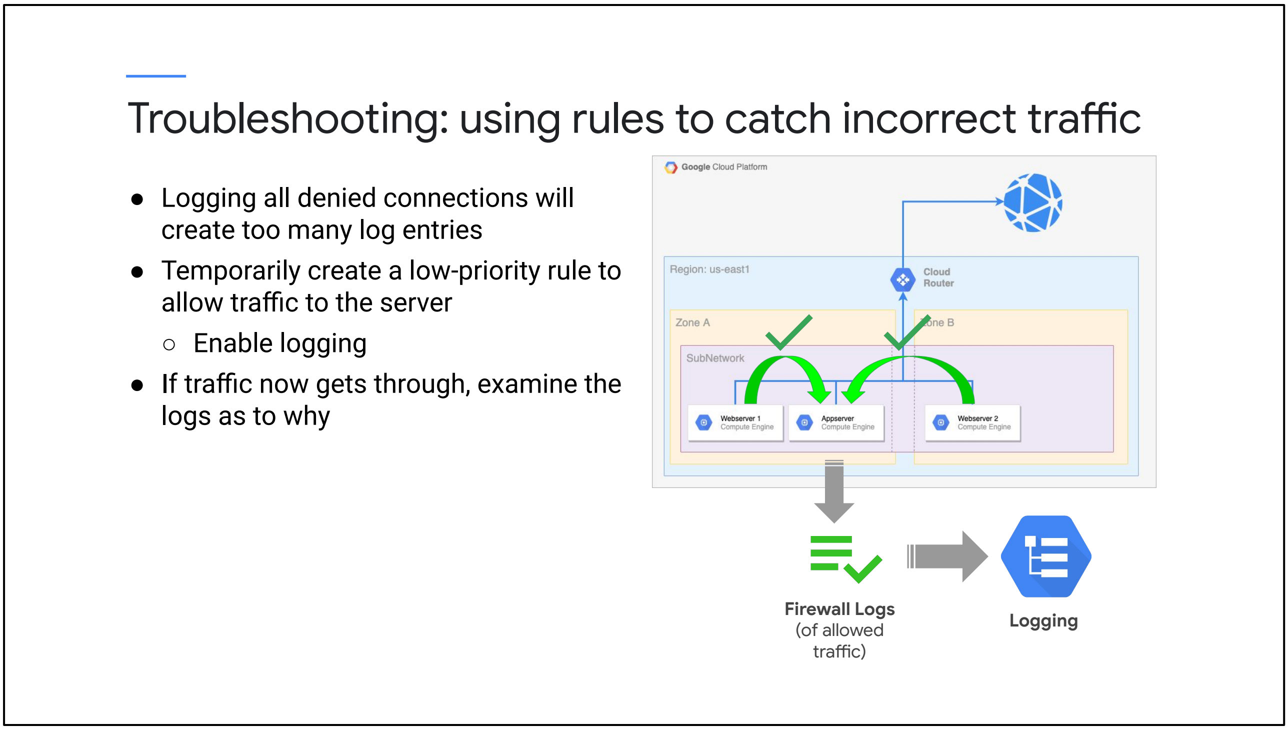
Google Cloud VPC Firewalls are micro-segmentation firewalls.

These function more like a bunch of micro firewalls, each sitting on the NIC of every VM connected to the VPC.

The micro firewalls can then grant or deny any configured incoming or outgoing traffic.

Now, imagine we have an issue. We have two different web servers, and after some configuration changes by a particular DevOps team, the web servers can no longer access the application server they both share.

How can we tell if this is a firewall related issue? Let's see.



Troubleshooting: using rules to catch incorrect traffic

- Logging all denied connections will create too many log entries
- Temporarily create a low-priority rule to allow traffic to the server
    - ○ Enable logging
- If traffic now gets through, examine the logs as to why

If the connectivity issue is related to a firewall, then there are two major possibilities.

1. There's a firewall rule that's actively blocking the incoming connections from the web servers, or
2. Since network traffic is blocked by default in most networks, there could be a firewall rule that isn't allowing the traffic from the web servers as it should.

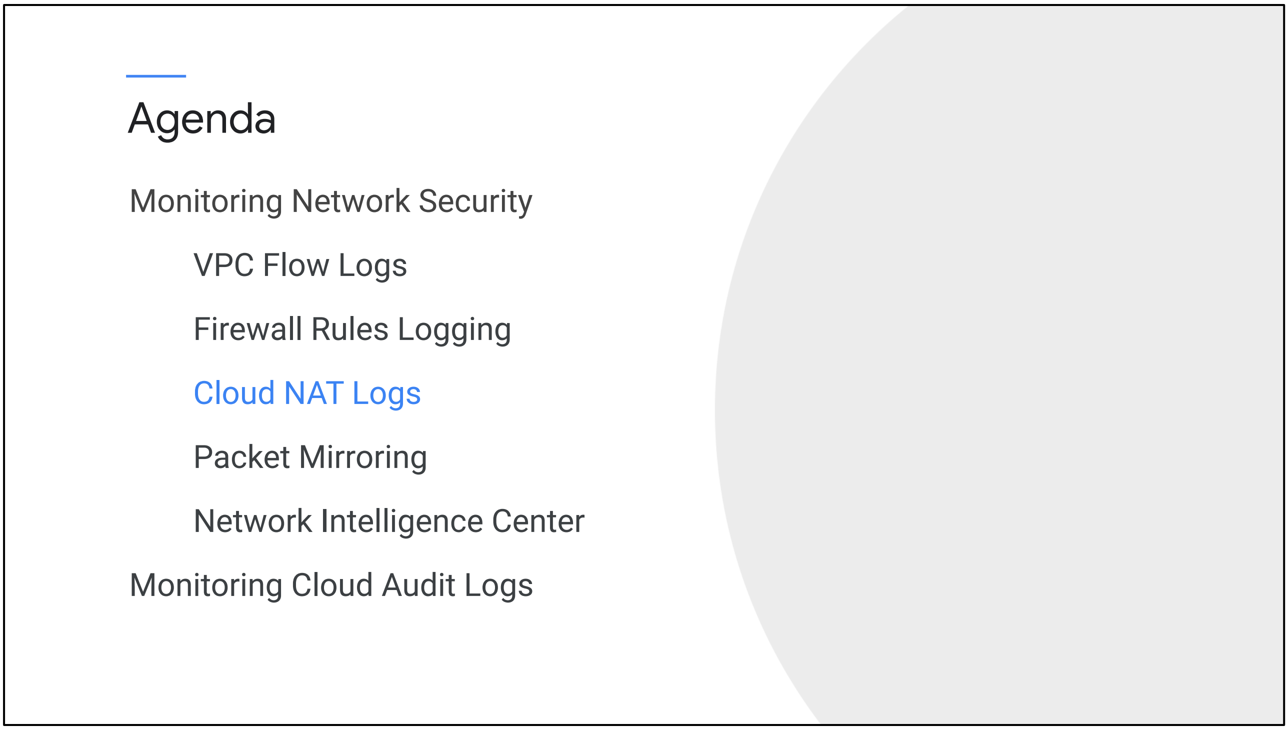
Two sides of the same coin.

Logging all denied connections could generate a lot of data that would take time and effort to go through. So, instead of starting with option one, let's start with option two.

Create a temporary low-priority rule specifically designed to allow the web server traffic through to the app server. Enable logging on it so you can examine the entries.

Suddenly the traffic is getting through, so you know it's firewall related. Now examine the log entries. Also, find the existing rule that's supposed to be allowing the traffic and see what you can find out.

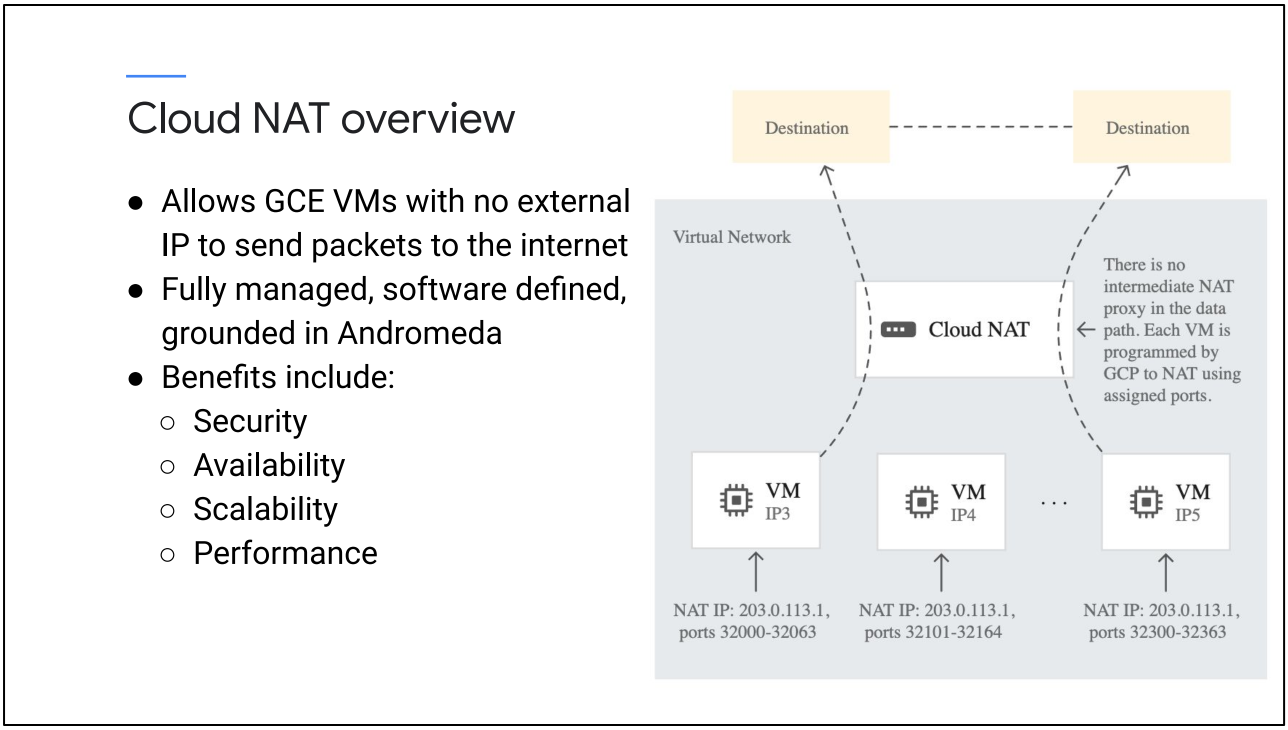
Hey, look at that! The rule that's supposed to be allowing the traffic is based on a network tag named webserver, and the web server machines are actually using the network tag web-server. There it is, that's your problem.



Agenda

- Monitoring Network Security
  - VPC Flow Logs
  - Firewall Rules Logging
  - Cloud NAT Logs
  - Packet Mirroring
  - Network Intelligence Center
- Monitoring Cloud Audit Logs

Another piece of the network telemetry features in Google Cloud is Cloud NAT Logs



Cloud NAT overview

- Allows GCE VMs with no external IP to send packets to the internet
- Fully managed, software defined, grounded in Andromeda
- Benefits include:
  - Security
  - Availability
  - Scalability
  - Performance

Destination
Destination
Virtual Network
Cloud NAT
VM
IP3
VM
IP4
. . .
VM
IP5
NAT IP: 203.0.113.1, ports 32000-32063
NAT IP: 203.0.113.1, ports 32101-32164
NAT IP: 203.0.113.1, ports 32300-32363

There is no intermediate NAT proxy in the data path. Each VM is programmed by GCP to NAT using assigned ports.

Cloud NAT (network address translation) allows Google Cloud virtual machine (VM) instances without external IP addresses and private Google Kubernetes Engine (GKE) clusters to send outbound packets to the internet and receive any corresponding established inbound response packets.

Cloud NAT is a distributed, software-defined, fully managed service, grounded in the Andromeda software that powers your VPC network. It provides source network address translation (SNAT) for VMs without external IP addresses, as well as destination network address translation (DNAT) for established inbound response packets.

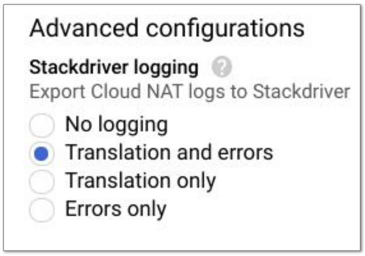
Cloud NAT benefits include:

- **Security**: You can reduce the need for individual VMs to have external IP addresses, lessening the surface area for attack. You can also confidently share a set of common external source IP addresses with a destination party.
- **Availability**: Cloud NAT is a distributed, software-defined, managed Google Cloud service. It doesn't depend on any VMs in your project or a single physical gateway device.
- **Scalability**: Cloud NAT can be configured to automatically scale the number of NAT IP addresses it uses, and it supports VMs that belong to managed instance groups, including those with autoscaling enabled.
- **Performance**: Cloud NAT does not reduce the network bandwidth per VM. Cloud NAT works directly with Google's Andromeda software-defined

- networking.

Cloud NAT logging

- Allows you to log NAT **connections** and/or **errors**
  - TCP and UDP traffic only
  - 50-100 entries per second, per vCPU
- Enable logging by editing the Cloud NAT settings
- View by filtering Logs Explorer:
  - Resource: Cloud NAT Gateway
  - (optional) Restrict to region or NAT Gateway



Advanced configurations

Stackdriver logging

Export Cloud NAT logs to Stackdriver

○ No logging
● Translation and errors
○ Translation only
○ Errors only

Cloud NAT logging allows you to log NAT TCP and UDP connections and errors. When Cloud NAT logging is enabled, a log entry can be generated when a network connection using NAT is created, and/or when an egress packet is dropped because no port was available for NAT.

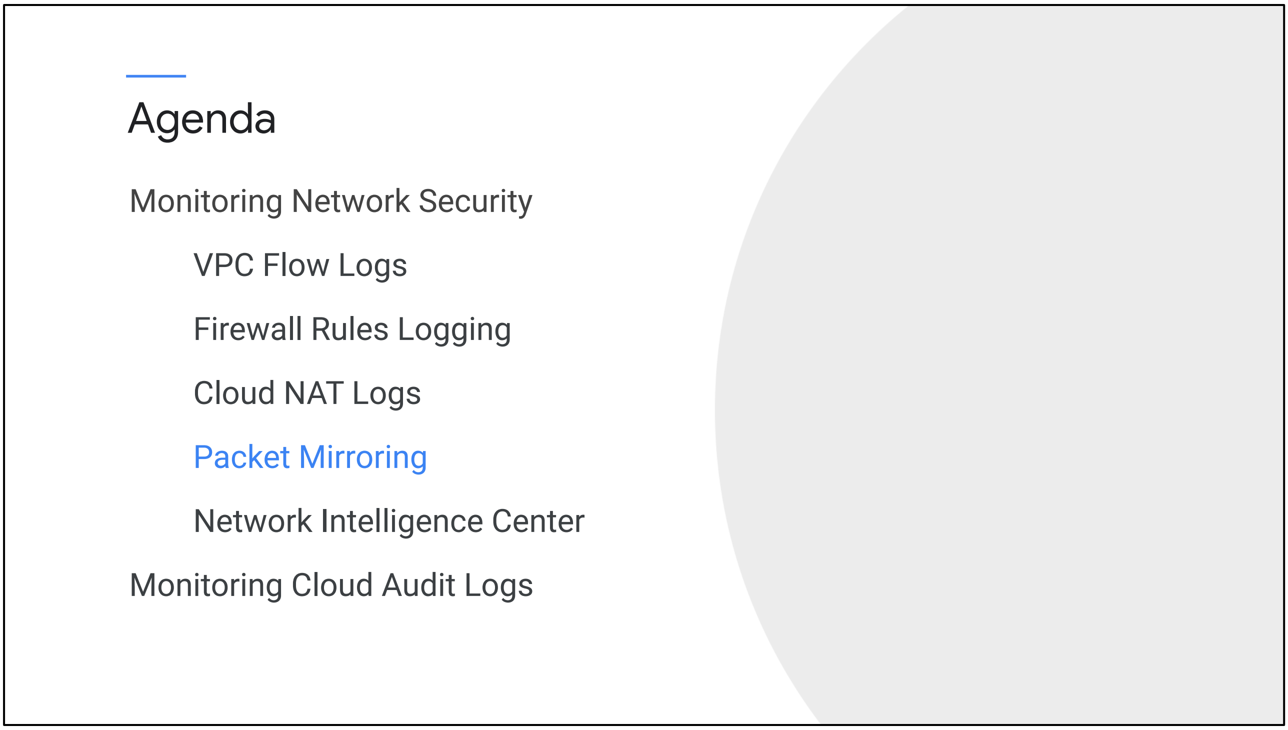
You can opt to log both kinds of events, or just one or the other. Logs contain TCP and UDP traffic only, and the log rate threshold will max out at 50-100 log events per vCPU before log filtering.

Cloud NAT logging may be enabled when a new Cloud NAT gateway is first created, or by editing an existing gateway's settings.

To view the collected logs in Logs Explorer, filter to the Cloud NAT Gateway resource and optionally, restrict to a particular region or Gateway.

The full query will look something like:

```
resource.type="nat_gateway"
logName="projects/{#project_id}/logs/compute.googleapis.com%2Fnat_flows"
```



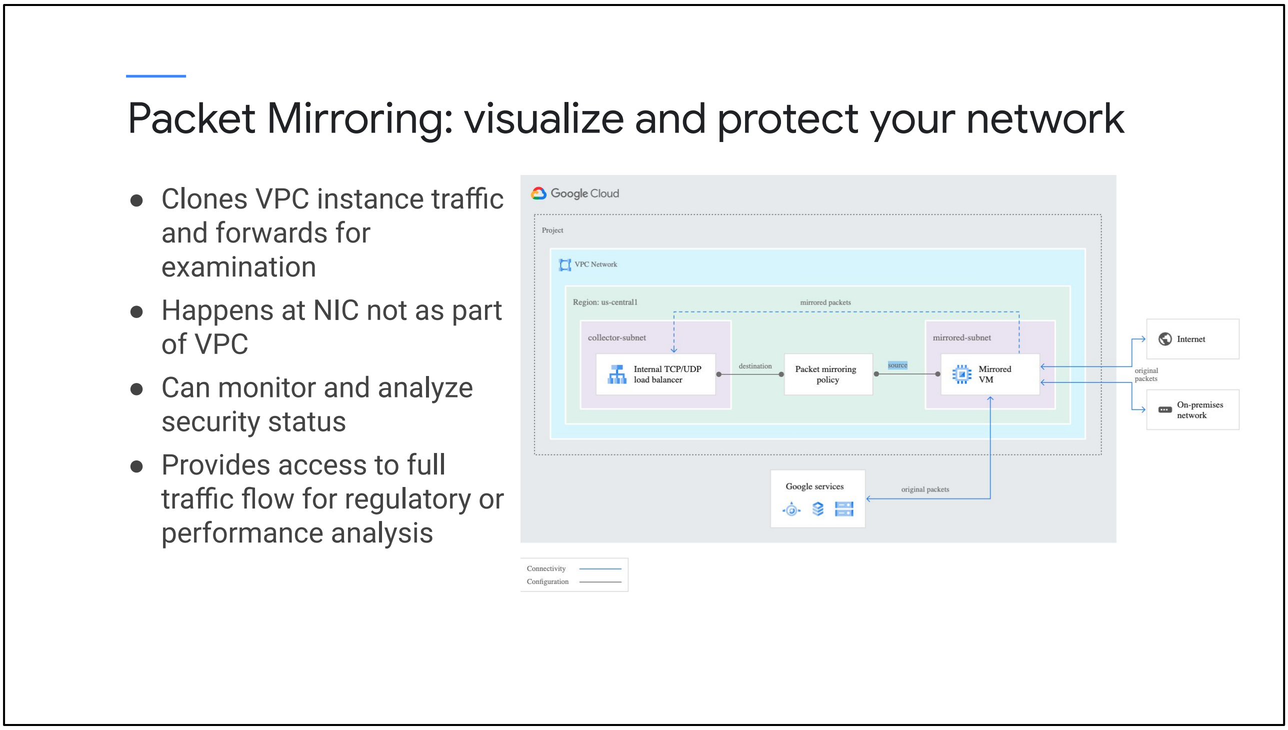
Agenda

Monitoring Network Security

- VPC Flow Logs
- Firewall Rules Logging
- Cloud NAT Logs
- Packet Mirroring
- Network Intelligence Center

Monitoring Cloud Audit Logs

Another way to monitor the network traffic flowing in and out of your Compute Engine virtual machines is to use packet mirroring.



Packet Mirroring: visualize and protect your network

- Clones VPC instance traffic and forwards for examination
- Happens at NIC not as part of VPC
- Can monitor and analyze security status
- Provides access to full traffic flow for regulatory or performance analysis

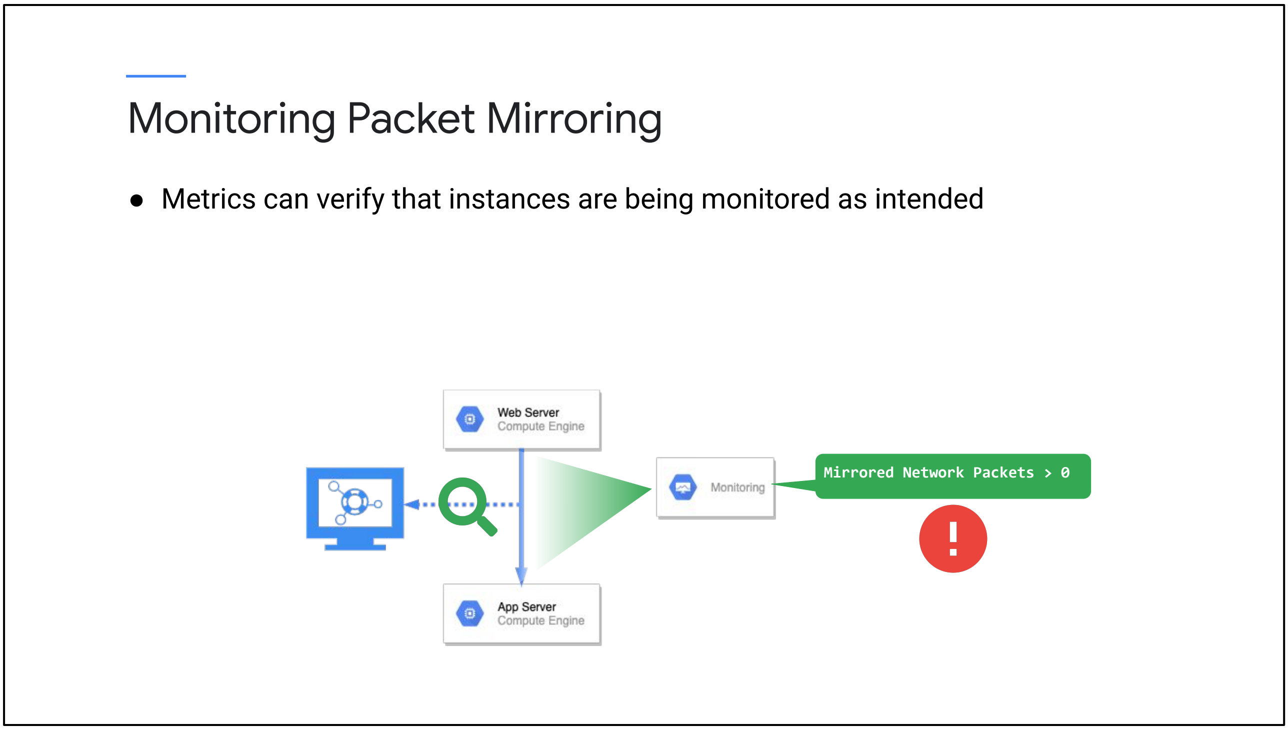
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all ingress and egress traffic and packet data, such as payloads and headers.

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 and to provide network forensics for PCI compliance and other regulatory use cases.

Obviously, this can generate a lot of data, so the recommended target is a load-balanced Compute Engine Managed Instance Group or equivalent technology.



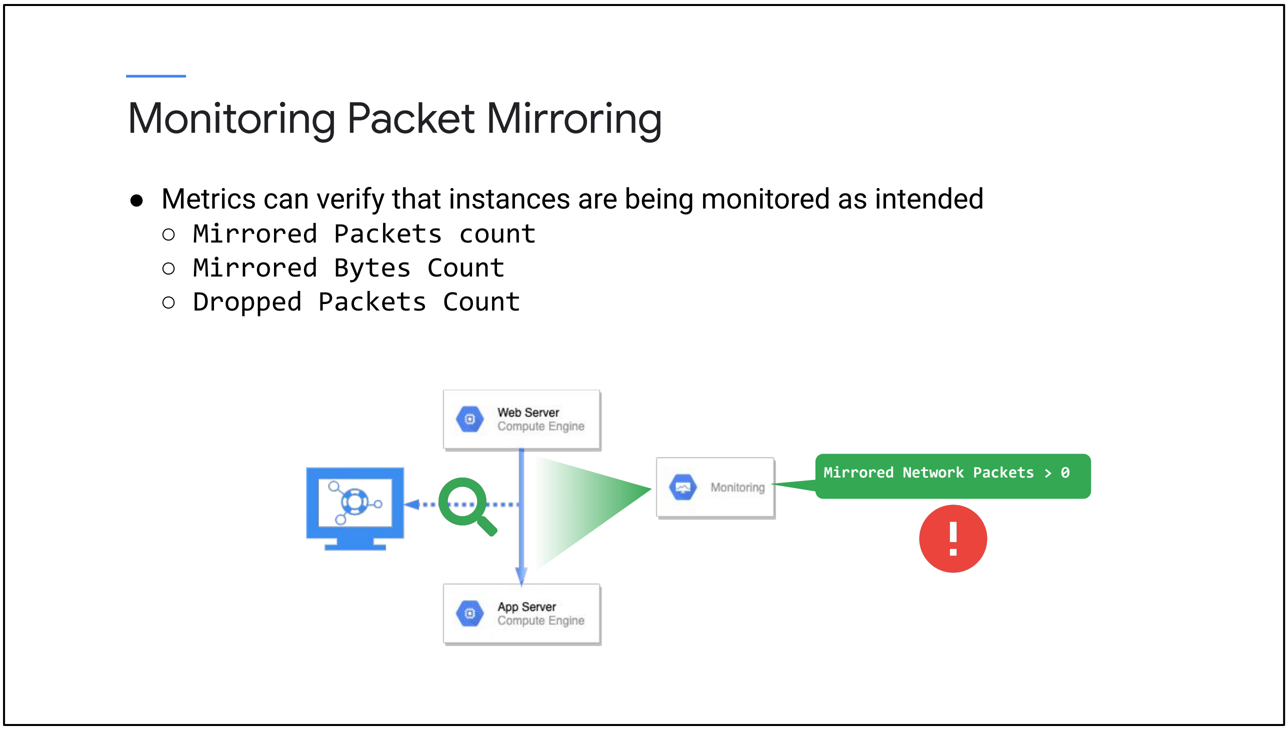
Monitoring Packet Mirroring

- Metrics can verify that instances are being monitored as intended

Packet Mirroring exports monitoring data about mirrored traffic to Cloud Monitoring.

You can use monitoring metrics to check whether traffic from a VM instance is being mirrored as intended.

For example, you can view the mirrored packet or byte count for a particular instance.



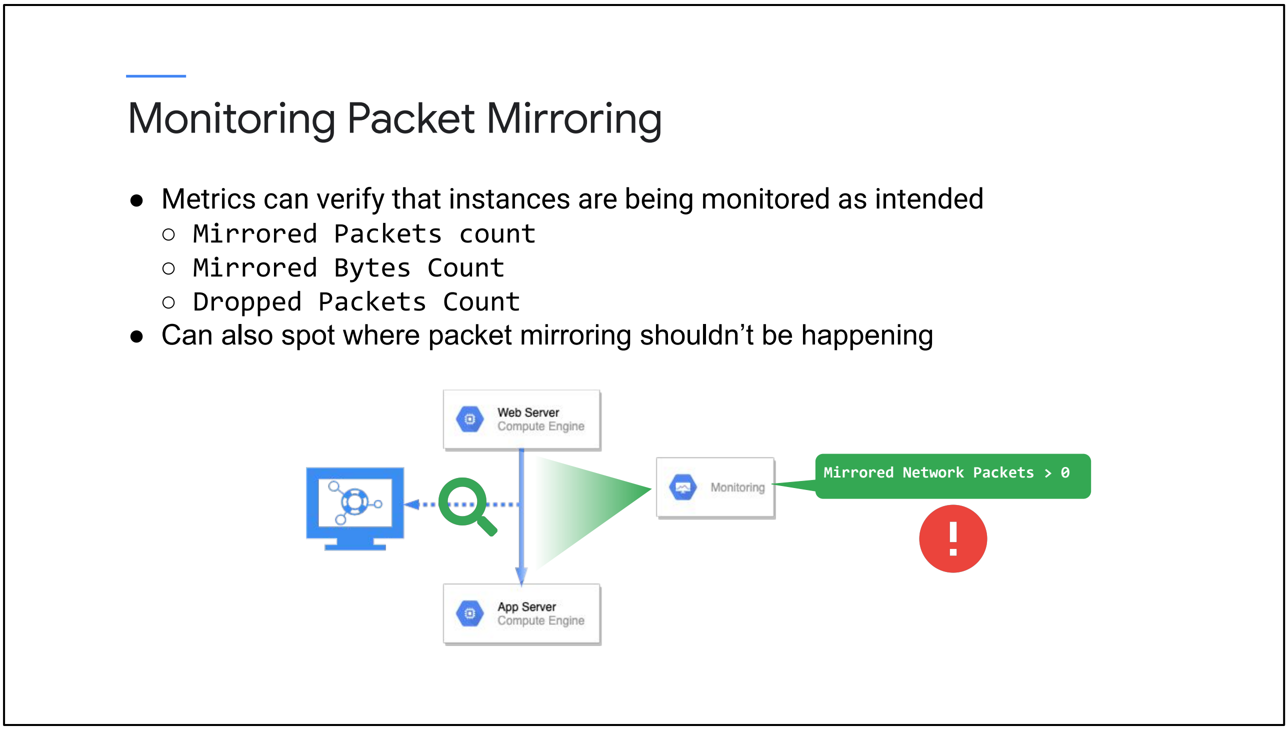
Monitoring Packet Mirroring

- Metrics can verify that instances are being monitored as intended
  - `Mirrored Packets count`
  - `Mirrored Bytes Count`
  - `Dropped Packets Count`

Web Server
Compute Engine
Monitoring
Mirrored Network Packets > 0
!
App Server
Compute Engine

You can view the monitoring metrics of mirrored VM instances or instances that are part of the collector destination (internal load balancer).

For mirrored VM instances, Packet Mirroring provides metrics specific to mirrored packets, such as /mirroring/mirrored_packets_count, /mirroring/mirrored_bytes_count, and /mirroring/dropped_packets_count.

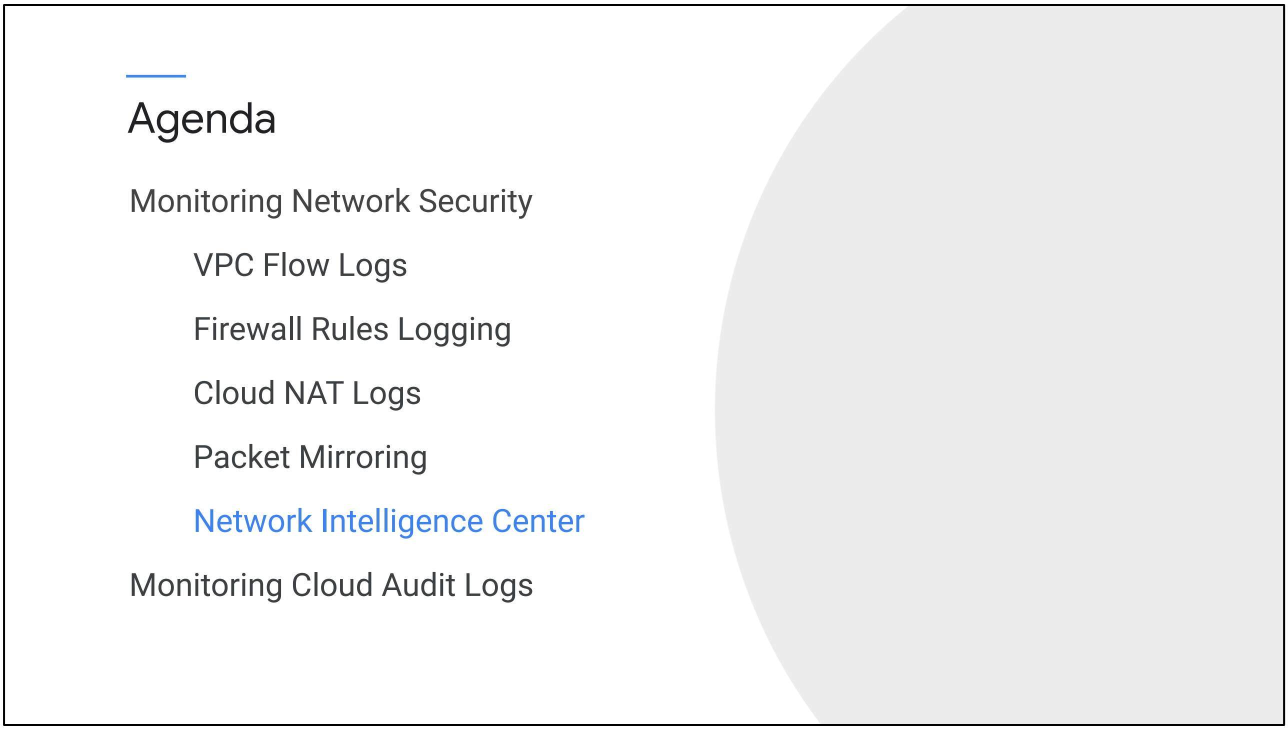


Monitoring Packet Mirroring

- Metrics can verify that instances are being monitored as intended
  - `Mirrored Packets count`
  - `Mirrored Bytes Count`
  - `Dropped Packets Count`
- Can also spot where packet mirroring shouldn't be happening

Monitoring can also spot where packet mirroring is being used unnecessarily or unexpectedly.

Keep in mind that, as noted, mirroring generates a lot of data that requires storage and processing, but also note that it slows the network throughput of the virtual machines being monitored and may accidentally expose sensitive data.



Agenda

Monitoring Network Security

- VPC Flow Logs
- Firewall Rules Logging
- Cloud NAT Logs
- Packet Mirroring
- Network Intelligence Center

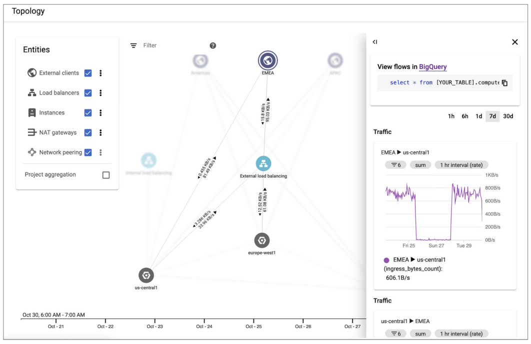
Monitoring Cloud Audit Logs

This section is a bit of a detour, but let’s at least mention the Network Intelligence Center and how it helps with network analysis.

Network Intelligence Center

Centralized Network monitoring and visibility

- Topology: view VPC topology and associated metrics
- Connectivity Tests: Evaluate connectivity to and from VPC resources
- Performance Dashboard: VPC packet loss and latency metrics
- Firewall Insights: Visibility into firewall usage and configuration issues



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

Google's Network Intelligence Center is all about giving you centralized monitoring and visibility into your network, reducing troubleshooting time and effort, increasing network security, all while improving the overall user experience.

Currently, it offers four modules: network topology, connectivity testing, a performance dashboard, and firewall insights.

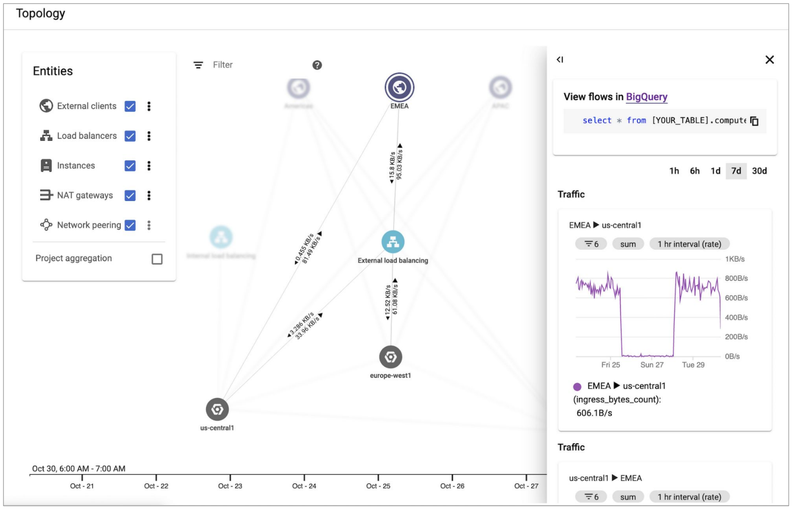
Network Topology is a visualization tool for viewing the topology of your VPC networks and the metrics that are associated with their Google Cloud resources.

Connectivity Tests enables you to evaluate connectivity to and from Google Cloud resources in your Virtual Private Cloud (VPC) network, by performing a static analysis of your resource configurations.

Performance Dashboard gives you visibility into the performance of your VPC network. It provides packet loss and latency (Round Trip Time) metrics between the zones where you have VMs.

Firewall Insights provides visibility into firewall usage and detects firewall configuration issues.

Topology



Topology

Entities

- External clients ☑
- Load balancers ☑
- Instances ☑
- NAT gateways ☑
- Network peering ☑

Project aggregation □

View flows in BigQuery

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

1h 6h 1d 7d 30d

Traffic

EMEA ▶ us-central1

6 sum 1 hr interval (rate)

● EMEA ▶ us-central1 (ingress_bytes_count): 606.1B/s

Traffic

us-central1 ▶ EMEA

6 sum 1 hr interval (rate)

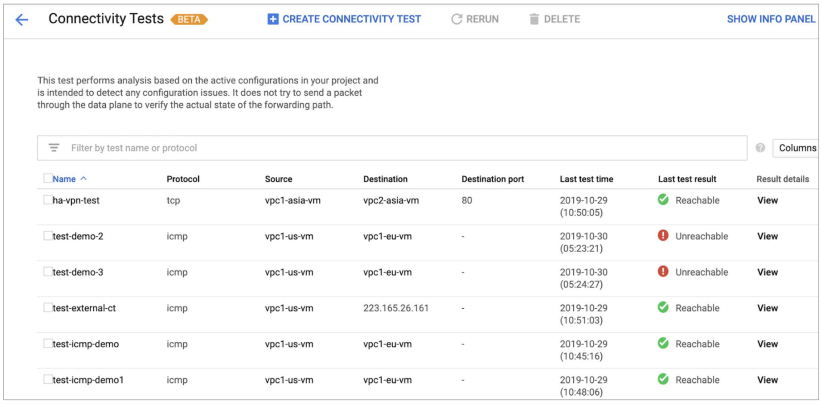
Network Topology visualizes your Google Cloud network as a graph.

You can use the graph to explore your existing configurations and quickly troubleshoot networking issues.

You can select network entities, filter, see lines of communication with bandwidth information, expand and collapse hierarchies, select time boundaries, and details for the item selected.

Connectivity Tests

- Quickly diagnose connectivity issues and prevent outages
- Verify configuration change impact to help prevent outages



This test performs analysis based on the active configurations in your project and is intended to detect any configuration issues. It does not try to send a packet through the data plane to verify the actual state of the forwarding path.

□ Name	Protocol	Source	Destination	Destination port	Last test time	Last test result	Result details
□ ha-vpn-test	tcp	vpc1-asia-vm	vpc2-asia-vm	80	2019-10-29 (10:50:05)	✓ Reachable	View
□ test-demo-2	icmp	vpc1-us-vm	vpc1-eu-vm	-	2019-10-30 (05:23:21)	! Unreachable	View
□ test-demo-3	icmp	vpc1-us-vm	vpc1-eu-vm	-	2019-10-30 (05:24:27)	! Unreachable	View
□ test-external-ct	icmp	vpc1-us-vm	223.165.26.161	-	2019-10-29 (10:51:03)	✓ Reachable	View
□ test-icmp-demo	icmp	vpc1-us-vm	vpc1-eu-vm	-	2019-10-29 (10:45:16)	✓ Reachable	View
□ test-icmp-demo1	icmp	vpc1-us-vm	vpc1-eu-vm	-	2019-10-29 (10:48:06)	✓ Reachable	View

Network Intelligence Center Connectivity Tests help to quickly diagnose connectivity issues and prevent outages.

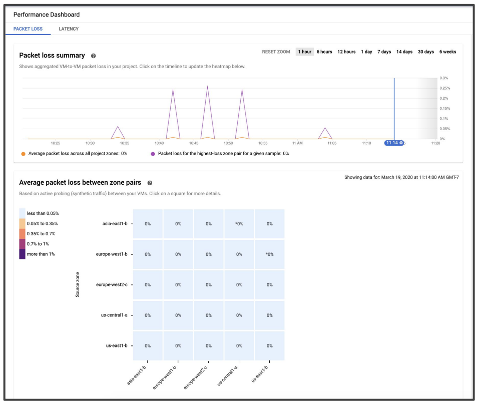
These tests enable you to self-diagnose connectivity issues within GCP or GCP to an external IP address (which could be on-prem or in another cloud) helping to isolate whether the issue is in GCP or not.

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.

Performance dashboard

- Packet loss metrics aggregated across zones



Packet loss summary

Shows aggregated VM-to-VM packet loss in your project. Click on the timeline to update the heatmap below.

● Average packet loss across all project zones: 0%

● Packet loss for the highest-loss zone pair for a given sample: 0%

Average packet loss between zone pairs

Showing data for: March 19, 2020 at 11:14:00 AM GMT-7

Based on active probing (synthetic traffic) between your VMs. Click on a square for more details.

Source zone	asia-east1-b	europe-west1-b	europe-west2-c	us-central1-a	us-east1-b
asia-east1-b	0%	0%	0%	*0%	0%
europe-west1-b	0%	0%	0%	0%	*0%
europe-west2-c	0%	0%	0%	0%	0%
us-central1-a	0%	0%	0%	0%	0%
us-east1-b	0%	0%	0%	0%	0%

Performance Dashboard gives you visibility into the performance of your VPC.

The Packet Loss tab shows the results of active probing between your VMs in a given VPC.

To get this data, it runs workers on the physical hosts that house your VMs.

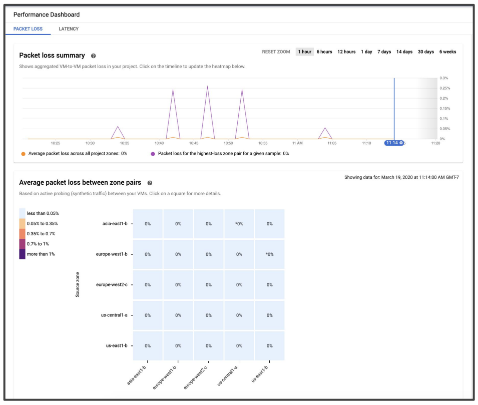
These workers insert and receive probe packets that run on the same network as your traffic, revealing issues on that network.

Because the workers run on the physical host and not on your VM, these workers do not consume VM resources and the traffic is not visible on your VMs.

Packet loss is aggregated for all zone pairs.

Performance dashboard

- Packet loss metrics aggregated across zones
- Median Latency summaries aggregated across zones



Performance Dashboard

PACKET LOSS LATENCY

Packet loss summary

RESET ZOOM 1 hour 6 hours 12 hours 1 day 7 days 14 days 30 days 6 weeks

Shows aggregated VM-to-VM packet loss in your project. Click on the timeline to update the heatmap below.

● Average packet loss across all project zones: 0%
● Packet loss for the highest-loss zone pair for a given sample: 0%

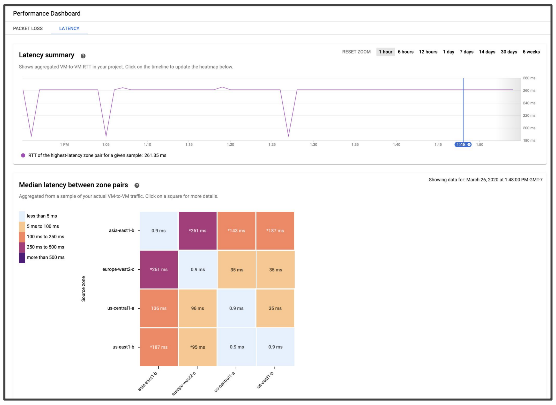
Average packet loss between zone pairs

Showing data for: March 19, 2020 at 11:14:00 AM GMT-7

Based on active probing (synthetic traffic) between your VMs. Click on a square for more details.

- less than 0.05%
- 0.05% to 0.35%
- 0.35% to 0.7%
- 0.7% to 1%
- more than 1%

Source zone	asia-east1-b	europe-west1-b	europe-west2-c	us-central1-a	us-east1-b
asia-east1-b	0%	0%	0%	*0%	0%
europe-west1-b	0%	0%	0%	0%	*0%
europe-west2-c	0%	0%	0%	0%	0%
us-central1-a	0%	0%	0%	0%	0%
us-east1-b	0%	0%	0%	0%	0%



Performance Dashboard

PACKET LOSS LATENCY

Latency summary

RESET ZOOM 1 hour 6 hours 12 hours 1 day 7 days 14 days 30 days 6 weeks

Shows aggregated VM-to-VM RTT in your project. Click on the timeline to update the heatmap below.

● RTT of the highest-latency zone pair for a given sample: 261.35 ms

Median latency between zone pairs

Showing data for: March 26, 2020 at 1:48:00 PM GMT-7

Aggregated from a sample of your actual VM-to-VM traffic. Click on a square for more details.

- less than 5 ms
- 5 ms to 100 ms
- 100 ms to 250 ms
- 250 ms to 500 ms
- more than 500 ms

Source zone	asia-east1-b	europe-west2-c	us-central1-a	us-east1-b
asia-east1-b	0.9 ms	*261 ms	*143 ms	*187 ms
europe-west2-c	*261 ms	0.9 ms	35 ms	35 ms
us-central1-a	136 ms	96 ms	0.9 ms	35 ms
us-east1-b	*187 ms	*95 ms	0.9 ms	0.9 ms

The Latency tab aggregates latency information based on a sample of your actual TCP VM traffic, using a method similar to the one used for VPC Flow Logs.

The latency is calculated as the time that elapses between sending a TCP sequence number (SEQ) and receiving a corresponding ACK that contains the network RTT and TCP stack related delay.

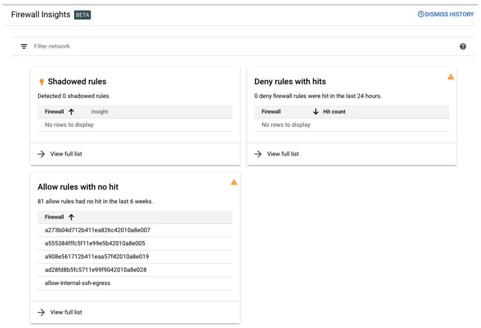
The latency metric is only available if TCP traffic is around 1000 packets per minute or higher.

Firewall Insights

- Metrics to help understand and optimize firewall configurations
  - Based on data collected by Firewall Rules Logging

Reports included for every firewall with logging enabled

- Allow/deny counts
- Last Used
- Unused rules
- Shadowed rules



Firewall Insights BETA

Shadowed rules

Detected 0 shadowed rules.

Firewall ↑	Insight
No rows to display	

Deny rules with hits

0 deny firewall rules were hit in the last 24 hours.

Firewall	↓ Hit count
No rows to display	

Allow rules with no hit

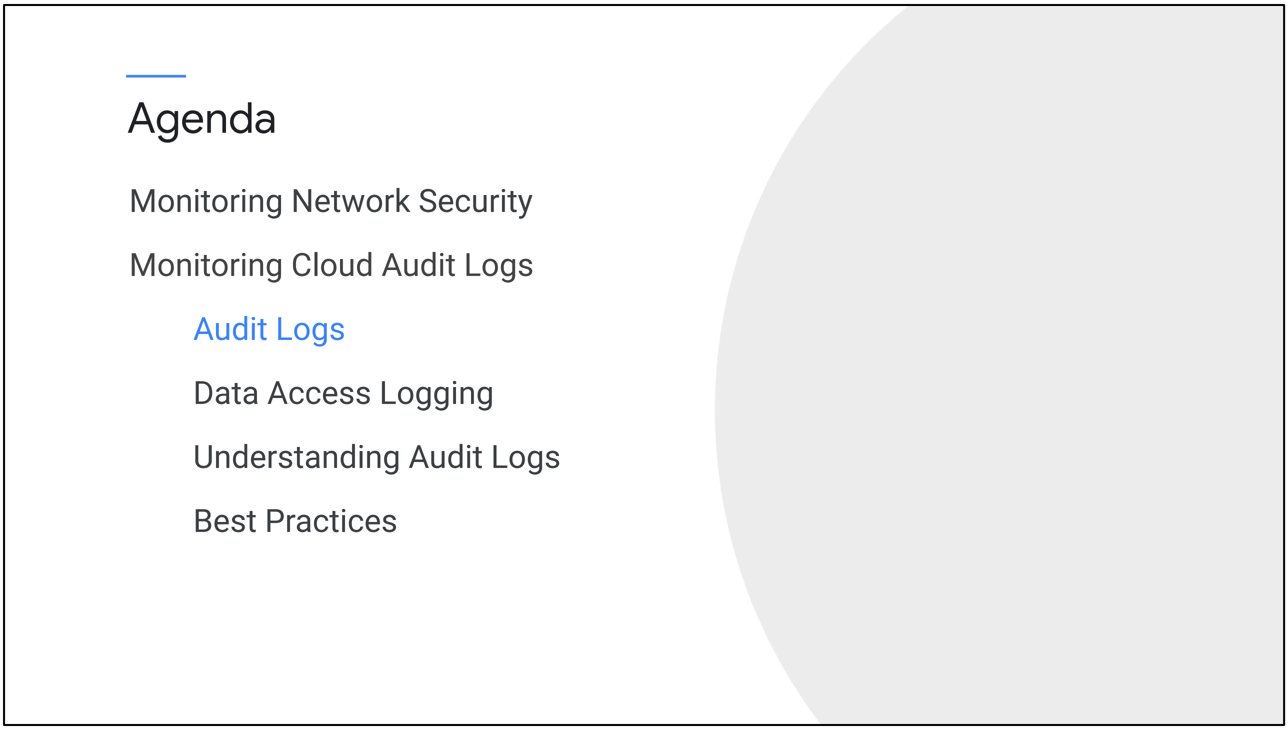
81 allow rules had no hit in the last 6 weeks.

Firewall ↑
a273b04d712b411ea826c42010a8e007
a555384fffc5f11e99e5b42010a8e005
a908e561712b411eaa57f42010a8e019
ad28fd8b5fc5711e99f9042010a8e028
allow-internal-ssh-egress

Firewall Insights enables you to better understand and safely optimize your firewall configurations by analyzing Firewall Rules logs and providing reports on firewall usage, and the impact of various firewall rules on your VPC.

For each firewall rule with logging enabled, you can see:

- How many times the firewall rule has blocked or allowed connections.
- The last time a particular firewall rule was applied to allow or deny traffic.
- A list of firewall rules that haven't been used in the last six weeks.
- and Shadowed firewall rules. (A *shadowed rule* is a firewall rule that has all of its relevant attributes, such as IP address range and ports, overlapped by attributes from one or more other firewall rules with higher or equal priority. A firewall doesn't evaluate a shadowed rule because of the overlap and because the shadowed rule has a lower priority than its shadowing rules.)



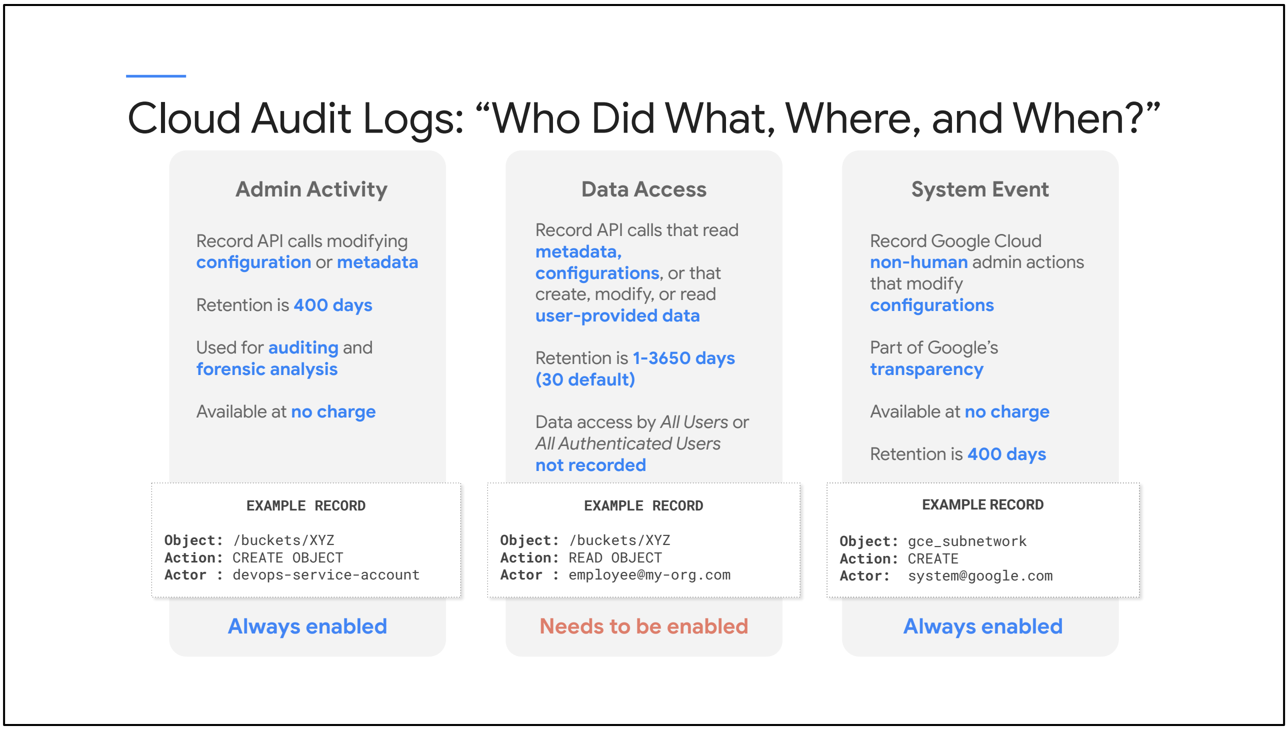
Agenda

Monitoring Network Security

Monitoring Cloud Audit Logs

- Audit Logs
- Data Access Logging
- Understanding Audit Logs
- Best Practices

In terms of sheer volume of useful information, probably the most important group of logs in Google Cloud are the Audit Logs.



Cloud Audit Logs: “Who Did What, Where, and When?”

Admin Activity

Record API calls modifying **configuration** or **metadata**

Retention is **400 days**

Used for **auditing** and **forensic analysis**

Available at **no charge**

EXAMPLE RECORD

```
Object: /buckets/XYZ
Action: CREATE OBJECT
Actor : devops-service-account
```

Always enabled

Data Access

Record API calls that read **metadata, configurations**, or that create, modify, or read **user-provided data**

Retention is **1-3650 days (30 default)**

Data access by *All Users* or *All Authenticated Users* **not recorded**

EXAMPLE RECORD

```
Object: /buckets/XYZ
Action: READ OBJECT
Actor : employee@my-org.com
```

Needs to be enabled

System Event

Record Google Cloud **non-human** admin actions that modify **configurations**

Part of Google’s **transparency**

Available at **no charge**

Retention is **400 days**

EXAMPLE RECORD

```
Object: gce_subnetwork
Action: CREATE
Actor:  system@google.com
```

Always enabled

Cloud Audit Logs help answer the question, "Who did what, when, and where?

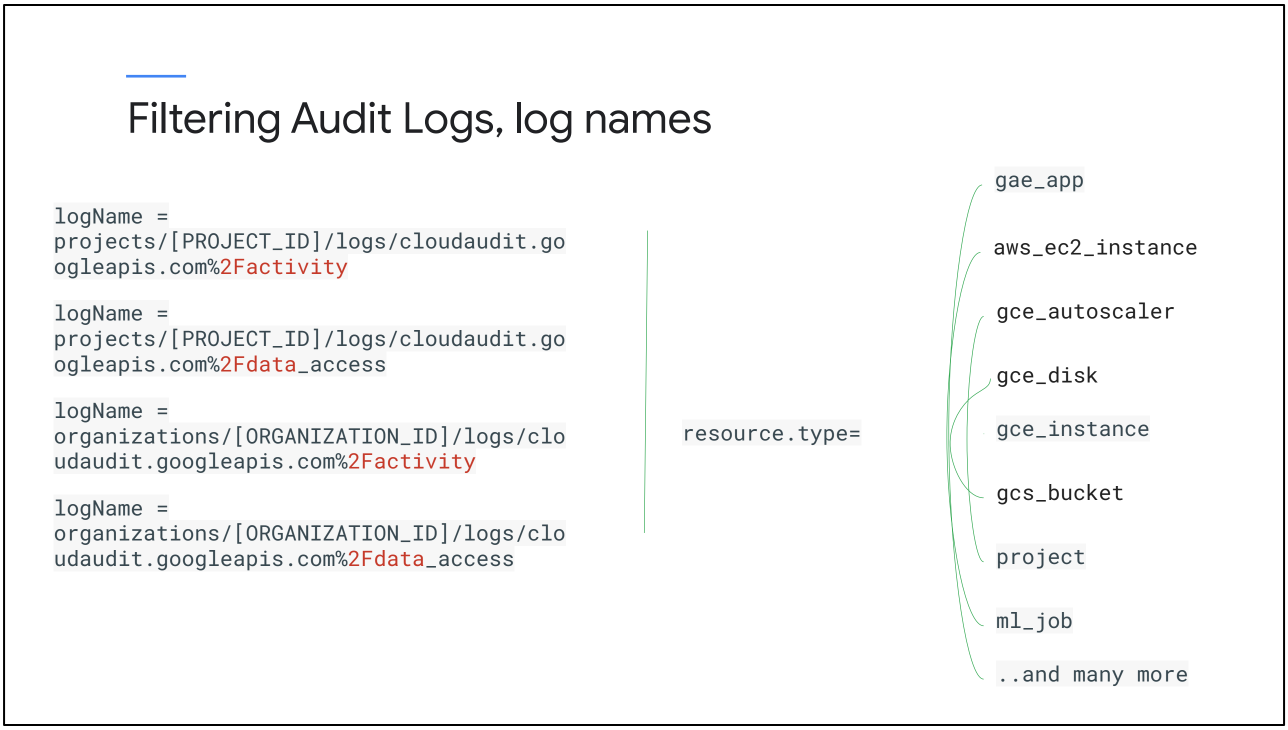
It maintains three audit logs for each Google Cloud project, folder, and organization: **Admin Activity**, **Data Access**, and **System Event**. All Google Cloud services will eventually provide audit logs. For now, see the Google services with audit logs documentation for coverage details.

Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Cloud Identity and Access Management permissions. They are always on, are retained for 400 days, and are available at no charge. To view these logs, you must have the Cloud IAM role **Logging/Logs Viewer** or **Project/Viewer**.

Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data. Data Access audit logs do not record the data-access operations on resources that are publicly shared (available to **All Users** or **All Authenticated Users**), or that can be accessed without logging into Google Cloud. They are disabled by default (except for BigQuery), and when enabled, the default retention is 30 days. To view these logs, you must have the Cloud IAM roles **Logging/Private Logs**

Viewer or **Project/Owner**.

System Event audit logs contain log entries for Google Cloud administrative actions that modify the configuration of resources. System Event audit logs are generated by Google systems; they are not driven by direct user action.
They are always enabled, free, and are retained for 400 days. To view these logs, you must have the Cloud IAM role **Logging/Logs Viewer** or **Project/Viewer**.



Filtering Audit Logs, log names

```
logName =
projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Factivity

logName =
projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Fdata_access

logName =
organizations/[ORGANIZATION_ID]/logs/cloudaudit.googleapis.com%2Factivity

logName =
organizations/[ORGANIZATION_ID]/logs/cloudaudit.googleapis.com%2Fdata_access
```

`resource.type=`

- `gae_app`
- `aws_ec2_instance`
- `gce_autoscaler`
- `gce_disk`
- `gce_instance`
- `gcs_bucket`
- `project`
- `ml_job`
- `..and many more`

Here is an easy, but not foolproof, trick to try.
Put the Logs Viewer in advanced mode and simply type “AuditLog” in the filter box.
That will find all audit log entries of all types, but be aware that it might also pick up non-audit log entries as well.

When looking for a particular log, a better way would be to set the resource.type to the Google Cloud resource type whose audit logs you want to see.
Then you can query: `logName = ("[log file name]")`

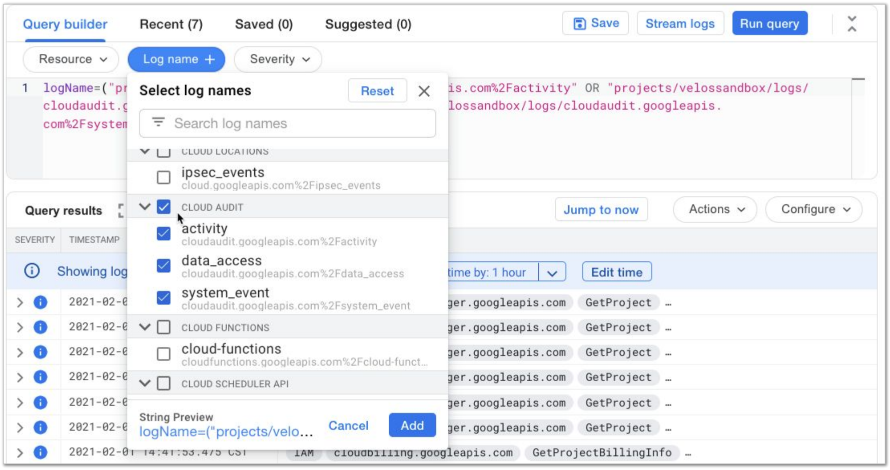
Where the name is one of the following. In the examples, PROJECT_ID can actually be the project id, folder id, or organization id:

```
projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Factivity

projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Fdata_access

projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Fsystem_event
```

Filtering Audit Logs, an example



```
logName=("pr                    is.com%2Factivity" OR "projects/velossandbox/logs/
cloudaudit.g                    lossandbox/logs/cloudaudit.googleapis.
com%2Fsystem
```

- CLOUD LOCATIONS
  - □ ipsec_events cloud.googleapis.com%2Fipsec_events
- ☑ CLOUD AUDIT
  - ☑ activity cloudaudit.googleapis.com%2Factivity
  - ☑ data_access cloudaudit.googleapis.com%2Fdata_access
  - ☑ system_event cloudaudit.googleapis.com%2Fsystem_event
- □ CLOUD FUNCTIONS
  - □ cloud-functions cloudfunctions.googleapis.com%2Fcloud-funct...
- □ CLOUD SCHEDULER API

String Preview logName=("projects/velo...

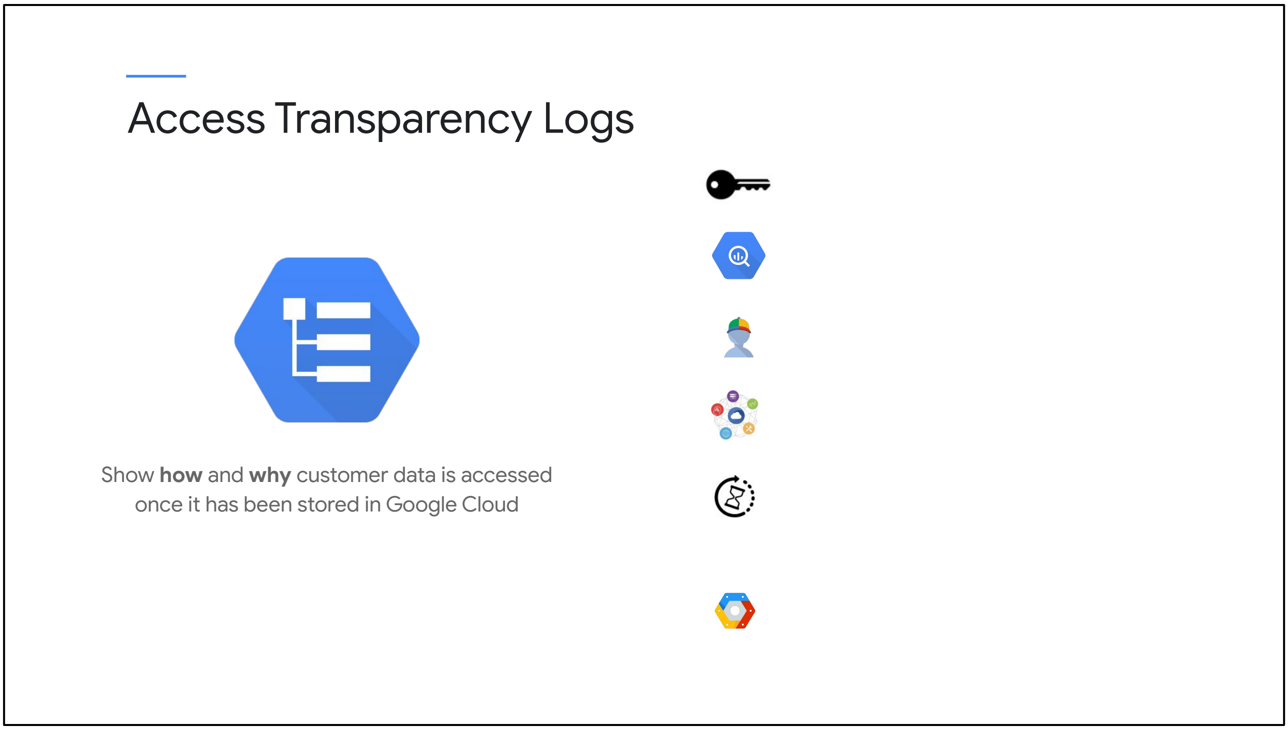
```
2021-02-0   ger.googleapis.com  GetProject ...
2021-02-0   ger.googleapis.com  GetProject ...
2021-02-0   ger.googleapis.com  GetProject ...
2021-02-0   ger.googleapis.com  GetProject ...
2021-02-0   ger.googleapis.com  GetProject ...
2021-02-0   ger.googleapis.com  GetProject ...
2021-02-01 14:41:53.475 CST   IAM  cloudbilling.googleapis.com  GetProjectBillingInfo ...
```

Here's an example where:

The resource is set to App Engine.

The log names are then set to the data access and admin activity logs for a single project.

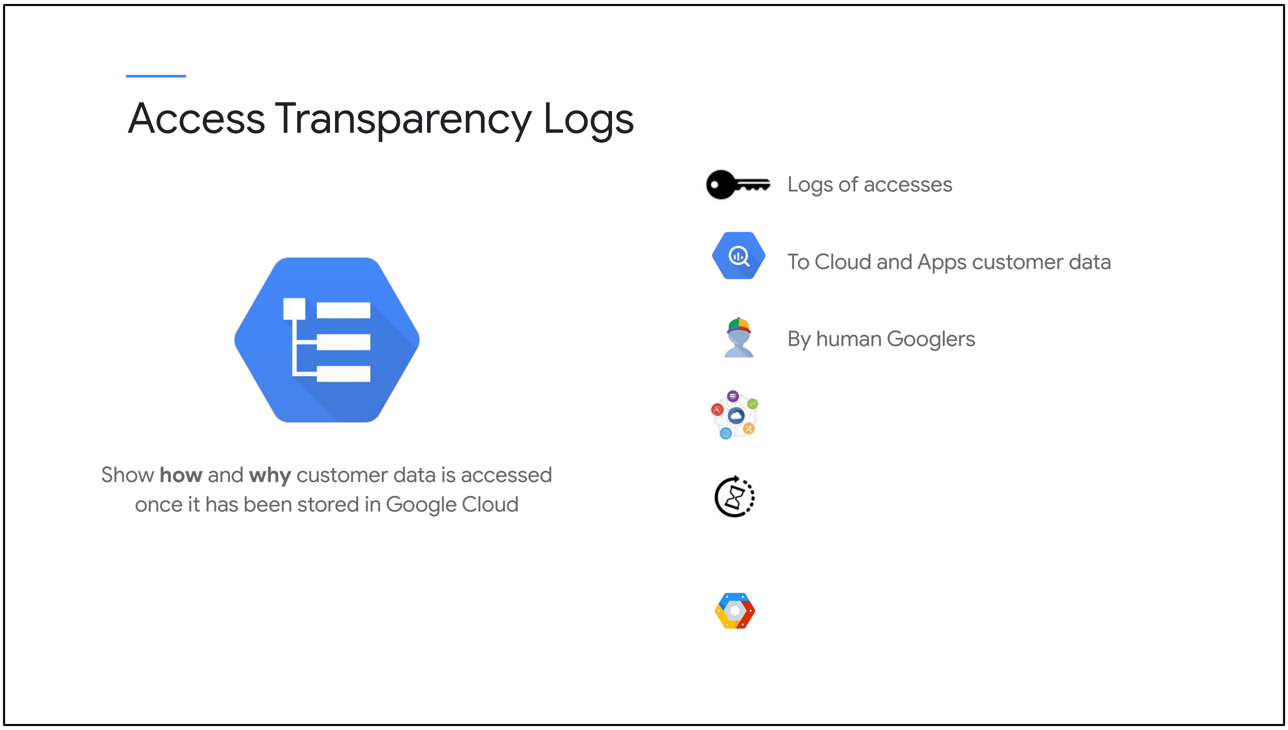
You see the results below the query.



Access Transparency Logs

Show **how** and **why** customer data is accessed once it has been stored in Google Cloud

Whether it's a hardware support engineer, or a rep working on a ticket, having dedicated experts manage parts of the infrastructure is a key benefit of operating in Google Cloud.

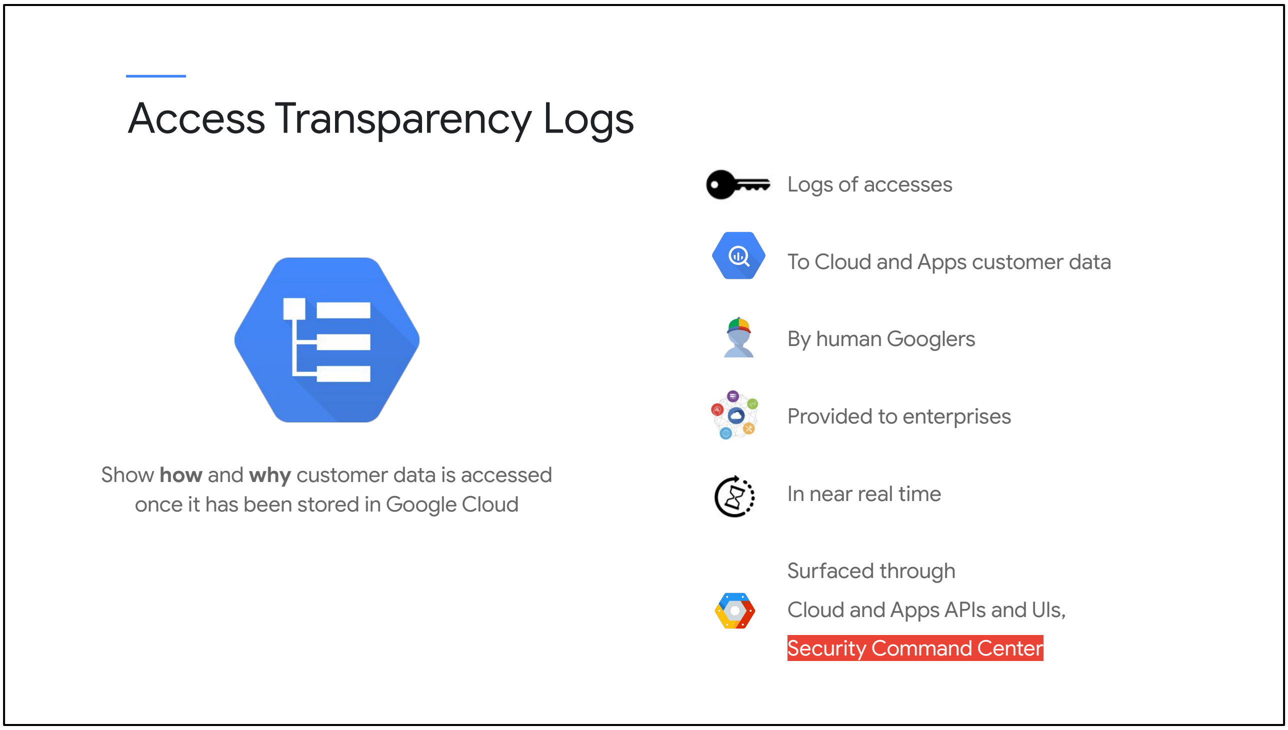


Access Transparency Logs

Show **how** and **why** customer data is accessed once it has been stored in Google Cloud

- Logs of accesses
- To Cloud and Apps customer data
- By human Googlers

Access transparency logs help by providing logs of accesses to your data by human Googlers (as opposed to automated systems).

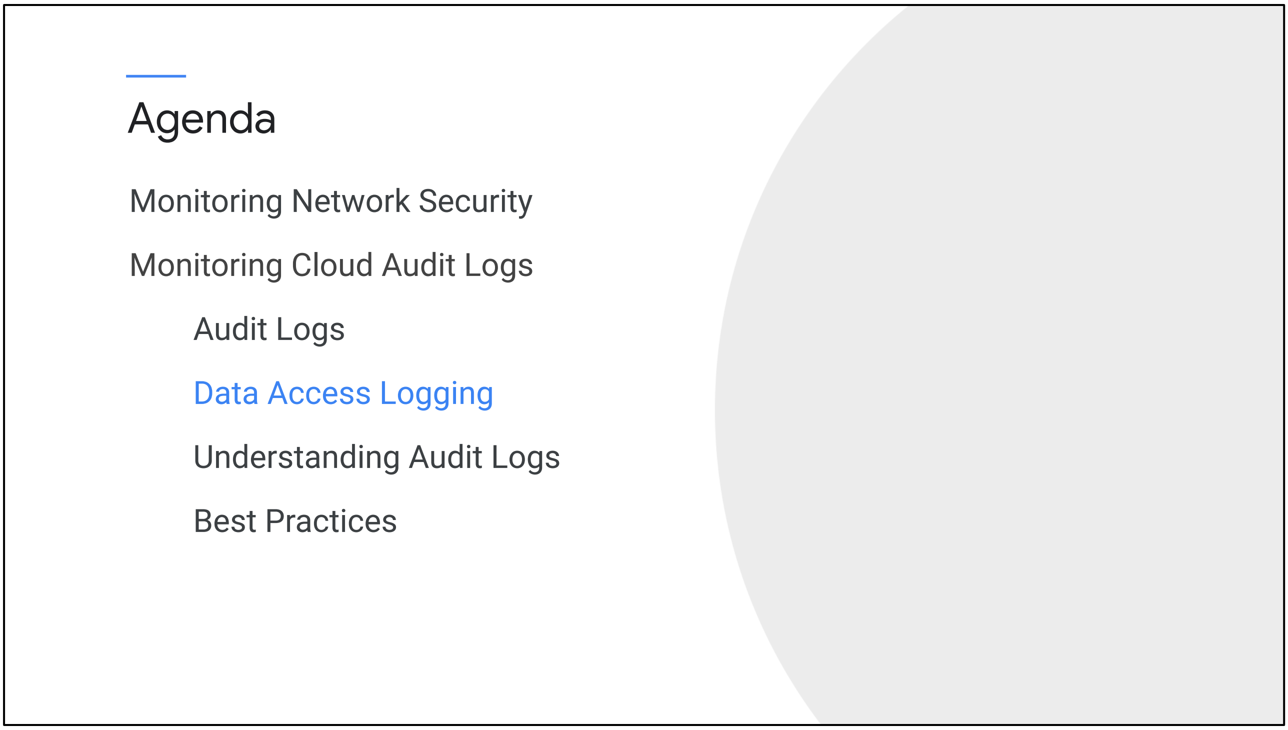


Access Transparency Logs

Show **how** and **why** customer data is accessed once it has been stored in Google Cloud

- Logs of accesses
- To Cloud and Apps customer data
- By human Googlers
- Provided to enterprises
- In near real time
- Surfaced through Cloud and Apps APIs and UIs, Security Command Center

Enterprises with appropriate support packages can enable the logs, and receive the log events in near real-time, surfaced through the APIs, Cloud Logging, and Security Command Center



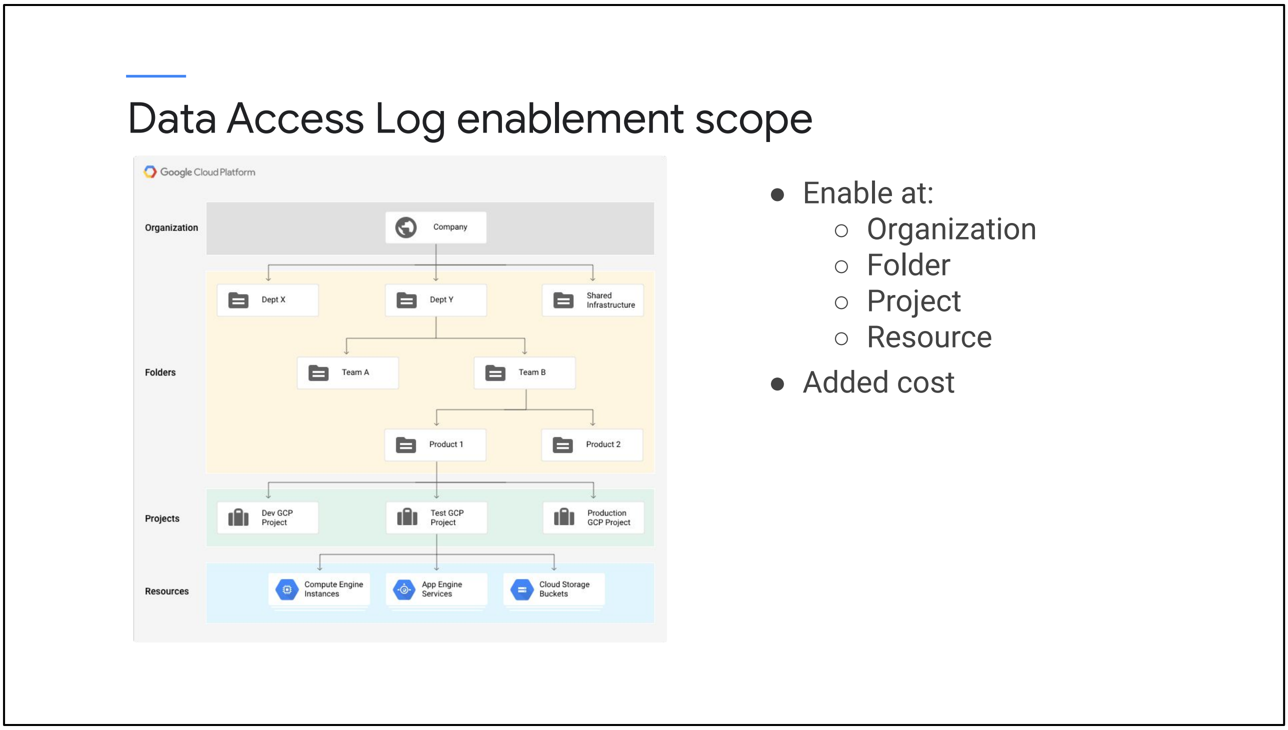
Agenda

Monitoring Network Security

Monitoring Cloud Audit Logs

- Audit Logs
- Data Access Logging
- Understanding Audit Logs
- Best Practices

Let’s continue by taking a look at Data Access Logs.



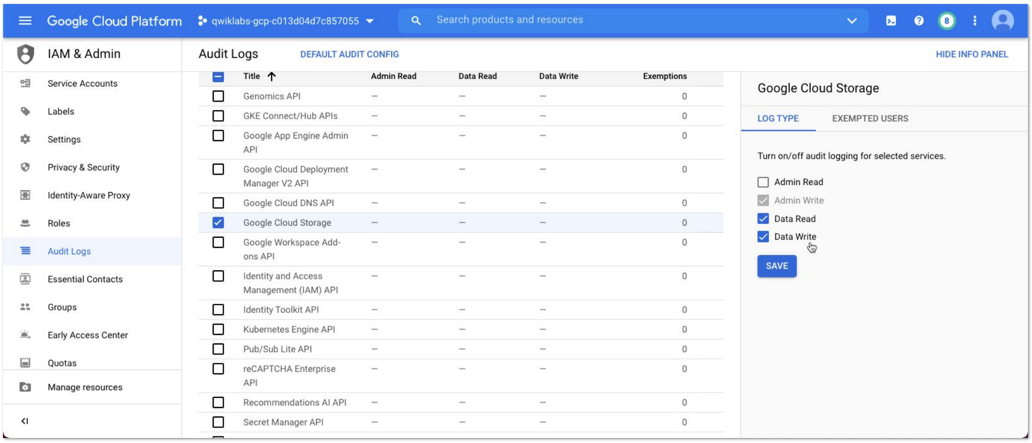
Data Access Log enablement scope

- Enable at:
  - Organization
  - Folder
  - Project
  - Resource
- Added cost

Data Access logs can be enabled at the organization, folder, project, or resources levels.

The added logging does add to the cost, currently: $.50 per gigabyte for ingestion.

Enabling Data Access logging per Google Cloud service



Audit Logs

	Title ↑	Admin Read	Data Read	Data Write	Exemptions
□	Genomics API	–	–	–	0
□	GKE Connect/Hub APIs	–	–	–	0
□	Google App Engine Admin API	–	–	–	0
□	Google Cloud Deployment Manager V2 API	–	–	–	0
□	Google Cloud DNS API	–	–	–	0
☑	Google Cloud Storage	–	–	–	0
□	Google Workspace Add-ons API	–	–	–	0
□	Identity and Access Management (IAM) API	–	–	–	0
□	Identity Toolkit API	–	–	–	0
□	Kubernetes Engine API	–	–	–	0
□	Pub/Sub Lite API	–	–	–	0
□	reCAPTCHA Enterprise API	–	–	–	0
□	Recommendations AI API	–	–	–	0
□	Secret Manager API	–	–	–	0

Google Cloud Storage

LOG TYPE | EXEMPTED USERS

Turn on/off audit logging for selected services.

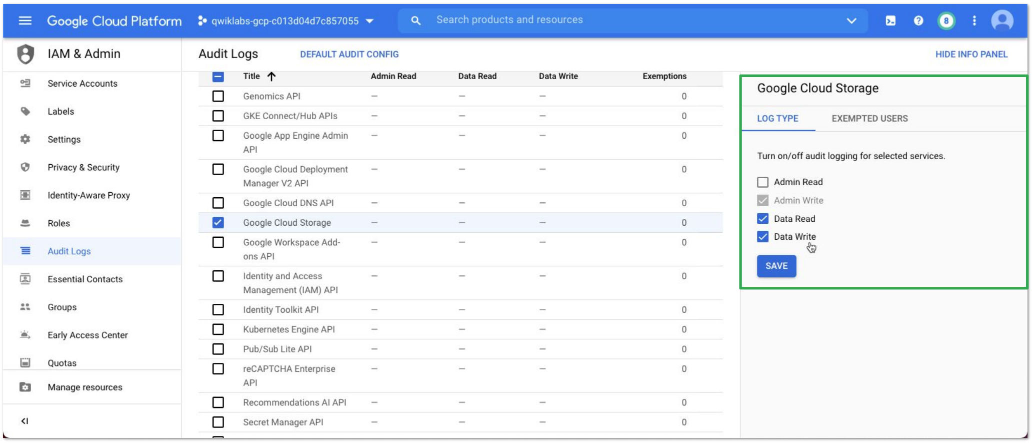
- □ Admin Read
- ☑ Admin Write
- ☑ Data Read
- ☑ Data Write

SAVE

Data Access logs are disabled by default, for everything but BigQuery.

You can enable and configure Data Access logs at the organization, folder, project, or service level.

Enabling Data Access logging per Google Cloud service



	Title	Admin Read	Data Read	Data Write	Exemptions
☐	Genomics API	–	–	–	0
☐	GKE Connect/Hub APIs	–	–	–	0
☐	Google App Engine Admin API	–	–	–	0
☐	Google Cloud Deployment Manager V2 API	–	–	–	0
☐	Google Cloud DNS API	–	–	–	0
☑	Google Cloud Storage	–	–	–	0
☐	Google Workspace Add-ons API	–	–	–	0
☐	Identity and Access Management (IAM) API	–	–	–	0
☐	Identity Toolkit API	–	–	–	0
☐	Kubernetes Engine API	–	–	–	0
☐	Pub/Sub Lite API	–	–	–	0
☐	reCAPTCHA Enterprise API	–	–	–	0
☐	Recommendations AI API	–	–	–	0
☐	Secret Manager API	–	–	–	0

Google Cloud Storage

LOG TYPE   EXEMPTED USERS

Turn on/off audit logging for selected services.

☐ Admin Read
☑ Admin Write
☑ Data Read
☑ Data Write

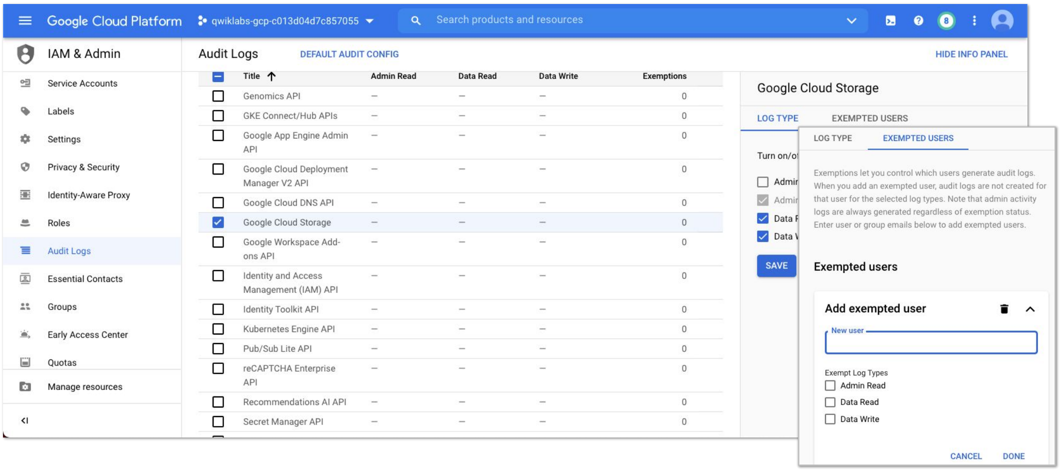
SAVE

You can control what kinds of information are kept in the audit logs.

There are three types of Data Access audit log information:

- **Admin-read:** Records operations that read metadata or configuration information. For example, you looked at the configurations for your bucket.
- **Data-read**: Records operations that read user-provided data. For example, you listed files and then downloaded one from GCS.
- **Data-write:** Records operations that write user-provided data. For example, you created a new GCS file.

Enabling Data Access logging per Google Cloud service



	Title	Admin Read	Data Read	Data Write	Exemptions
□	Genomics API	–	–	–	0
□	GKE Connect/Hub APIs	–	–	–	0
□	Google App Engine Admin API	–	–	–	0
□	Google Cloud Deployment Manager V2 API	–	–	–	0
□	Google Cloud DNS API	–	–	–	0
☑	Google Cloud Storage	–	–	–	0
□	Google Workspace Add-ons API	–	–	–	0
□	Identity and Access Management (IAM) API	–	–	–	0
□	Identity Toolkit API	–	–	–	0
□	Kubernetes Engine API	–	–	–	0
□	Pub/Sub Lite API	–	–	–	0
□	reCAPTCHA Enterprise API	–	–	–	0
□	Recommendations AI API	–	–	–	0
□	Secret Manager API	–	–	–	0

LOG TYPE | EXEMPTED USERS

Exemptions let you control which users generate audit logs. When you add an exempted user, audit logs are not created for that user for the selected log types. Note that admin activity logs are always generated regardless of exemption status. Enter user or group emails below to add exempted users.

Exempted users

Add exempted user

New user

Exempt Log Types

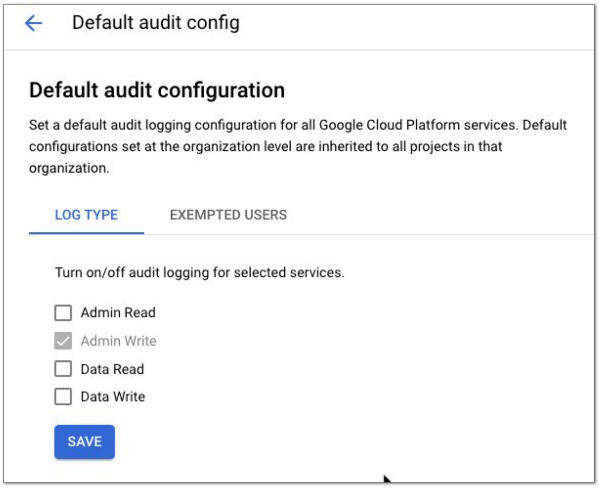
□ Admin Read
□ Data Read
□ Data Write

CANCEL DONE

You can exempt specific users or groups from having their data accesses recorded.

As an example, you might decide to exempt your internal testing accounts from having their Cloud Debugger operations recorded.

Setting the default Data Access Logging behavior



Default audit config

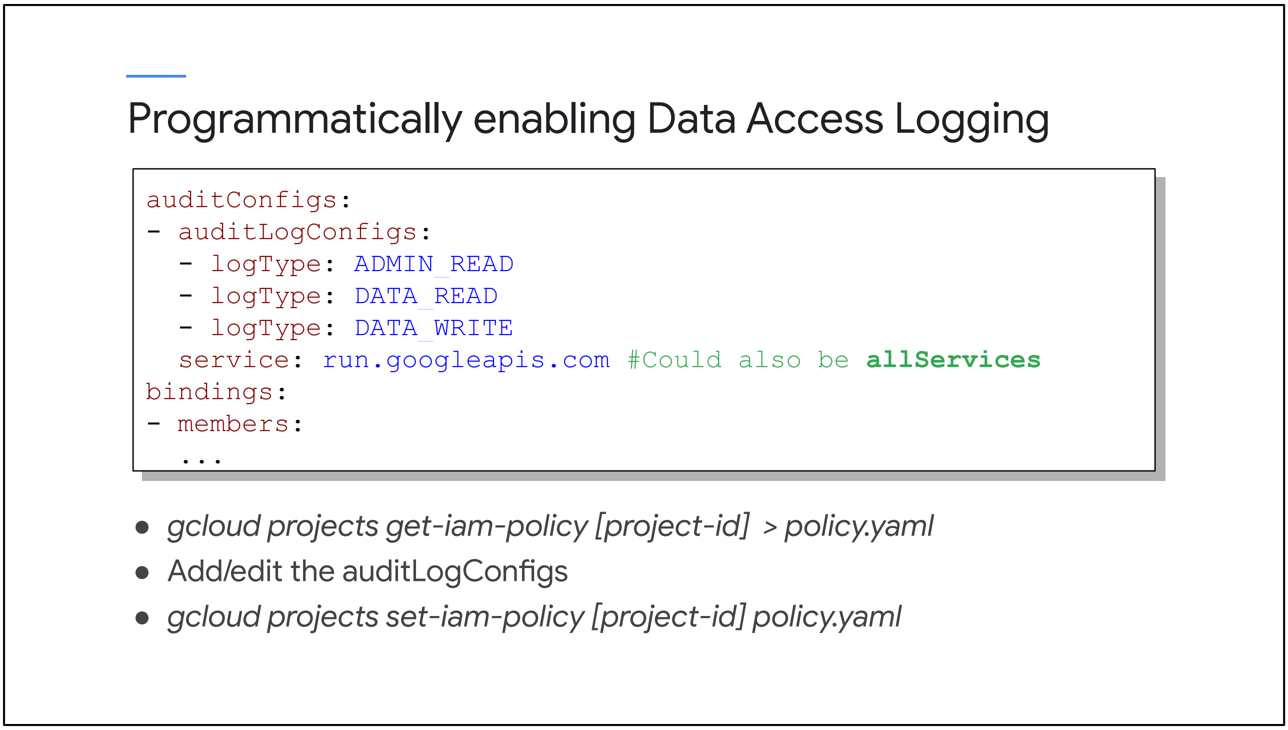
Default audit configuration

Set a default audit logging configuration for all Google Cloud Platform services. Default configurations set at the organization level are inherited to all projects in that organization.

Turn on/off audit logging for selected services.

- ☐ Admin Read
- ☑ Admin Write
- ☐ Data Read
- ☐ Data Write

Set a configuration for all new and existing Google Cloud services in your project, folder, or organization inherit, ensuring that Data Access audit logs are captured.



Programmatically enabling Data Access Logging

```
auditConfigs:
- auditLogConfigs:
  - logType: ADMIN_READ
  - logType: DATA_READ
  - logType: DATA_WRITE
  service: run.googleapis.com #Could also be allServices
bindings:
- members:
  ...
```

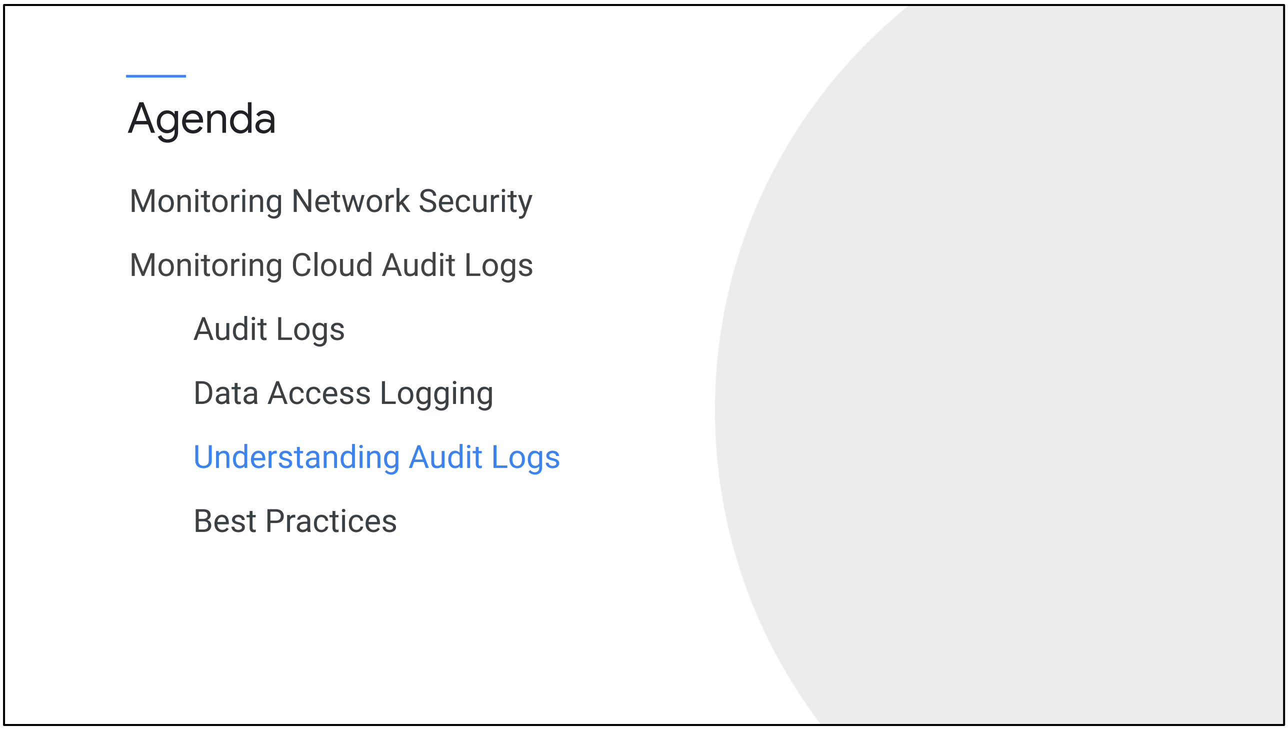
- *gcloud projects get-iam-policy [project-id] > policy.yaml*
- Add/edit the auditLogConfigs
- *gcloud projects set-iam-policy [project-id] policy.yaml*

You can also use gcloud or the API to enable data access logging.

If you're using gcloud, frequently, the easiest way is to get the current IAM policies, as seen in the bullet, and write them to a file.

Then you can edit the file to add or edit the auditLogConfigs. You can also add the log details per service, like this example is enabling logging for cloud run, or even enable logging on all services.

Then, as seen in the bullet, you would set that as the new IAM policy.



Agenda

Monitoring Network Security

Monitoring Cloud Audit Logs

- Audit Logs
- Data Access Logging
- Understanding Audit Logs
- Best Practices

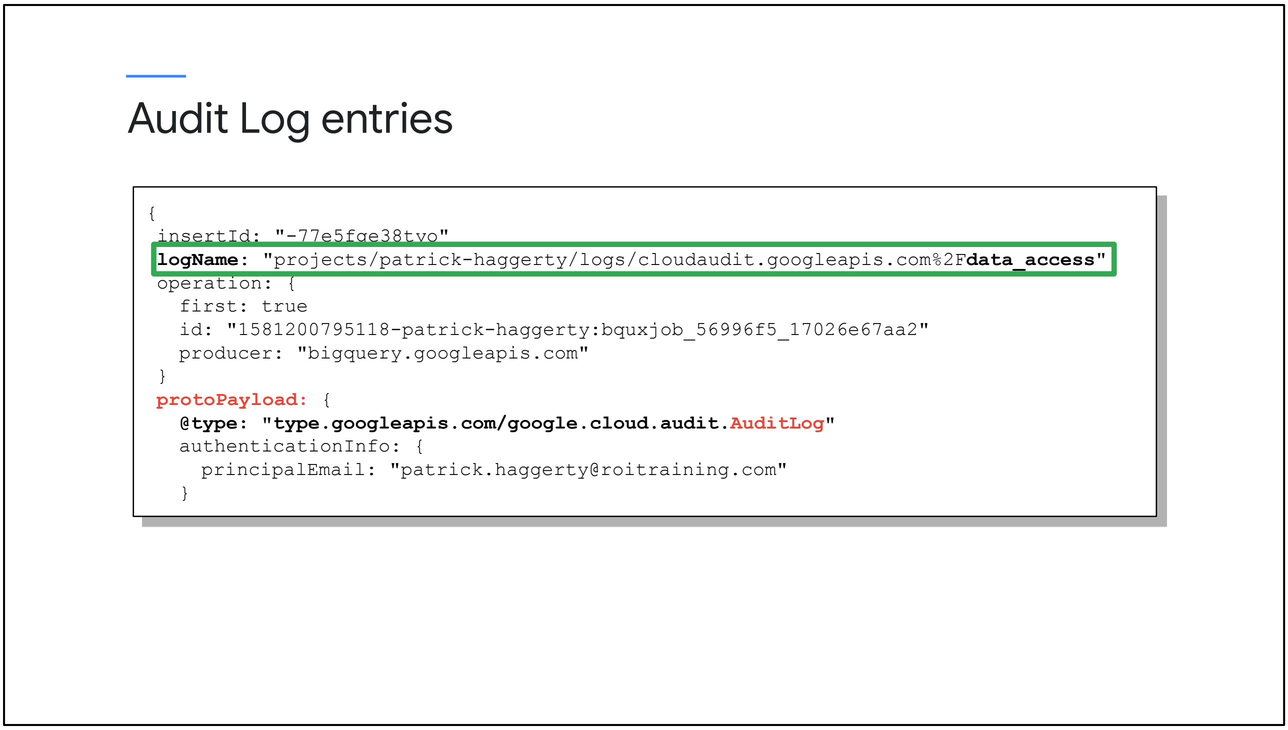
Now that we can enable the logs we need, let’s examine the logging entries themselves.

Audit Log entries

```
{
 insertId: "-77e5fge38tyo"
 logName: "projects/patrick-haggerty/logs/cloudaudit.googleapis.com%2Fdata_access"
 operation: {
   first: true
   id: "1581200795118-patrick-haggerty:bquxjob_56996f5_17026e67aa2"
   producer: "bigquery.googleapis.com"
 }
 protoPayload: {
   @type: "type.googleapis.com/google.cloud.audit.AuditLog"
   authenticationInfo: {
     principalEmail: "patrick.haggerty@roitraining.com"
   }
```

Every audit log entry in Cloud Logging is an object of type LogEntry.

What distinguishes an audit log entry from other log entries is the protoPayload field, which contains an AuditLog object that stores the audit logging data.

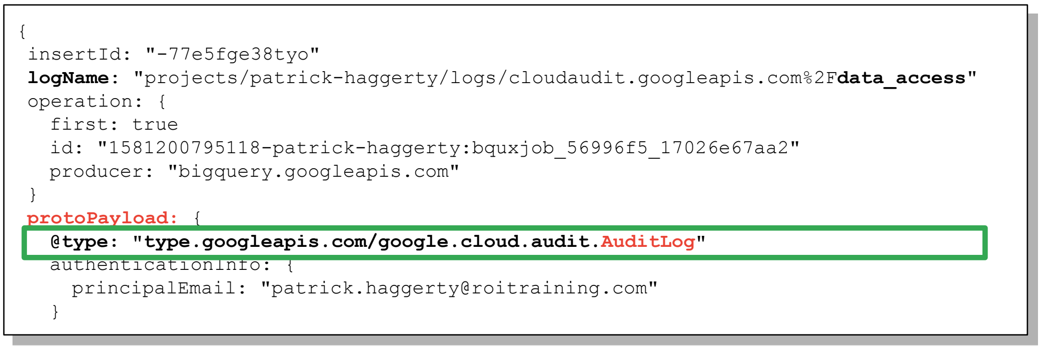


Audit Log entries

```
{
 insertId: "-77e5fqe38tvo"
 logName: "projects/patrick-haggerty/logs/cloudaudit.googleapis.com%2Fdata_access"
 operation: {
   first: true
   id: "1581200795118-patrick-haggerty:bquxjob_56996f5_17026e67aa2"
   producer: "bigquery.googleapis.com"
 }
 protoPayload: {
   @type: "type.googleapis.com/google.cloud.audit.AuditLog"
   authenticationInfo: {
     principalEmail: "patrick.haggerty@roitraining.com"
   }
```

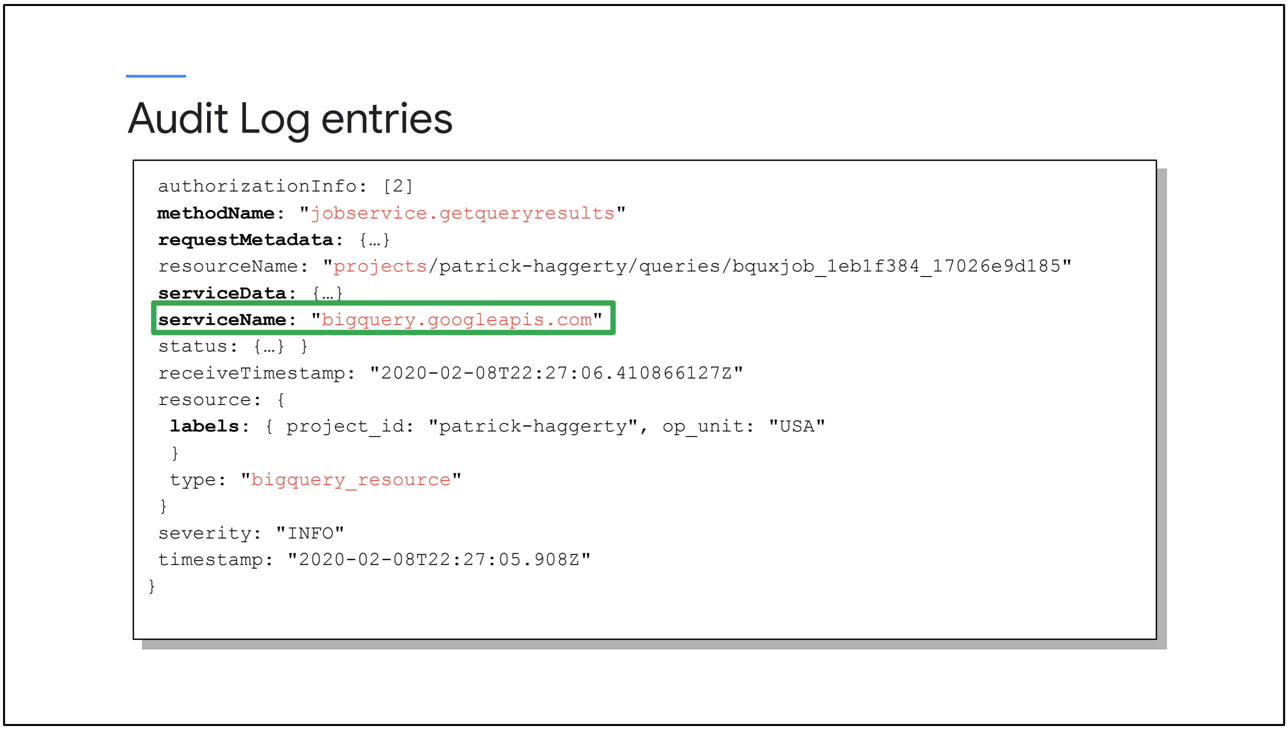
Here, note the log name. This tells us that we're looking at an example from the data access log.

Audit Log entries



```
{
 insertId: "-77e5fge38tyo"
 logName: "projects/patrick-haggerty/logs/cloudaudit.googleapis.com%2Fdata_access"
 operation: {
   first: true
   id: "1581200795118-patrick-haggerty:bquxjob_56996f5_17026e67aa2"
   producer: "bigquery.googleapis.com"
 }
 protoPayload: {
   @type: "type.googleapis.com/google.cloud.audit.AuditLog"
   authenticationInfo: {
     principalEmail: "patrick.haggerty@roitraining.com"
   }
```

Now, note the AuditLog type in the protoPayload.

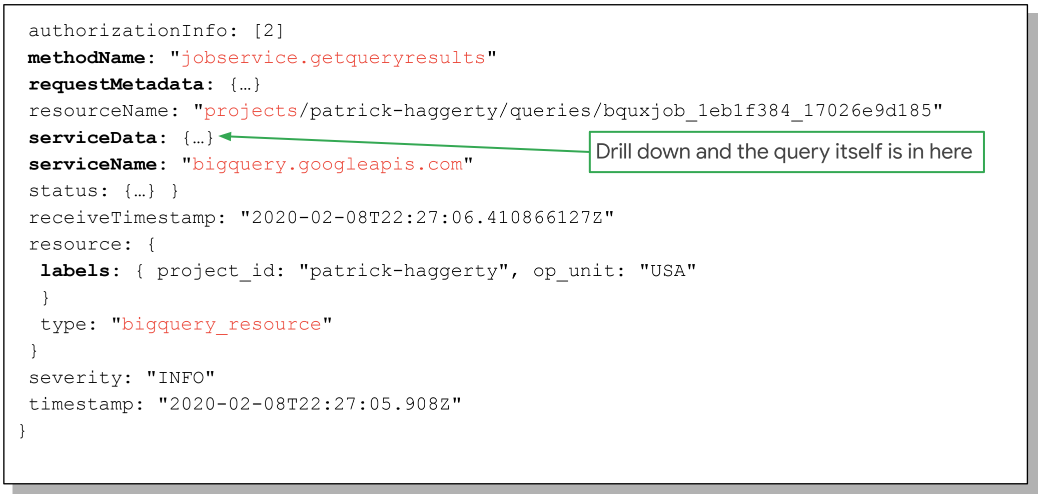


Audit Log entries

```
 authorizationInfo: [2]
 methodName: "jobservice.getqueryresults"
 requestMetadata: {…}
 resourceName: "projects/patrick-haggerty/queries/bquxjob_1eb1f384_17026e9d185"
 serviceData: {…}
 serviceName: "bigquery.googleapis.com"
 status: {…} }
 receiveTimestamp: "2020-02-08T22:27:06.410866127Z"
 resource: {
  labels: { project_id: "patrick-haggerty", op_unit: "USA"
  }
  type: "bigquery_resource"
 }
 severity: "INFO"
 timestamp: "2020-02-08T22:27:05.908Z"
}
```

Google has a standard List of official service names. You can use this list as a handy reference.

Audit Log entries



```
 authorizationInfo: [2]
 methodName: "jobservice.getqueryresults"
 requestMetadata: {…}
 resourceName: "projects/patrick-haggerty/queries/bquxjob_1eb1f384_17026e9d185"
 serviceData: {…}
 serviceName: "bigquery.googleapis.com"
 status: {…} }
 receiveTimestamp: "2020-02-08T22:27:06.410866127Z"
 resource: {
  labels: { project_id: "patrick-haggerty", op_unit: "USA"
  }
  type: "bigquery_resource"
 }
 severity: "INFO"
 timestamp: "2020-02-08T22:27:05.908Z"
}
```

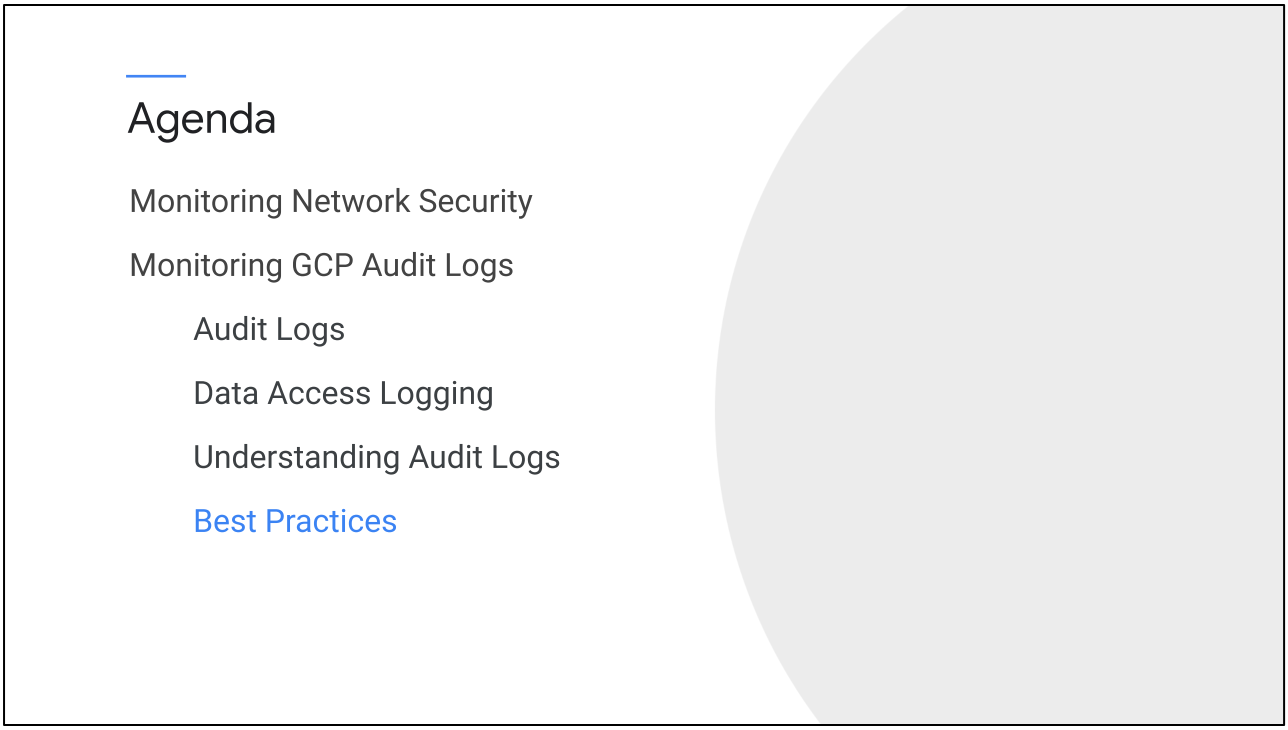
Drill down and the query itself is in here

In this slide, you can tell we're looking at a query that was run in BigQuery.

If you expanded the serviceData field, you could actually see the query itself.

So, when someone at your organization runs that unexpected, $40,000 query, you can figure out who and what the query was.

Then you can go learn more about price controls and BigQuery :-).



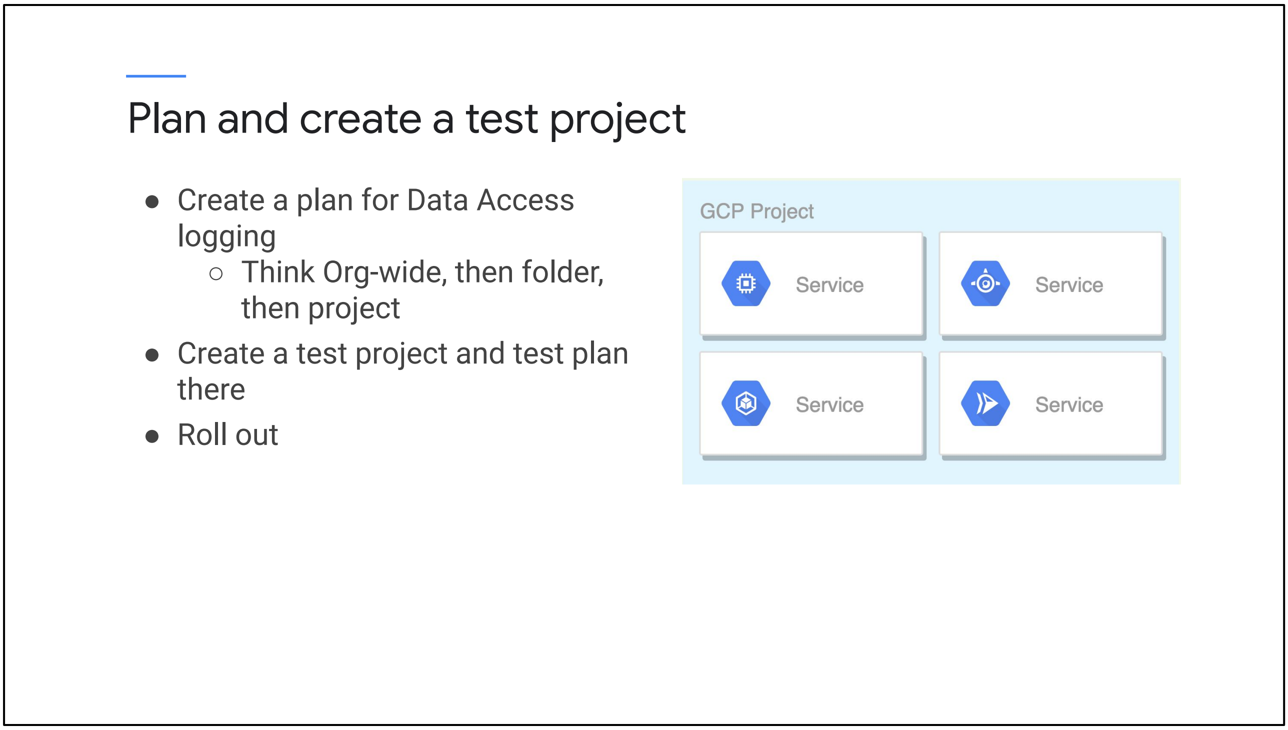
Agenda

Monitoring Network Security

Monitoring GCP Audit Logs

- Audit Logs
- Data Access Logging
- Understanding Audit Logs
- Best Practices

Let’s go over a few best practices before we wrap up this module.



Plan and create a test project

- Create a plan for Data Access logging
  - Think Org-wide, then folder, then project
- Create a test project and test plan there
- Roll out

GCP Project

Service

Service

Service

Service

Plan, Plan, Plan.

Like anything in the cloud, start by planning first.

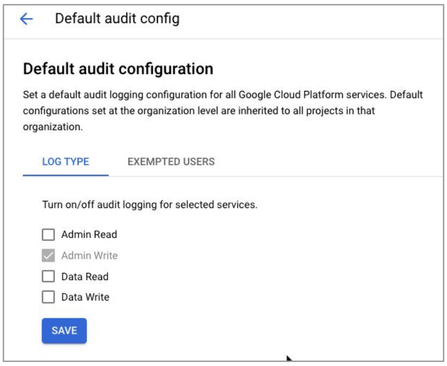
Spend time and create a solid plan for Data Access logs. Think organization, folder, then project. Like most organizations, some of your projects will be very specialized, but usually, they do break down into common organizational types.

Then, create a test project and experiment to see if the logging works the way you expect.

Then roll out, and don't forget automation (Infrastructure as Code, coming soon).

Decide and set org level data access

- Pro: detailed information on exactly who, accessed/edited/deleted what, and when
  - Free tier
  - Some logs always free
- Con: logs can be quite large
  - $0.50/GiB



Default audit configuration

Set a default audit logging configuration for all Google Cloud Platform services. Default configurations set at the organization level are inherited to all projects in that organization.

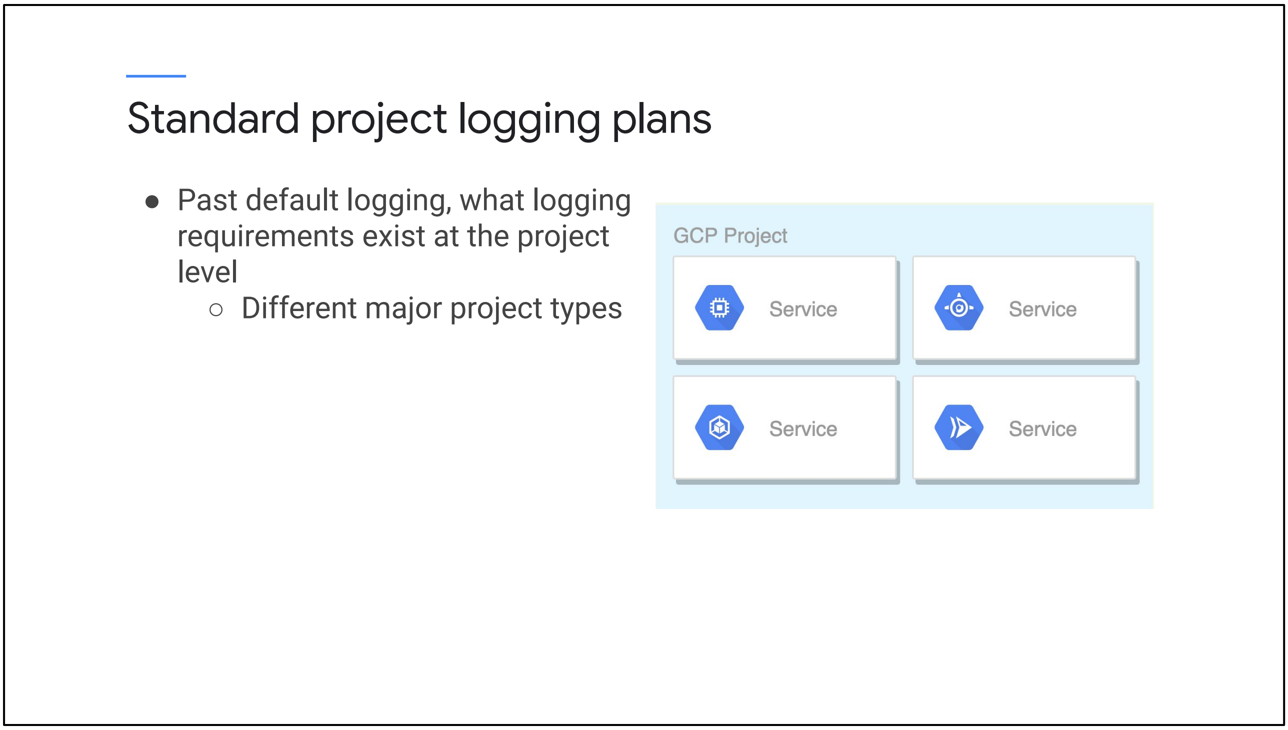
Turn on/off audit logging for selected services.

- ☐ Admin Read
- ☑ Admin Write
- ☐ Data Read
- ☐ Data Write

Remember that Data Access logs can be enabled as high as the organization.

The pro would be a lot of very detailed information on exactly who accessed, edited, and deleted what, and when.

The con is that Data Access logs can grow to be quite large, and are billed at $.50 a gig.

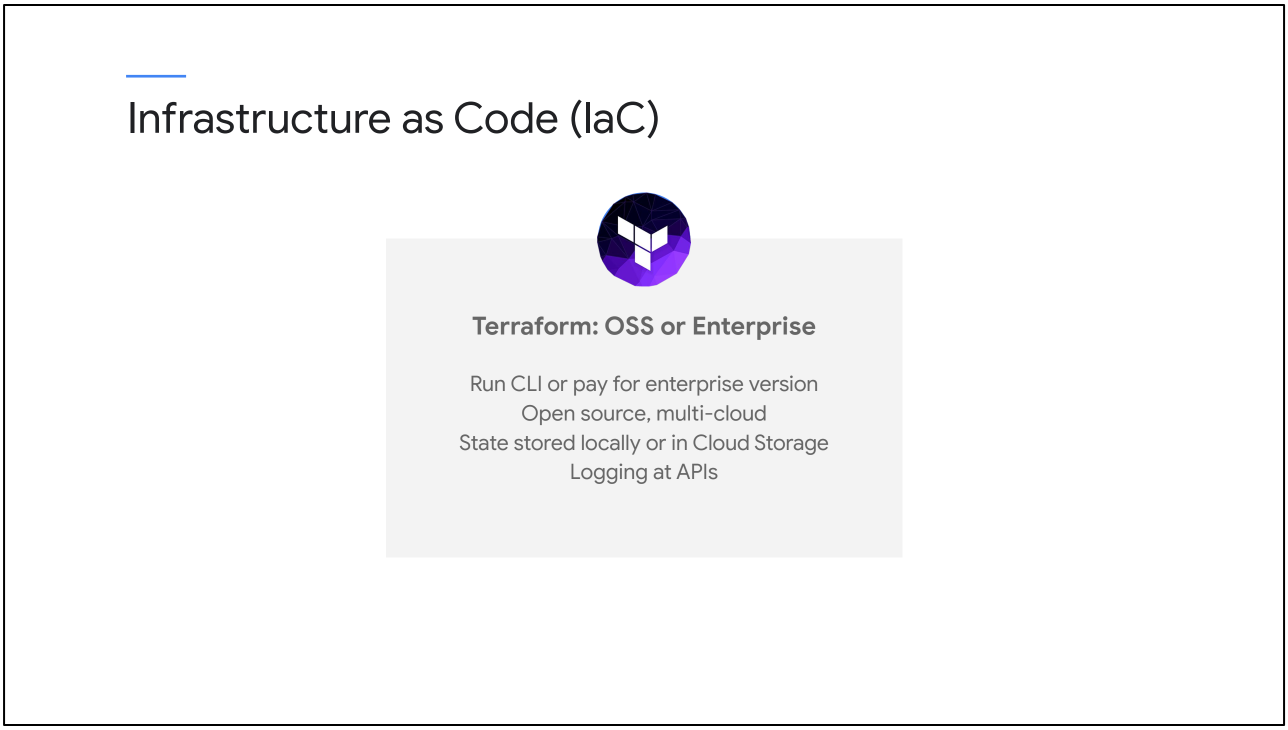


Standard project logging plans

- Past default logging, what logging requirements exist at the project level
  - Different major project types

GCP Project
Service
Service
Service
Service

Outside of whatever default logging you institute, every project needs to be analyzed for specialized logging requirements.



Infrastructure as Code (IaC)

Terraform: OSS or Enterprise

Run CLI or pay for enterprise version
Open source, multi-cloud
State stored locally or in Cloud Storage
Logging at APIs

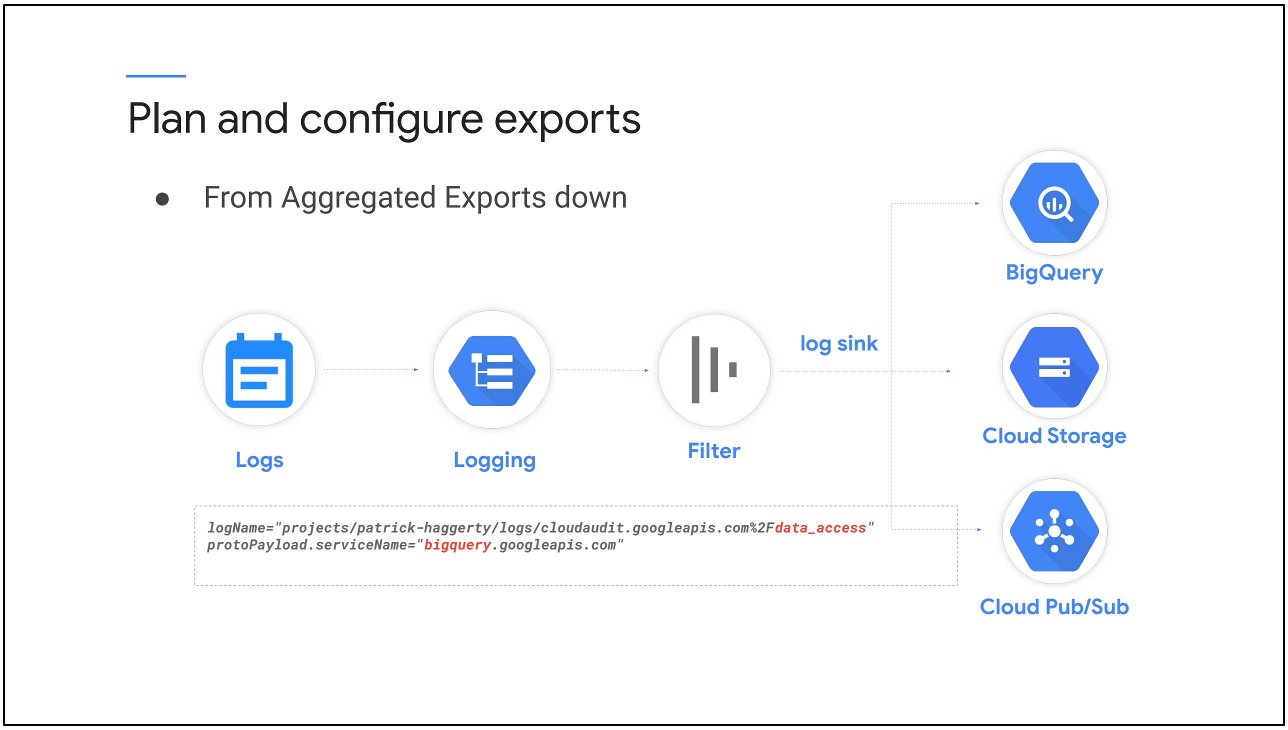
Infrastructure as Code (IaC) is essentially the process of automating the creation and modifications to your infrastructure using a platform that supports configuration files, which can be put through a CI/CD pipeline, just the same as code.

Terraform is an open-source package from Hashicorp.

It isn't hosted directly in Google Cloud, though it is installed by default in Cloud Shell.

State management is a decision point for your organization.

Options include using Cloud Storage, using a Git repo like GitHub, setting up something local to your organization, or using Hashicorp's pay Enterprise service.



Plan and configure exports

- From Aggregated Exports down

```
logName="projects/patrick-haggerty/logs/cloudaudit.googleapis.com%2Fdata_access"
protoPayload.serviceName="bigquery.googleapis.com"
```

We've discussed the options and benefits of exporting logs. Again, make this part of your plan.

Start by deciding what, if anything, you will export from Aggregated Exports at the organization level.

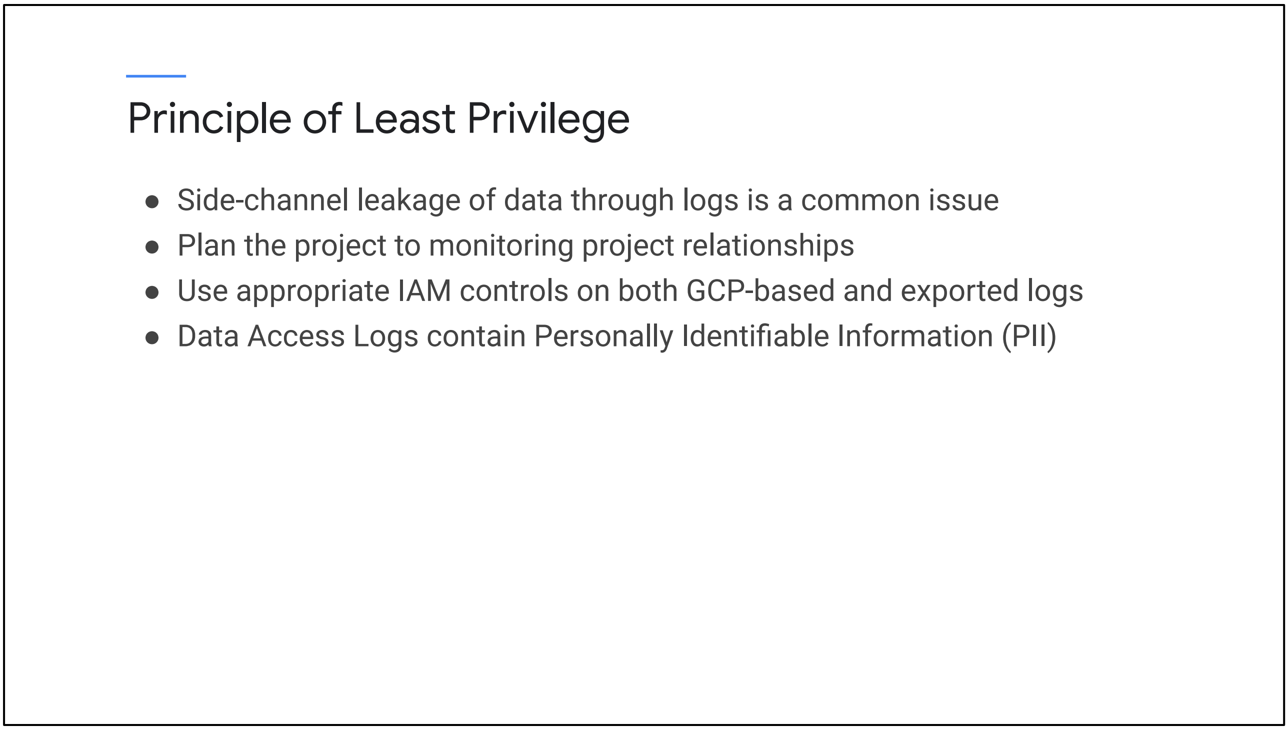
Then decide what options you will use, project by project, folder by folder, etc.

Then, carefully consider your filters - both what they leave in, and what they leave out.

This applies to all logging, not just to exports.

Lastly, carefully consider what, if anything, you will fully exclude from logging.

Remember that **excluded entries will be gone forever.**



Principle of Least Privilege

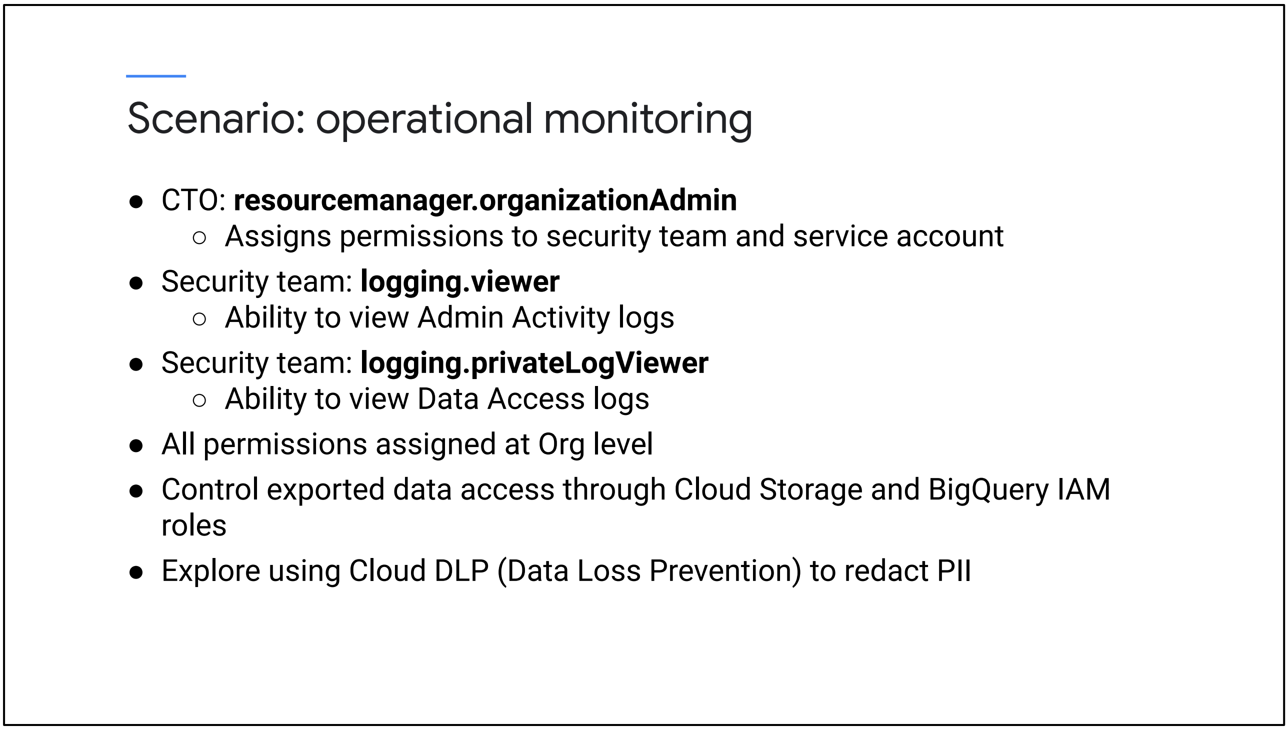
- Side-channel leakage of data through logs is a common issue
- Plan the project to monitoring project relationships
- Use appropriate IAM controls on both GCP-based and exported logs
- Data Access Logs contain Personally Identifiable Information (PII)

Side-channel leakage of data through logs is a common issue. You need to be careful who, gets what kind of access, to which logs.

Remember some of the discussions earlier in this course on monitoring workspaces and how a monitoring workspace can monitor the current project, or it can also monitor up to 100 other projects?
That's where your security starts. Are you monitoring project by project, or are you selectively grouping work projects into higher-level monitored projects?

Use appropriate IAM controls on both Google Cloud-based and exported logs, only allowing the minimal access required to get the job done.

Especially scrutinize the Data Access Log permissions, as they will often contain Personally Identifiable Information (PII)



Scenario: operational monitoring

- CTO: **resourcemanager.organizationAdmin**
  - Assigns permissions to security team and service account
- Security team: **logging.viewer**
  - Ability to view Admin Activity logs
- Security team: **logging.privateLogViewer**
  - Ability to view Data Access logs
- All permissions assigned at Org level
- Control exported data access through Cloud Storage and BigQuery IAM roles
- Explore using Cloud DLP (Data Loss Prevention) to redact PII

Lastly, let's look at a few access scenarios, starting with operational monitoring.

These scenarios illustrate a typical high-level team and their assignments.

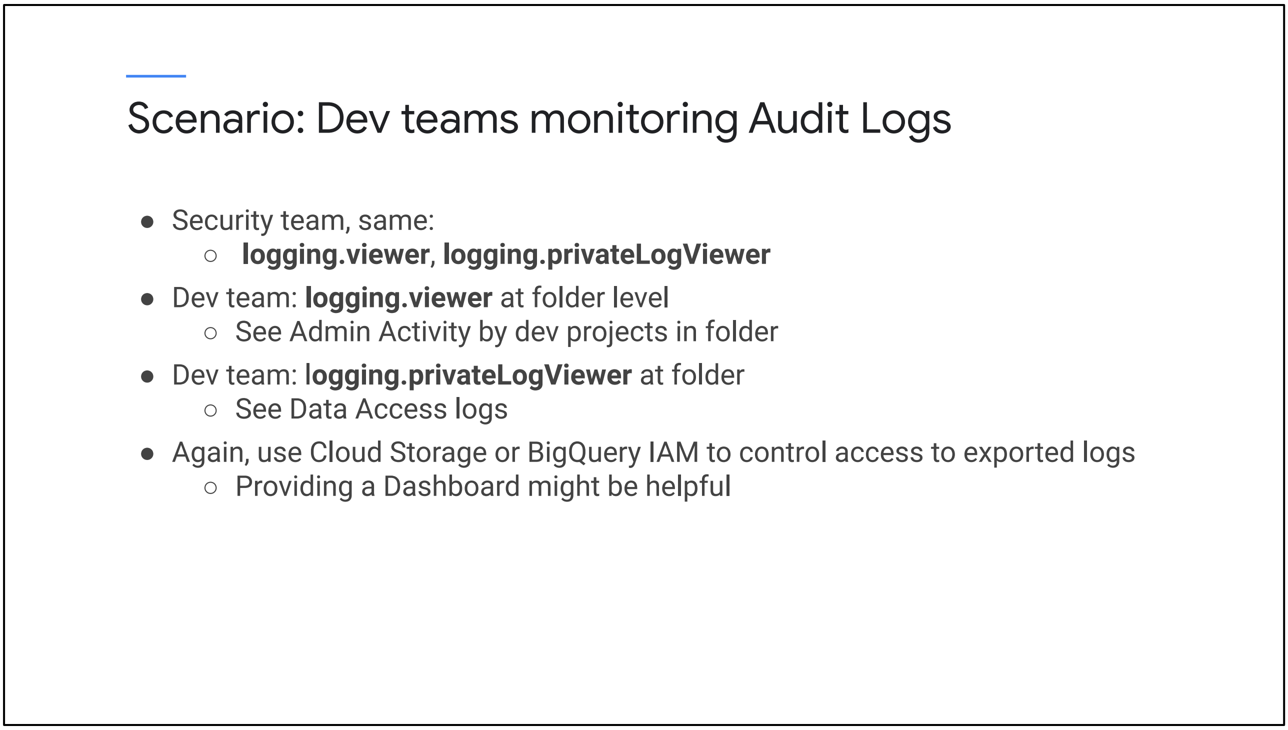
For example: The CTO has high level resourcemanager.organizationAdmin privileges, so he/she can assign permissions to the security team and service accounts.

The CTO can then give the security team logging.viewer permissions so that they may view the Admin Activity logs, and logging.privateLogViewer permissions, so they may view the Data Access logs.

These permissions would be assigned at the organization level, so they would be global in scope.

Access control to data exported to Cloud Storage or BigQuery will be controlled selectively with IAM.

You might also want to explore using Google's Cloud Data Loss Prevention API to redact PII from files and images.



Scenario: Dev teams monitoring Audit Logs

- Security team, same:
  - **logging.viewer**, **logging.privateLogViewer**
- Dev team: **logging.viewer** at folder level
  - See Admin Activity by dev projects in folder
- Dev team: l**ogging.privateLogViewer** at folder
  - See Data Access logs
- Again, use Cloud Storage or BigQuery IAM to control access to exported logs
  - Providing a Dashboard might be helpful

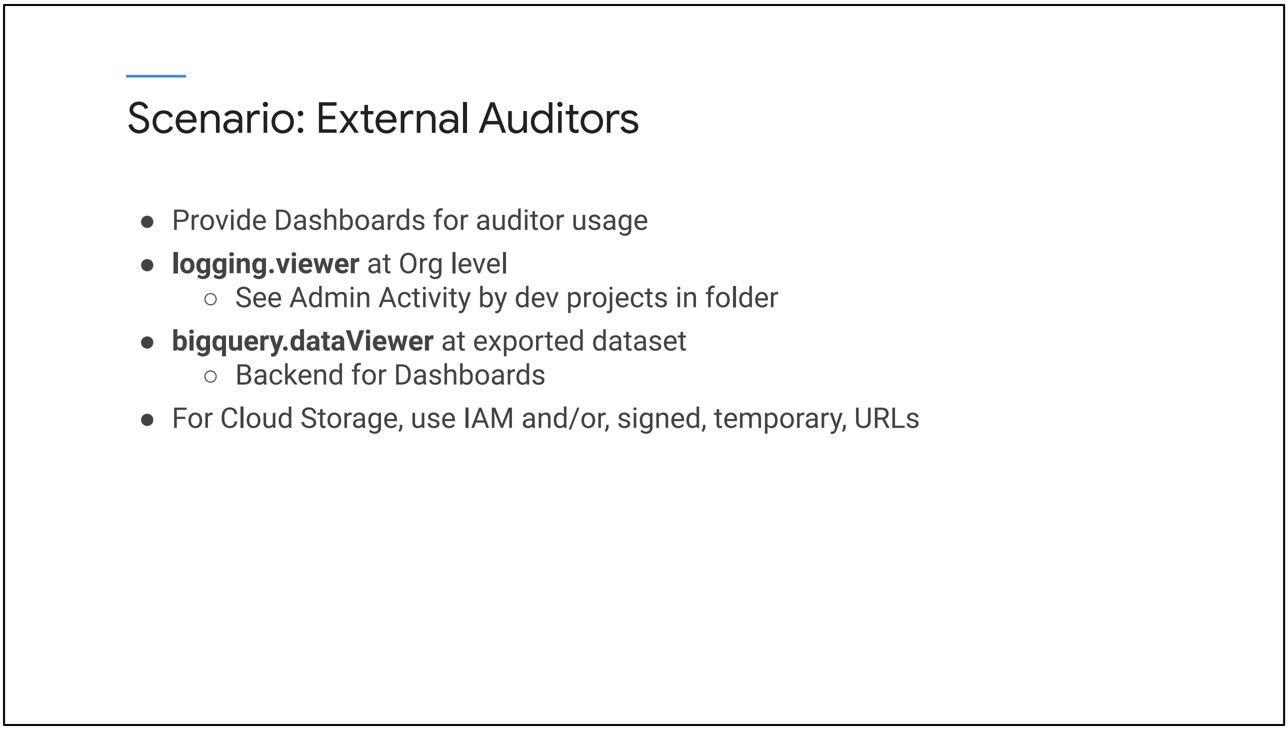
Now let's move on to development teams.

The security team is unchanged from the last slide. They already have logging.viewer, and logging.privateLogViewer from the global assignment.

The dev team might get logging.viewer at the folder level so they can see the Admin Activity logs for the projects under their development control.

They probably also need logging.privateLogViewer at the dev folder so they can see the Data Access logs. Limit data they test with though, so they aren't viewing actual customer information.

Again, use Cloud Storage or BigQuery IAM to control access to exported logs. Prebuilding dashboards might also be a good option.



Scenario: External Auditors

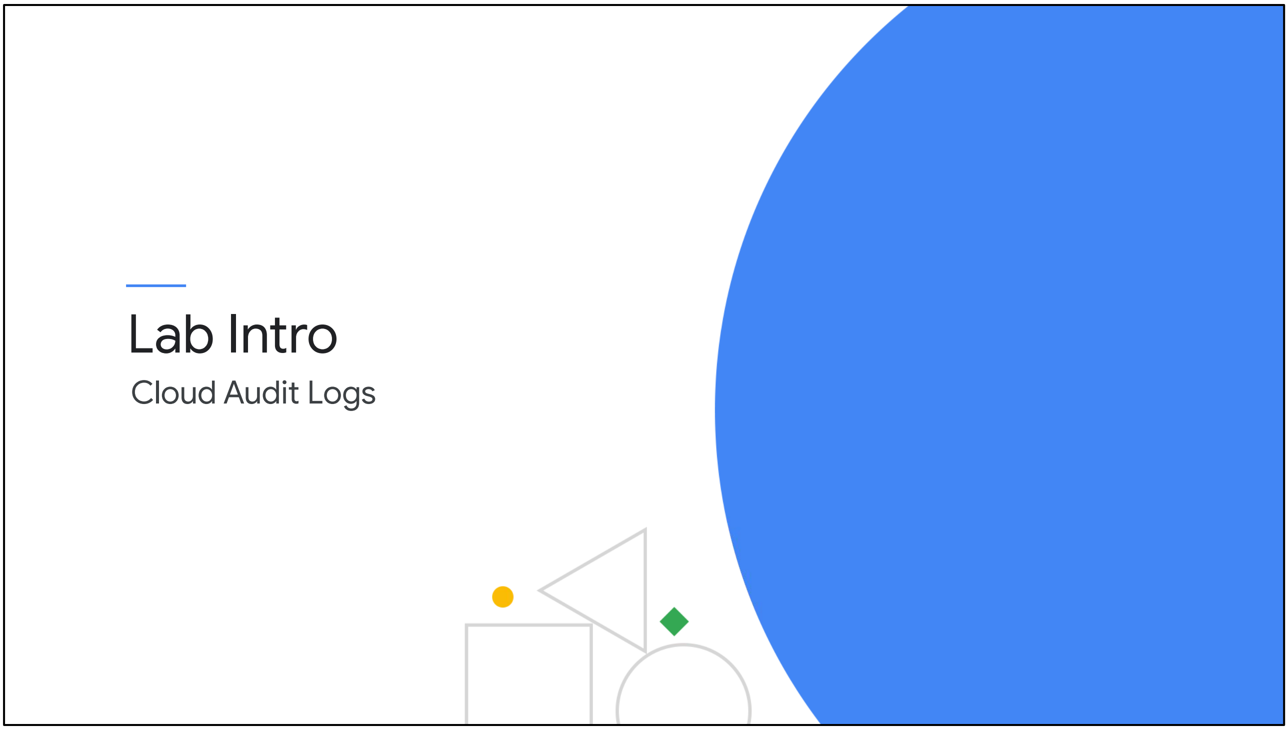
- Provide Dashboards for auditor usage
- **logging.viewer** at Org level
  - See Admin Activity by dev projects in folder
- **bigquery.dataViewer** at exported dataset
  - Backend for Dashboards
- For Cloud Storage, use IAM and/or, signed, temporary, URLs

For external auditors, provide pre-created dashboards where possible.

If they need broad access, you might make them logging.viewer at the org level.

For BigQuery, they could be bigquery.dataViewer on the exported dataset.

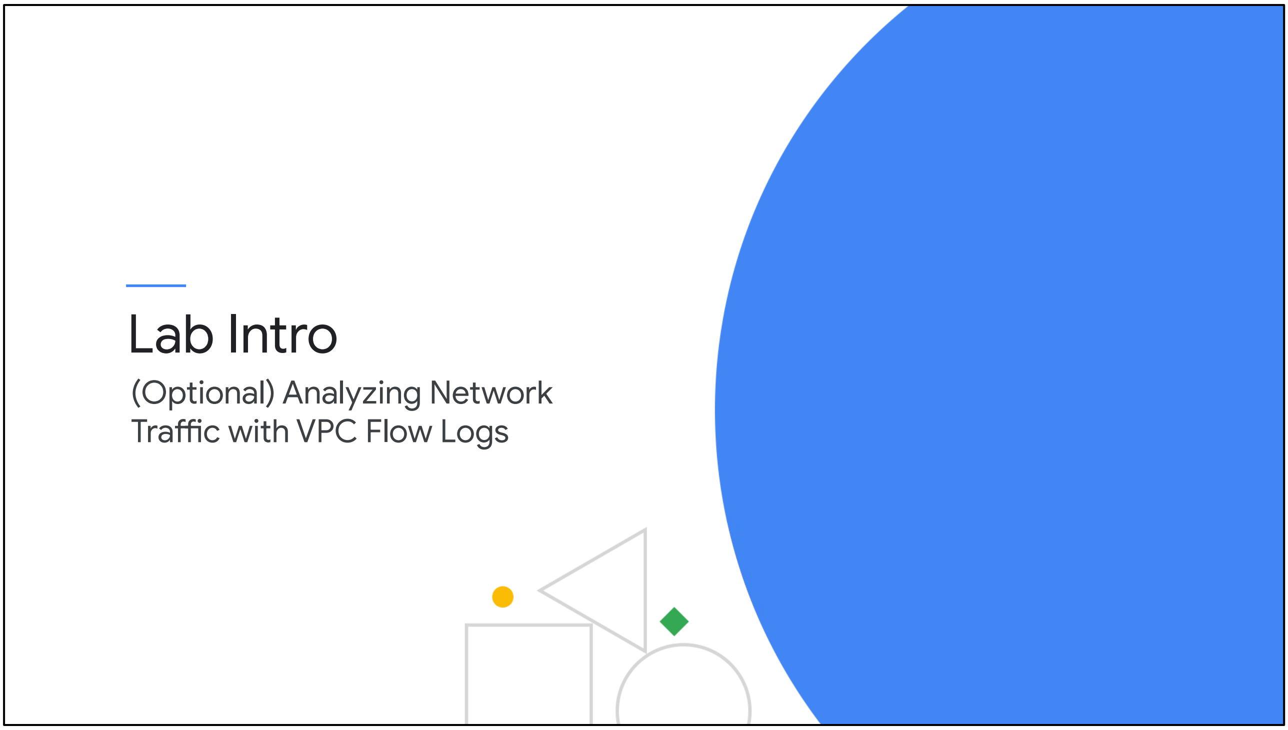
For Cloud Storage, again, you could use IAM, but also remember the temporary access URLs that Cloud Storage supports.



Lab Intro

Cloud Audit Logs

In this lab, you investigate Google Cloud Audit Logging. Cloud Audit Logging maintains multiple audit logs for each project, folder, and organization: Admin Activity tracks changes to Google cloud configurations and metadata. Data Access is more directly related to who accessed what data, and when.



Lab Intro

(Optional) Analyzing Network Traffic with VPC Flow Logs

In this lab, you configure a network to record traffic to and from an Apache web server using VPC Flow Logs. You then export the logs to BigQuery to analyze them.