Google Cloud

Partner Certification Academy

Professional Cloud Network Engineer

The information in this presentation is classified:

Google confidential & proprietary

⚠️ This presentation is shared with you under NDA.

- Do **not** record or take screenshots of this presentation.
- Do **not** share or otherwise distribute the information in this presentation with anyone **inside** or **outside** of your organization.

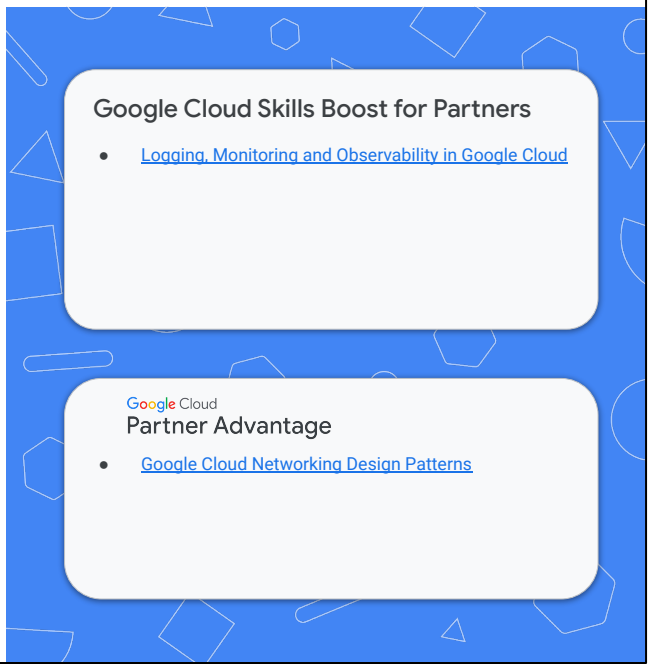
Thank you!

Google Cloud

Source Materials

Some of this program's content has been sourced from the following resources:

- Google Cloud certification site
- Google Cloud documentation
- Google Cloud console
- Google Cloud courses and workshops
- Google Cloud white papers
- Google Cloud Blog
- Google Cloud YouTube channel
- Google Cloud partner-exclusive resources



Session logistics

Questions

In Google Meet, click the raise hand button or add your question to the Q&A section.

Answers may be deferred until the end of the session.

Slide availability

These slides are available in the Student Lecture section of your Qwiklabs classroom.

Recording

The session is **not** recorded.

Chat

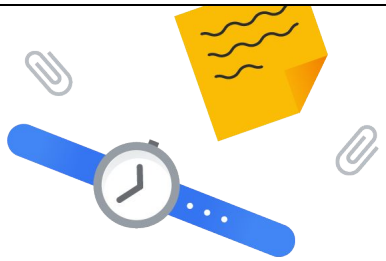
As Google Meet does not have persistent chat, you will lose chat history if you get disconnected. Save URLs as they appear.

When you have a question, please:
Click the Raise hand button in Google Meet.
Or add your question to the Q&A section of Google Meet.
Please note that answers may be deferred until the end of the session.

These slides are available in the Student Lecture section of your Qwiklabs classroom.

The session is not recorded.

Google Meet does not have persistent chat.
If you get disconnected, you will lose the chat history.
Please copy any important URLs to a local text file as they appear in the chat.



Today's agenda

01 Advanced Logging and Analysis

02 Monitoring Network Security and Audit Logs

03 Network Architecture Design Approach

04 Designing the VPC Architecture for the Workloads

05 Designing the Hybrid Connectivity

06 Hybrid Connectivity to a Single VPC (for Shared VPC)

Objectives

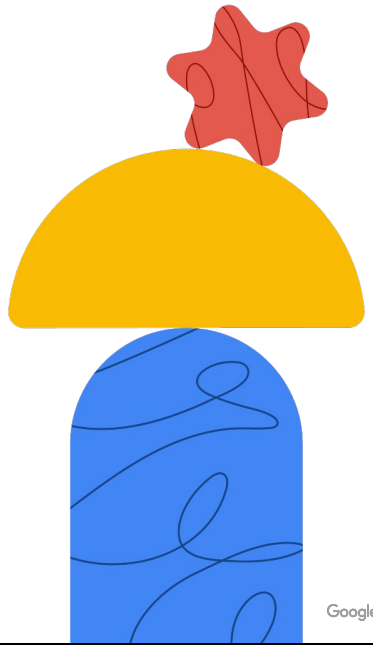
01 Explain network-related monitoring.

02 Explain network-related logging.

03 Describe network design approach.

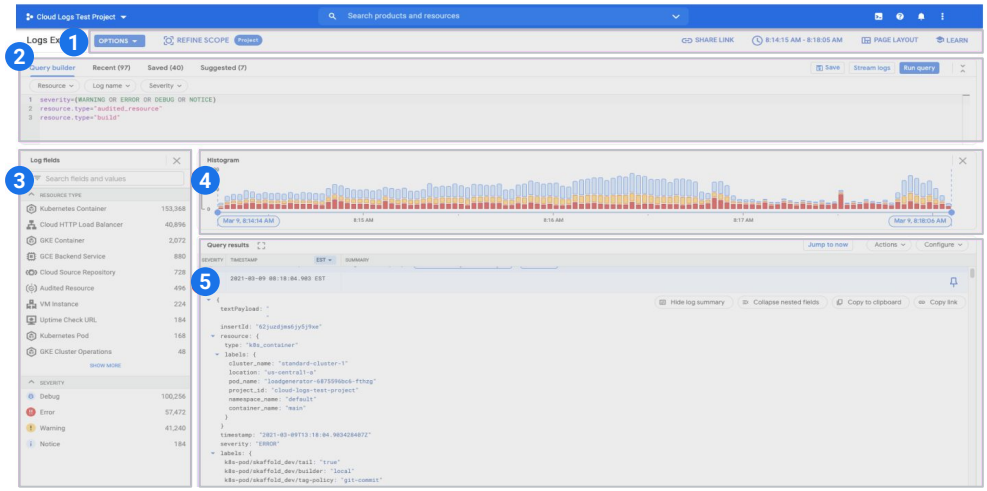
AGENDA

Advanced Logging and Analysis



n this module, you'll examine some of Google Cloud's advanced logging and analysis capabilities.

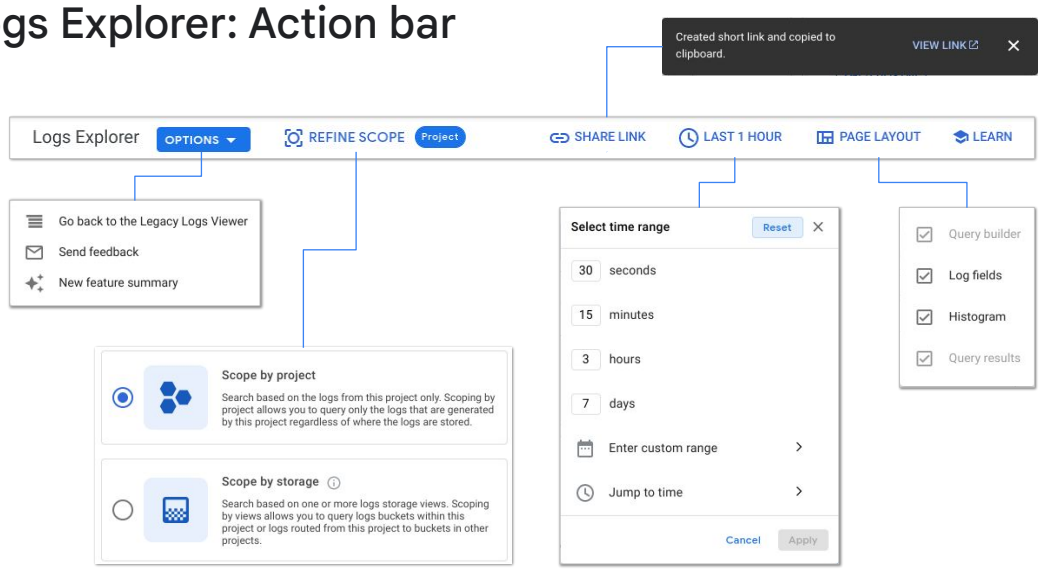
Logs Explorer interface



The Logs Explorer interface lets you retrieve logs, parse and analyze log data, and refine your query parameters. The Logs Explorer contains the following panes:

1. Action bar
2. Query builder
3. Log fields
4. Histogram
5. Query results

Logs Explorer: Action bar



From the **Action bar** pane, you can access the following:

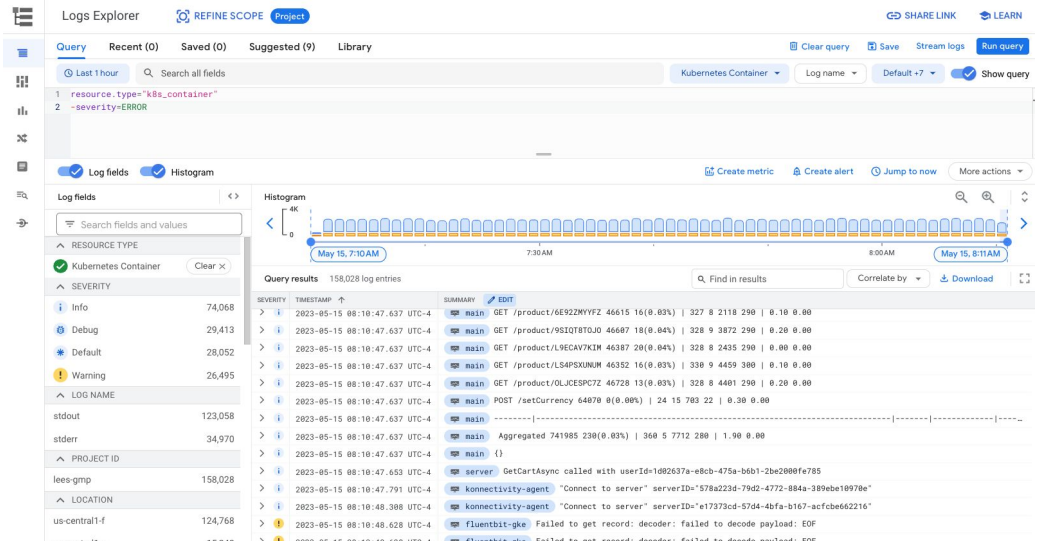
1. **Options**: Lets you go to the Legacy Logs Viewer, send feedback, and view a summary of new Logging features.
2. **Refine scope**: Lets you scope your search by logs in your current Cloud project only or by one or more storage views. For more information, see Refining scope.
3. **Share link**: Lets you create a shortened URL of the current query and copies it to your clipboard, making it easier to share a query.
4. **Time-range selector**: Lets you restrict query results by time range. The default time range is one hour.
5. **Page layout**: Lets you enable and disable the **Histogram** and **Logs field explorer** panes.
6. **Learn**: Lets you view links to relevant documentation.

Logs Explorer: Query builder

From the **Query builder** pane,you can access the following:

1. **Query-builder field**: Lets you build queries using the Logging query language.
2. **Query builder drop-down menus**: Lets you add query expressions based on **Resource**, **Log name**, and **Severity**. For more information, see Query builder drop-down menus.
3. **Recent**: Lets you view your recent queries. For more information, see Recent queries.
4. **Saved**: Lets you view your saved queries and queries that other users of the Cloud project have shared with you. For more information, see Saved queries and Shared queries.
5. **Suggested**: Lets you view suggested queries based on the resources in your Cloud project. For more information, see Suggested queries.
6. **Save**: Lets you save queries that can be viewed and run from the **Saved** tab.
7. **Stream logs**: Lets you view log entries as Logging ingests them. For more information, see Streaming logs.
8. **Run query**: Lets you run your queries after you have built them in the query-builder field.

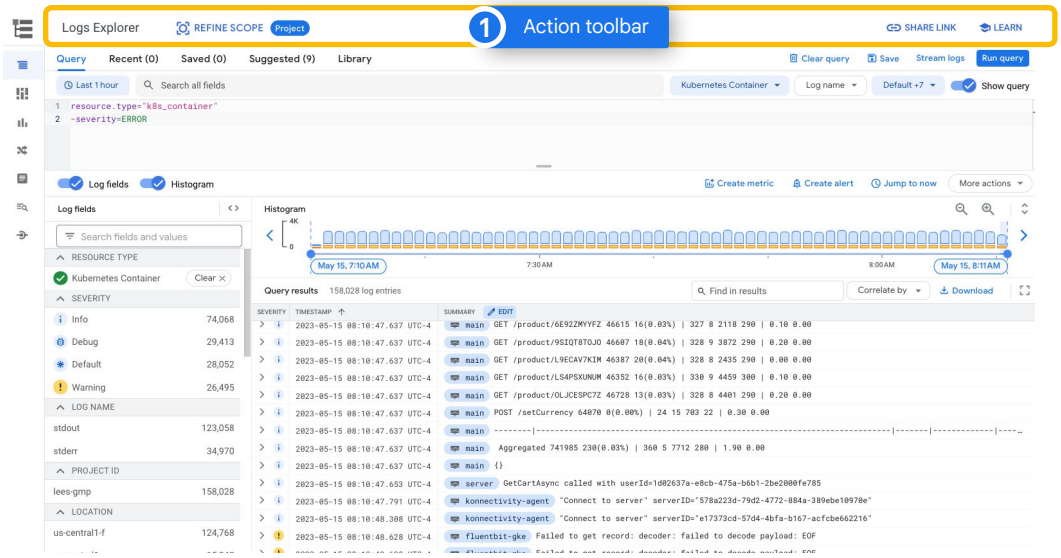
Logs Explorer: Query results



Google Cloud

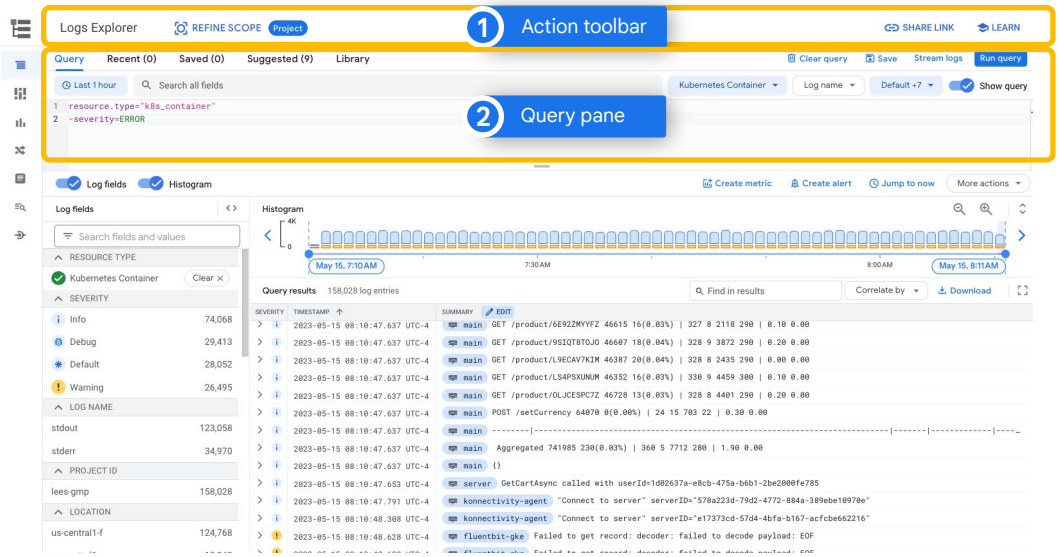
The Logs Explorer interface lets you retrieve logs, parse and analyze log data, and refine your query parameters. The Logs Explorer contains the following panes:

Logs Explorer: Query results



1. **Action toolbar:** Action toolbar to refine logs to projects or storage views, share a link and learn about logs explorer.

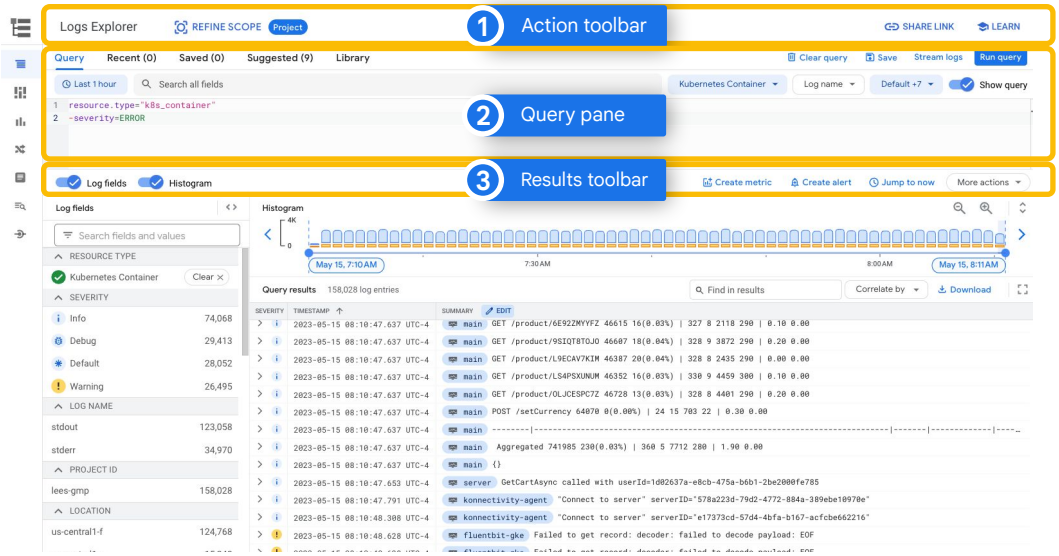
Logs Explorer: Query results



Google Cloud

2. **Query pane:** Query pane is where you can build queries, view recently viewed and saved queries and a lot more.

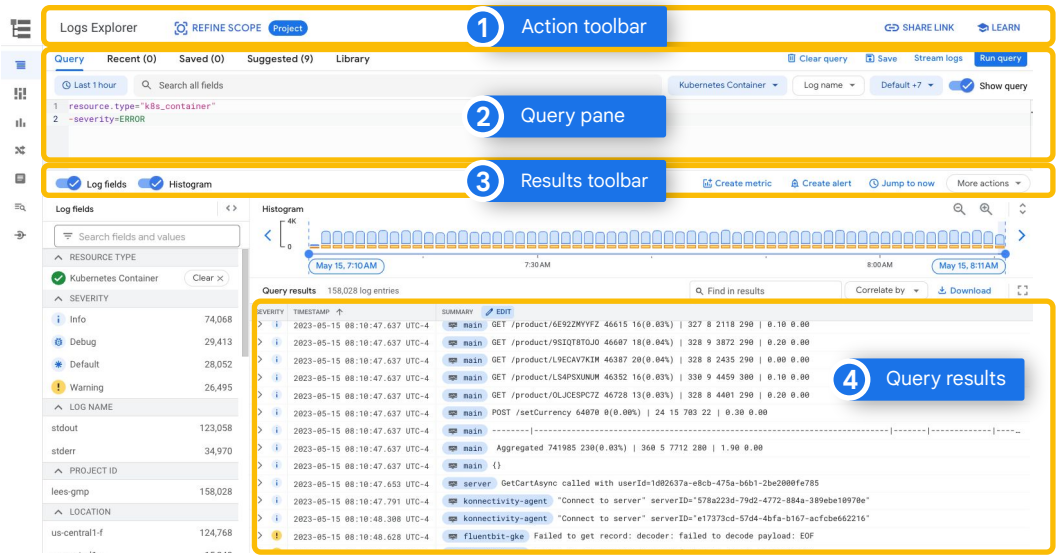
Logs Explorer: Query results



Google Cloud

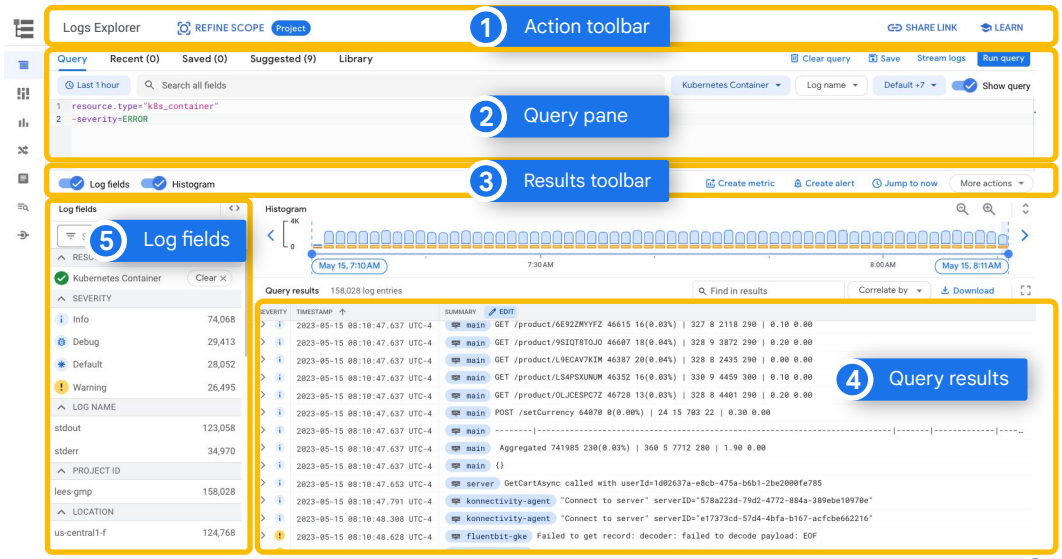
3. **Results Toolbar:** This can be used to quickly show or hide logs and histogram pane nad create a log based metric or alert. **Jump to now** option helps query and view the current time results.

Logs Explorer: Query results



4. **Query results:** Is the details of results with a summary and timestamp that helps troubleshoot further.

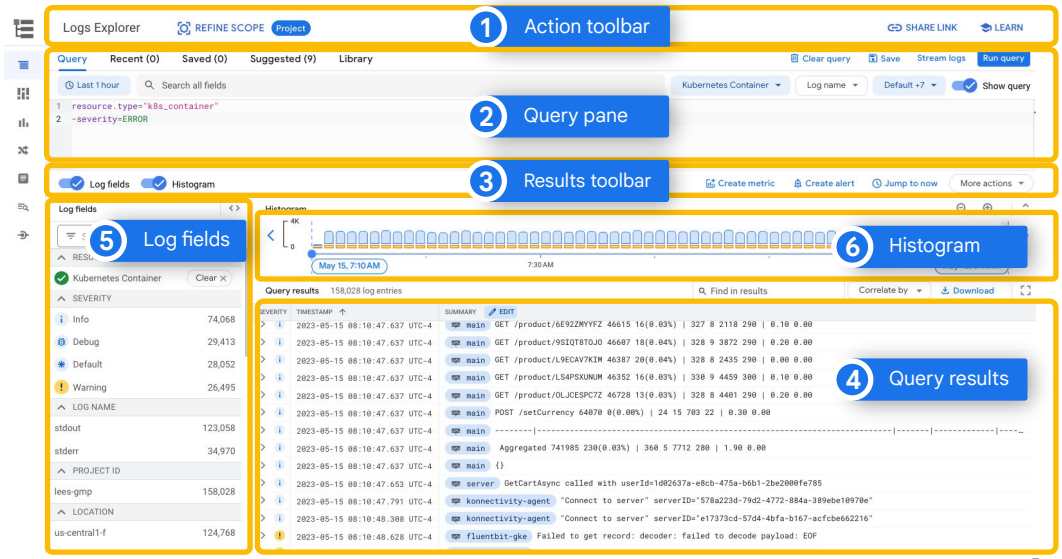
Logs Explorer: Query results



Google Cloud

5. **Log fields**: Log fields pane is used to filter your options based on various factors such as a resource type, log name, project ID, etc,.

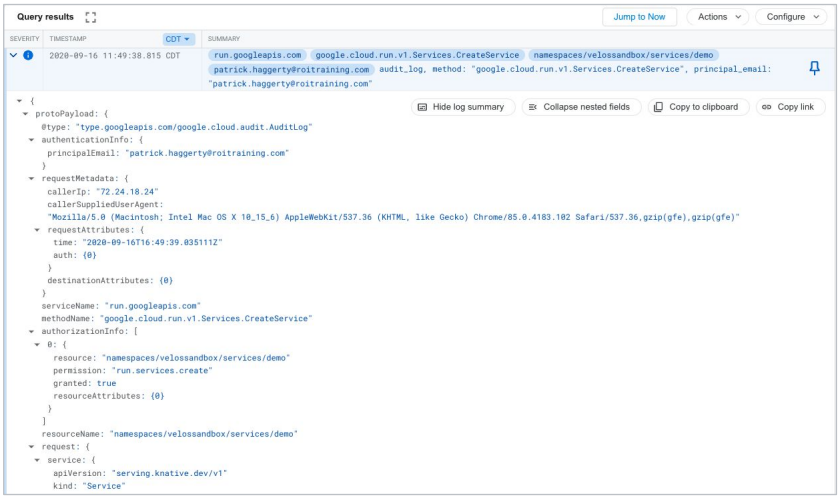
Logs Explorer: Query results



Google Cloud

6. **Histogram:** Histogram is where the query result is visualized a histogram bars, where each bar is a time range and is color coded based on severity.

Entries are returned as LogEntry objects



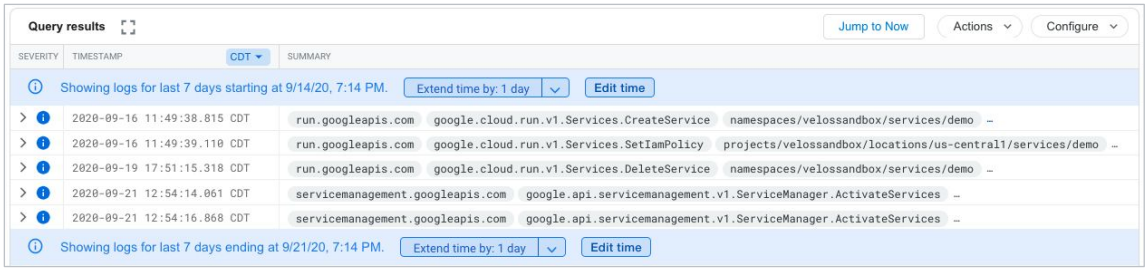
The entries returned in Logs Explorer are based on Google's LogEntry datatype. They contain data like the logName, severity, resource.type, and various payload fields.

Primary log fields

Field name	Description
logName	Resource name of the log to which this log entry belongs (ex: projects/[PROJECT_ID]/logs/[LOG_ID])
insertId	Unique identifier
severity	Entry severity, defaults to LogSeverity.DEFAULT
timestamp/receiveTimestamp	The time the event described by the log entry occurred/was received by Logging
resource.type	The name of a resource type. Example: gce_instance
resource.labels.KEY	The value associated with a resource label key
httpRequest.FIELD	The value of a field in an HttpRequest object (method, url, size, status, etc.)
labels.KEY	The value associated with a label key
operation.FIELD	The value of a field in a LogEntryOperation object
protoPayload.FIELD	Log entry payload represented as a protocol buffer
jsonPayload.FIELD	The value of a field within a JSON object
textPayload	The log entry payload, represented as a Unicode string (UTF-8)

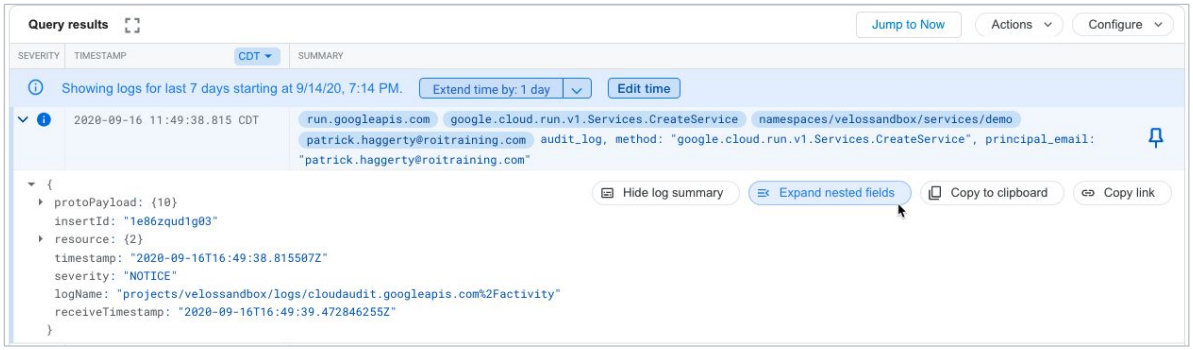
~~Here you see common~~ What is displayed now is common LogEntry properties. Note that *textPayload*, *jsonPayload*, and *textPayload* are mutually exclusive. Also, the information that is typically most interesting and/or most relevant will be found in the provided payload section.

Log entries



The log-entry table displays an entry line for each log entry. In the line, you see the entry severity, timestamp, and any values for fields that have been promoted to the summary.

Log entry details



To view the full details for one log entry, click the expander arrow (▸) at the front of the summary line, and then click **Expand nested fields**. The log entry is displayed using JSON format.

Locate (or hide) similar entries

You can click the value of a specific field in the expanded log entry view and then either show or hide all log entries with the same value. Doing so will modify the log query appropriately.

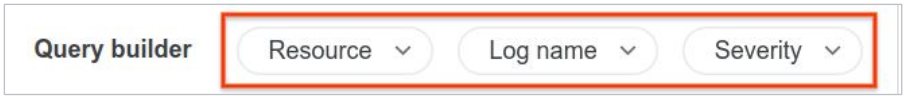
Ultimately, it's the query that selects the entries

- Start with what you know about the entry you're trying to find.
- If it belongs to a resource, a particular log file, or has a known severity, use the query builder drop-down menus.

Ultimately, it's the query that selects the entries displayed by Logs Explorer. Queries may be created directly with the Logging Query Language (LQL), using the drop-down menus, the logs field explorer, or by clicking fields in the results themselves.

Start with what you know about the entry you're trying to find. If it belongs to a resource, a particular log file, or has a known severity, use the query builder drop-down menus.

Using the query builder drop-down menu



The query builder drop-down menu makes it easy to start narrowing your log choices.

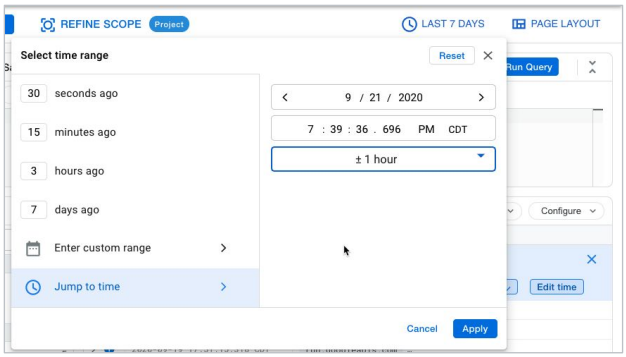
- **Resource**: Lets you specify resource.type. You can select a single resource at a time to add to the **Query builder**. Entries use the logical operator AND.
- **Log name**: Lets you specify logName. You can select multiple log names at once to add to the **Query builder**. When selecting multiple entries, the logical operator OR is used.
- **Severity**: Lets you specify severity. You can select multiple severity levels at once to add to the **Query builder**. When selecting multiple entries, the logical operator OR is used.

Advanced filter comparison operators

=	**Equals**	`resource.type="gce_instance"`
!=	**Does not equal**	`resource.labels.instance_id!="1234567890"`
<=	**Less than equal**	`timestamp <= "2018-08-13T20:00:00Z"`
>=	**More than equal**	`timestamp >= "2018-08-13T20:00:00Z"`
>	**More than**	`timestamp > "2018-08-13T20:00:00Z"`
<	**Less than**	`timestamp < "2018-08-13T20:00:00Z"`
:	**Has**	`textPayload:"GET /check"`

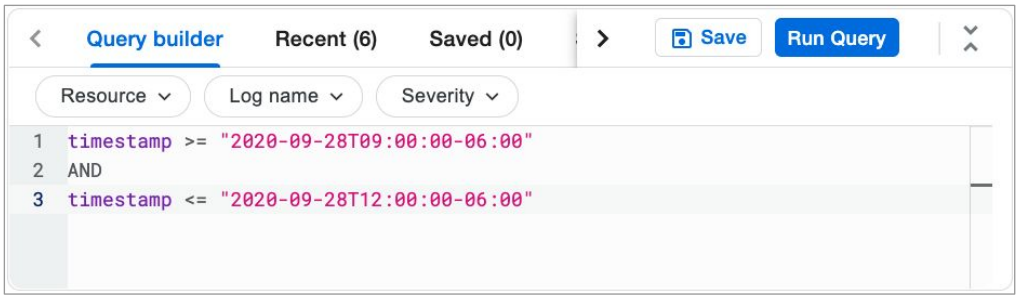
The next several slides are included for reference. Advanced queries support multiple comparison operators as seen here.

Finding log entries, set the time range

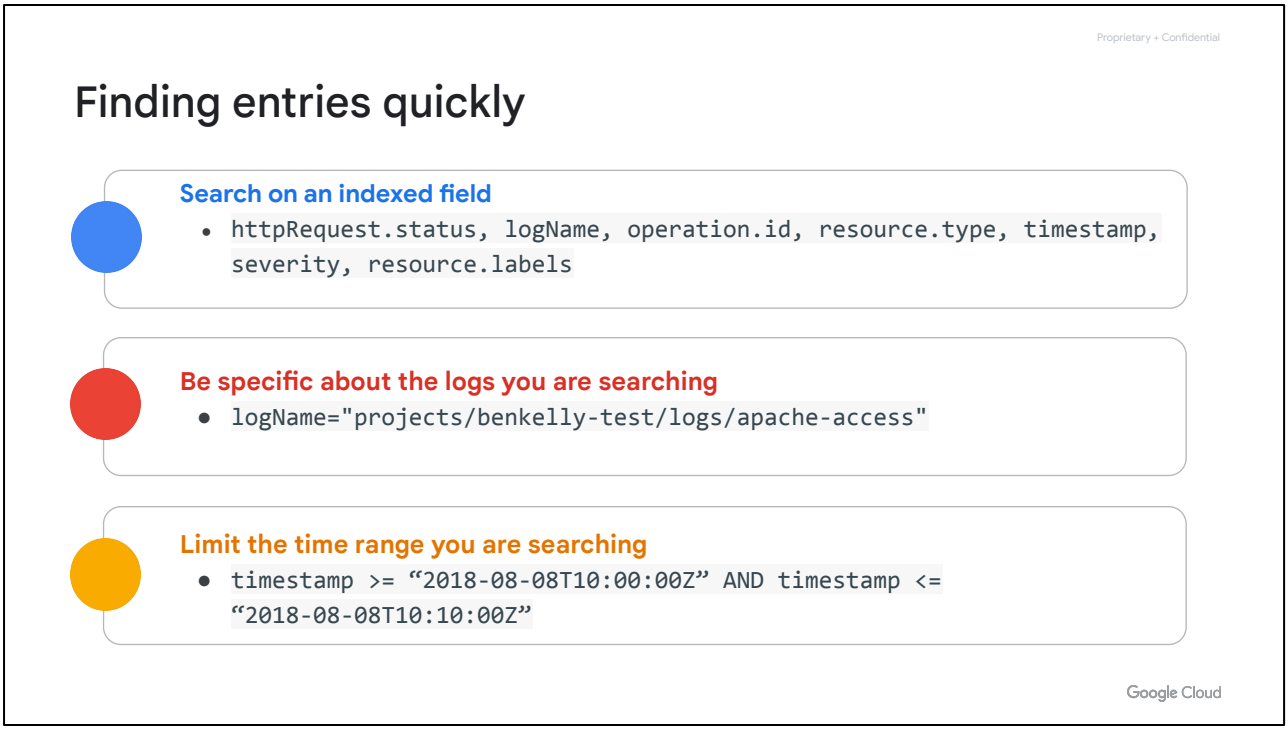


If you're looking for a specific set of log entries and have a rough idea when they would have been generated, start by narrowing to a specific time range. You can select one of the pre-created choices, set a custom range, or jump to a particular time +/- an amount.

You can also manually restrict the time range

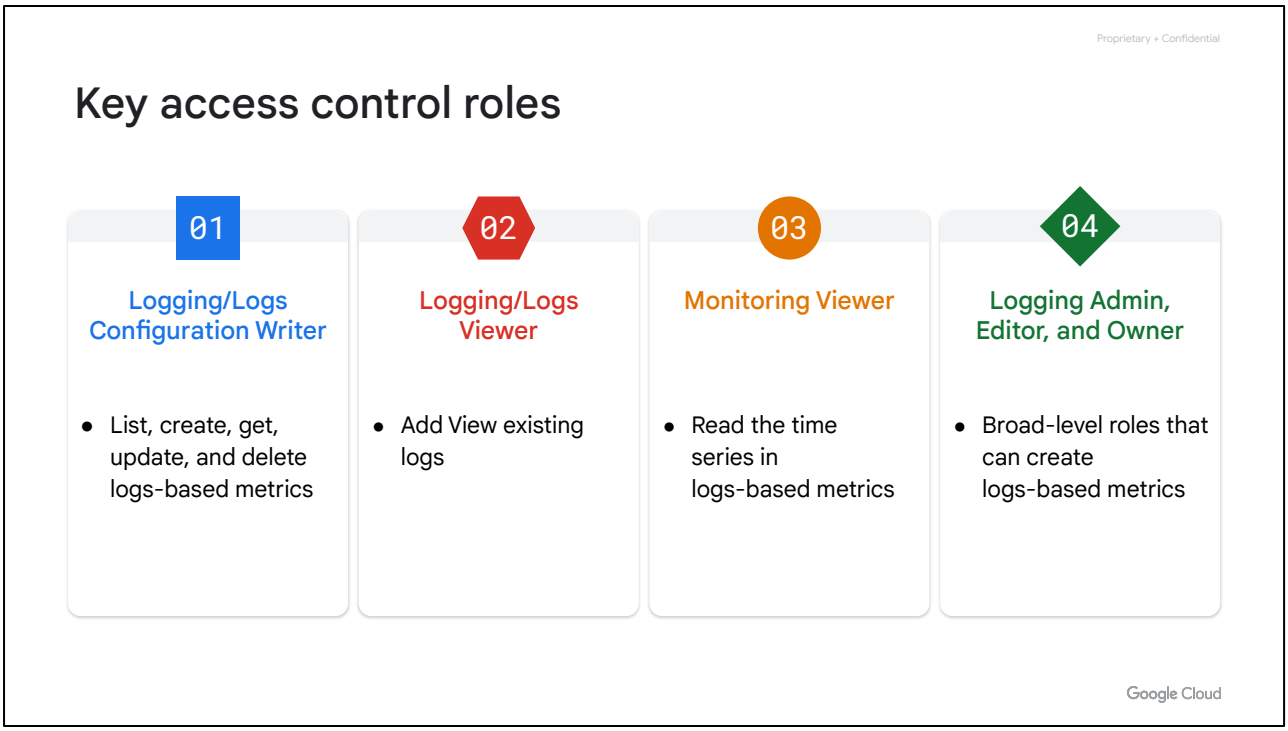


You can also manually restrict the time range using the timestamp keyword, a comparator, and a time in RFC 3339 format.



Some tips on finding log entries quickly:

- Search for specific values of indexed fields, like the log entry name, resource type, and resource labels.
- As seen in the example, be specific on which logs you are searching by referring to it or them by name.
- Limit the time range you are searching to lessen the log data being queried.



A refresher of the key IAM roles that relate to logging and monitoring.

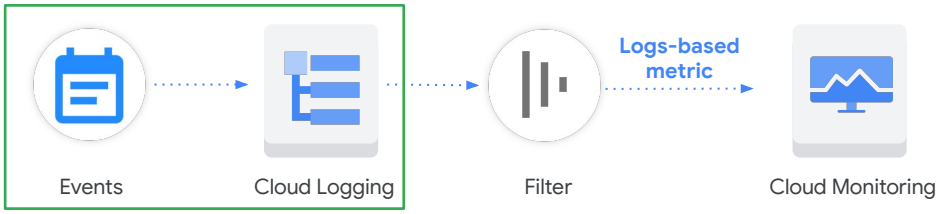
First, on the logging side:

- **Logs Configuration Writers** can list, create, get, update, and delete logs-based metrics.
- **Logs Viewers** can view existing metrics.

On the monitoring side, **Monitoring Viewers** can read the time series in logs-based metrics.

And finally, **Logging Admins**, **Editors**, and **Owners** are all broad-level roles that can create logs-based metrics.

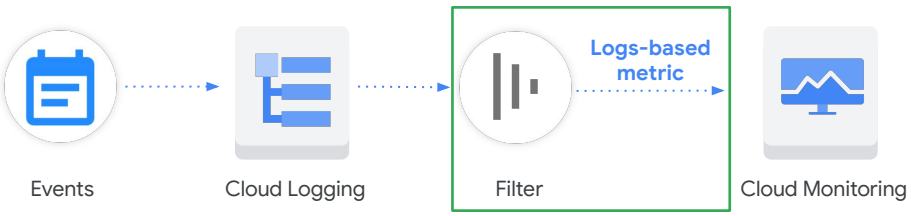
Logs-based metrics



Logs-based metrics are Cloud Monitoring metrics that are based on the content of log entries.

Resources generate logging events that are streamed into Google Cloud Logging.

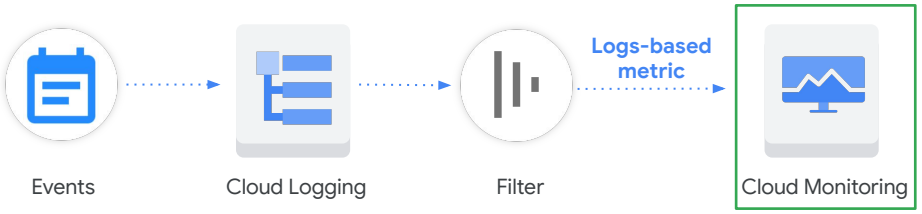
Logs-based metrics



Logs-based metrics apply a **filter** to locate particular entries.

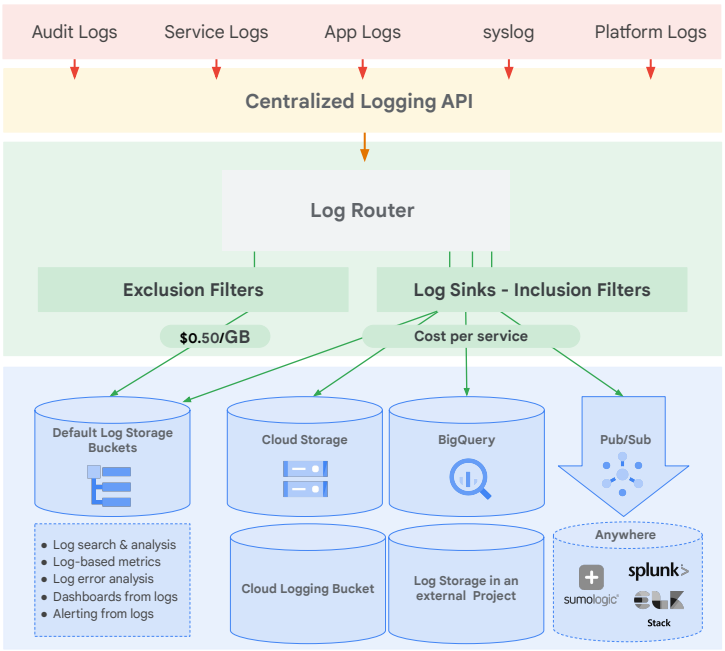
For example, the metrics might record the number of log entries containing particular messages, or that were generated by a particular resource.

Logs-based metrics



Once created, you can use logs-based metrics in Cloud Monitoring charts and alerting policies.

Logging architecture



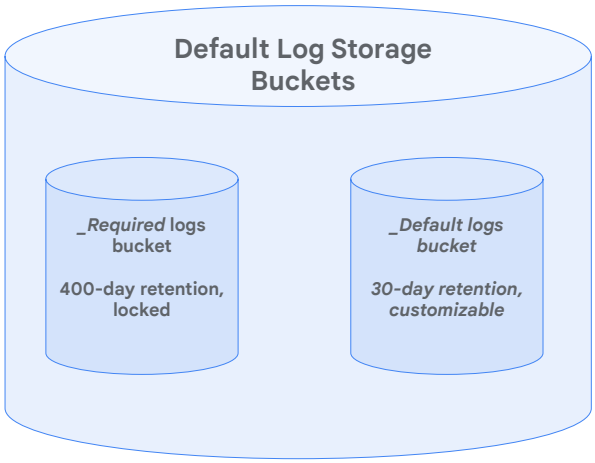
What we call Google Cloud Logging is actually a collection of components exposed through a centralized logging API. Entries are passed through the API and fed to the Log Router. Log Router is optimized for processing streaming data, reliably buffering it, and sending it to any combination of Log Storage and sink (export) locations.

By default, log entries are fed into one of the default log storage buckets. Exclusion filters may be created to partially or totally prevent this behavior.

Log Sinks run in parallel with the default log flow and may be used to direct entries to external locations, including additional Cloud Logging Buckets, Cloud Storage, BigQuery, Pub/Sub, or external projects.

Inclusion and exclusion filters can control exactly which logging entries end up at a particular destination, and which are ignored completely.

Default logs buckets



For each Google Cloud project, Logging automatically creates two logs buckets: *_Required* and *_Default*, and corresponding log sinks with the same names. All logs generated in the project are stored in one of these two locations:

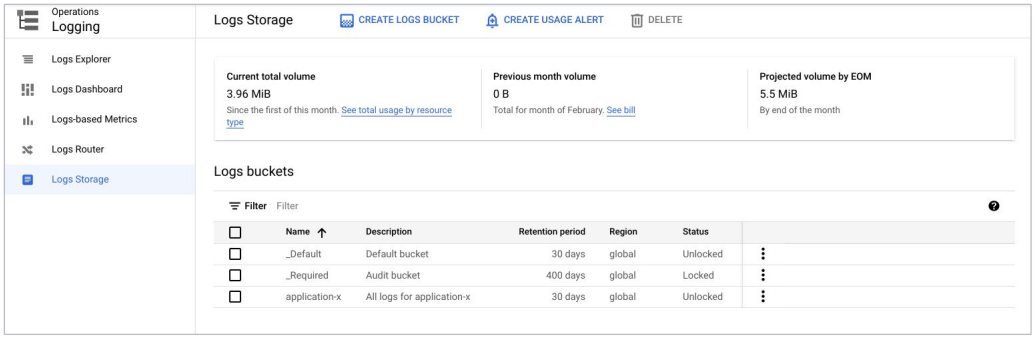
- *_Required*: This bucket holds Admin Activity audit logs, System Event audit logs, and Access Transparency logs, and retains them for 400 days. You aren't charged for the logs stored in *_Required*, and the retention period of the logs stored here cannot be modified. You cannot delete this bucket.
- *_Default:* This bucket holds all other ingested logs in a Google Cloud project, except for the logs held in the *_Required* bucket. Standard Cloud Logging pricing applies to these logs. Log entries held in the *_Default* bucket are retained for 30 days, unless you apply custom retention rules. You can't delete this bucket, but you can disable the *_Default* log sink that routes logs to this bucket.

Use gcloud to adjust the retention:

```
    gcloud beta logging buckets update _Default
--location=global --retention-days=[RETENTION_DAYS]
```

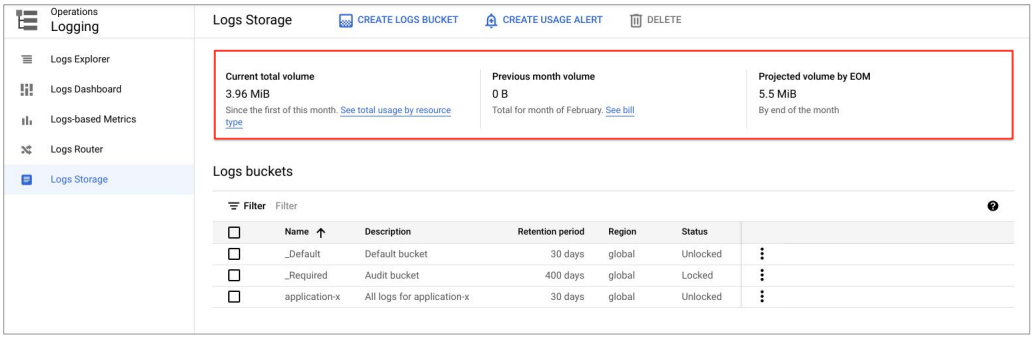
Note: Effective March 31, 2021, storage costs will apply to all chargeable logs retained longer than the default retention periods at the rate of $.01 per GiB per month (or fraction thereof). For details, see Logs storage pricing.

Create specialized buckets in current or remote projects



Logs buckets are containers in your Google Cloud projects that hold your logs data. You can create logs sinks to route all, or just a subset, of your logs to any logs bucket. This flexibility allows you to choose which Google Cloud project your logs are stored in and what other logs are stored with them. Log buckets may also be placed in specific regions for regulatory compliance. Using the gcloud command-line tool and the Google Cloud Console, you can create, update, and delete your custom logs buckets.

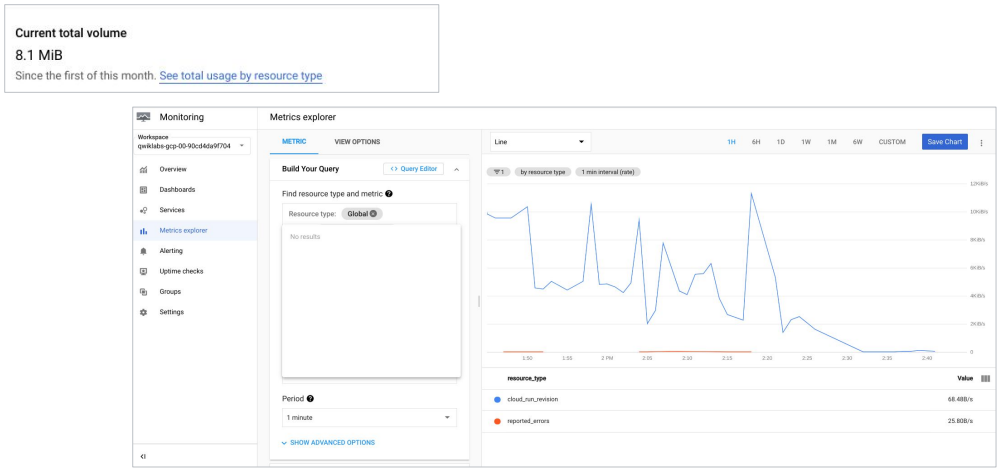
Resource usage



The top of the Logs Storage page displays a summary of statistics for the logs that your project is receiving, including:

- **Current total volume**: The amount of logs your project has received since the first date of the current month.
- **Previous month volume**: The amount of logs your project received in the last calendar month.
- **Projected volume by EOM**: The estimated amount of logs your project will receive by the end of the current month, based on current usage.

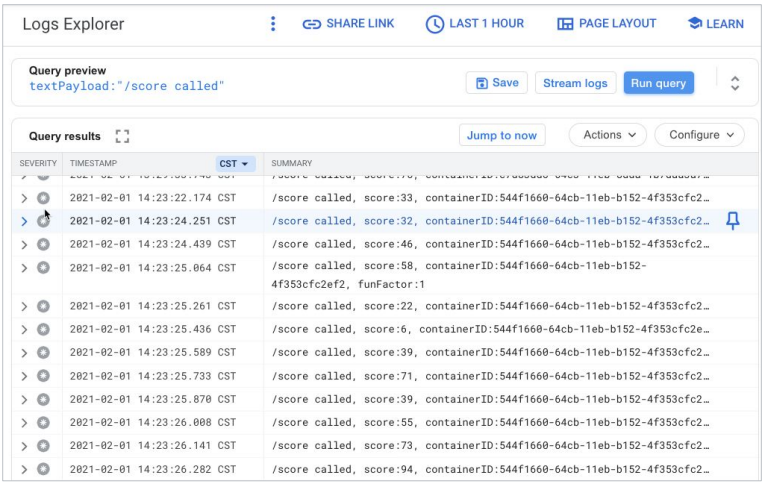
Resource usage



You can view the total usage by resource type for the current total volume. The link opens Metrics Explorer, which allows you to build charts for any metric collected by your project.

For more information on using Metrics Explorer, see https://cloud.google.com/monitoring/charts/metrics-explorer.

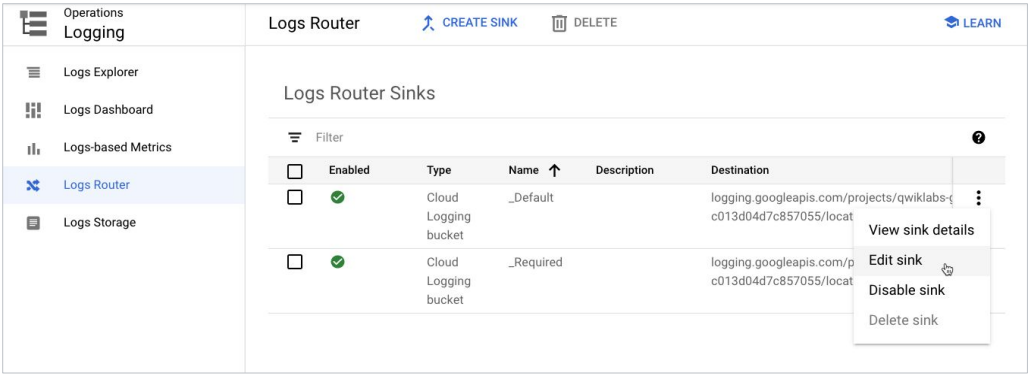
Exclusions: Identify log entries



Use **Logs Explorer** to build a query that selects the logs you want to exclude.

Save the query to use when building the exclusion.

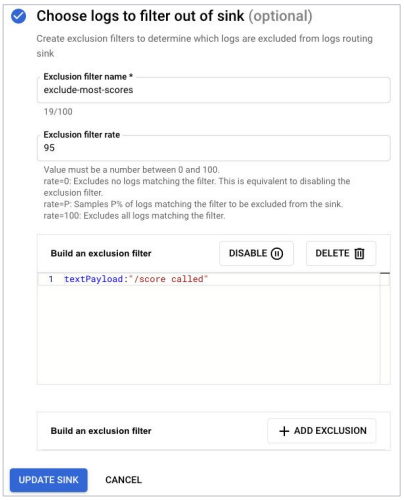
Exclusions: Edit the target log sink



Use the "hamburger menu" to the right of the target log sink to initiate editing of that entity

Take care here, because excluded log events will be lost forever.

Exclusions: Build the exclusion

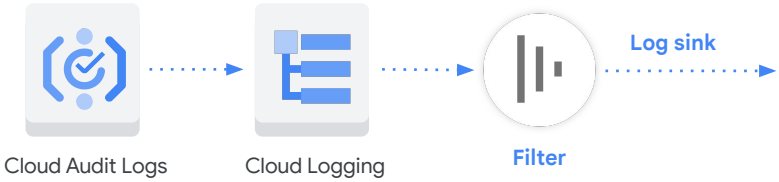


Use the **Log Explorer** query to create an exclusion filter that filters the unwanted entries out of the sink. Give the exclusion a name and description and decide the percentage of log entries to exclude.

It might be helpful to leave some representative events, depending on the exclusion.

Create the exclusion and it will go into effect immediately.

Log router sinks

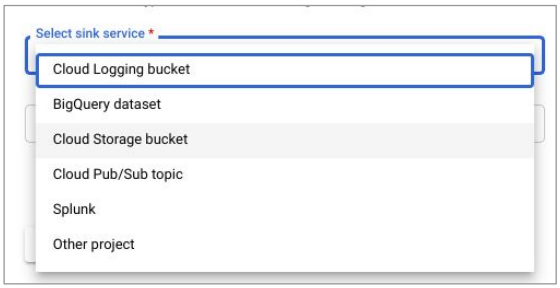



```
severity >= ERROR
resource.type="k8s_container"
resource.labels.project_id="XX"
```


Logs router sinks can be used to forward copies of some or all of your log entries to non-default locations. Use cases include storing logs for extended periods, querying logs with SQL, and access control.

Here, you see we've started creating a sink by creating a logs query for a particular subset of entries. We will pass that subset to one of the available sink locations.

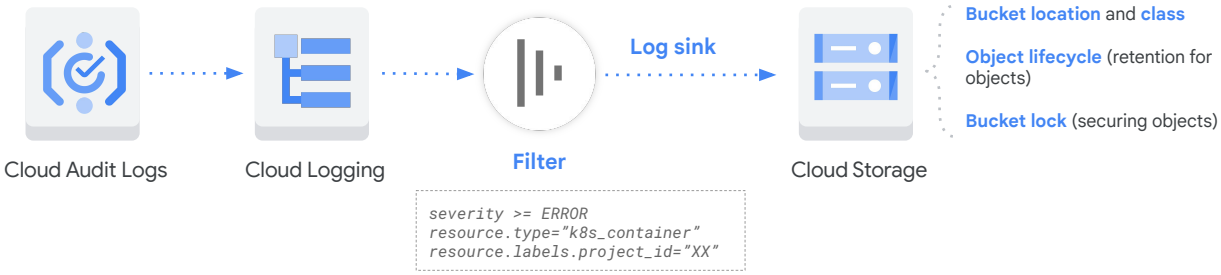
There are several sink locations, depending on need



There are several sink locations, depending on need:

- **Cloud Logging bucket** works well to help pre-separate log entries into a distinct log storage bucket.
- **BigQuery dataset** allows the SQL query power of BigQuery to be brought to bear on large and complex log entries.
- **Cloud Storage bucket** is a simple external Cloud Storage location, perhaps for long-term storage or processing with other systems.
- **Cloud Pub/Sub topic** can export log entries to message handling third-party applications or systems created with code and running somewhere like Dataflow or Cloud Functions.
- **Splunk** for integration of logs into existing Splunk-based system.
- **Other project** is useful to help control access to a subset of log entries.

Cloud Storage works well for general storage



Cloud storage works well for general log storage. It allows the control of bucket location, storage class, object lifecycle rules, and bucket locks. The files can also be easily processed with a number of tools and products.

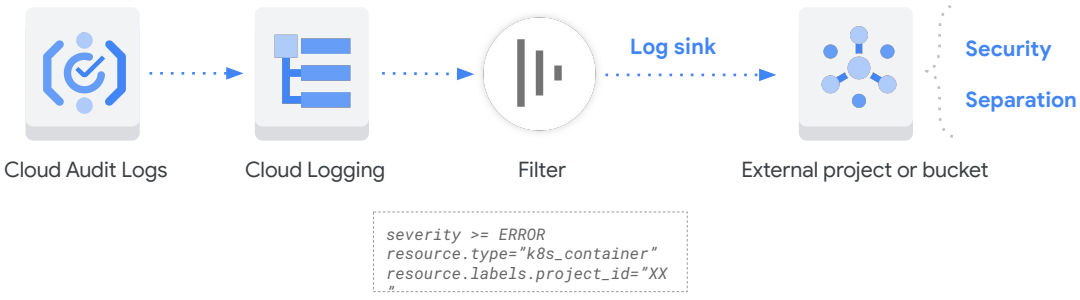
BigQuery for easy warehousing and analysis

BigQuery is a common log sink because it allows both long-term, cost-effective storage and the ability to implement powerful analytics with SQL queries. BigQuery also supports analysis with machine learning, and works well as a back end for visualization.

ub/Sub to connect with external systems and applications

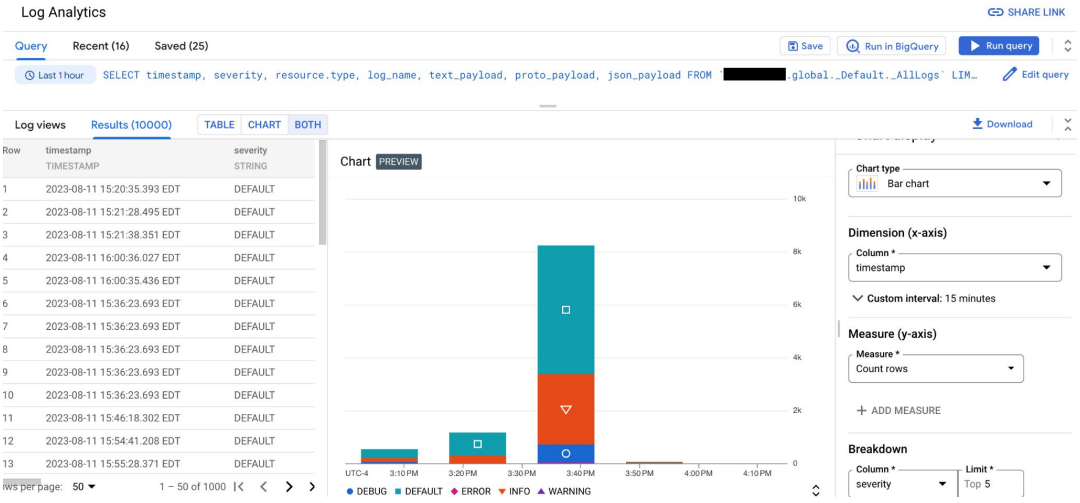
Pub/Sub allows logging events to be streamed asynchronously to code, event processing pipelines created in Cloud Functions, Cloud Run, or Dataflow, or to third-party log analysis tools.

Log exports



Using a specialized bucket or external project is a great way to limit access and to control log entry location.

Log Analytics: Use SQL to query your logs



Google Cloud

Log Analytics is an alternative way of viewing and querying your logs. You query the logs using the SQL language, as shown above.

https://cloud.google.com/logging/docs/log-analytics#analytics

Monitoring Network Security and Audit Logs

In this module, let’s spend some time analyzing the Google Cloud Virtual Private Cloud.

Firewall Rules

01 VPC Flow Logs

02 Firewall Rules Logging

03 Load Balancer Logs

04 Cloud NAT Logs

05 Packet Mirroring

06 Network Intelligence Center

VPC Flow Logs record a sample of network flows

VPC Flow Logs record 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
protocol	int32	IANA protocol number

Other fields:

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

Cloud Logging

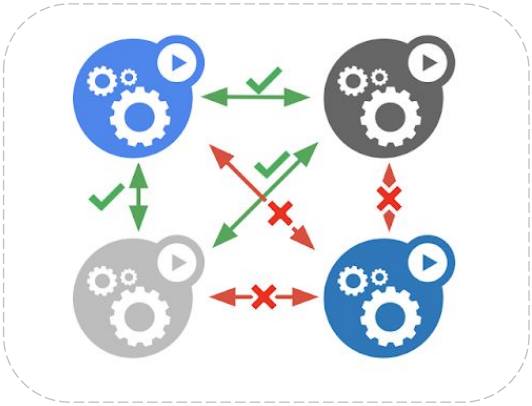
You can enable or disable VPC Flow Logs per VPC subnet. Once enabled for a subnet, VPC Flow Logs collect data from all VM instances in that subnet.

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 here: https://cloud.google.com/vpc/docs/using-flow-logs#logs_collection

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

01 VPC Flow Logs

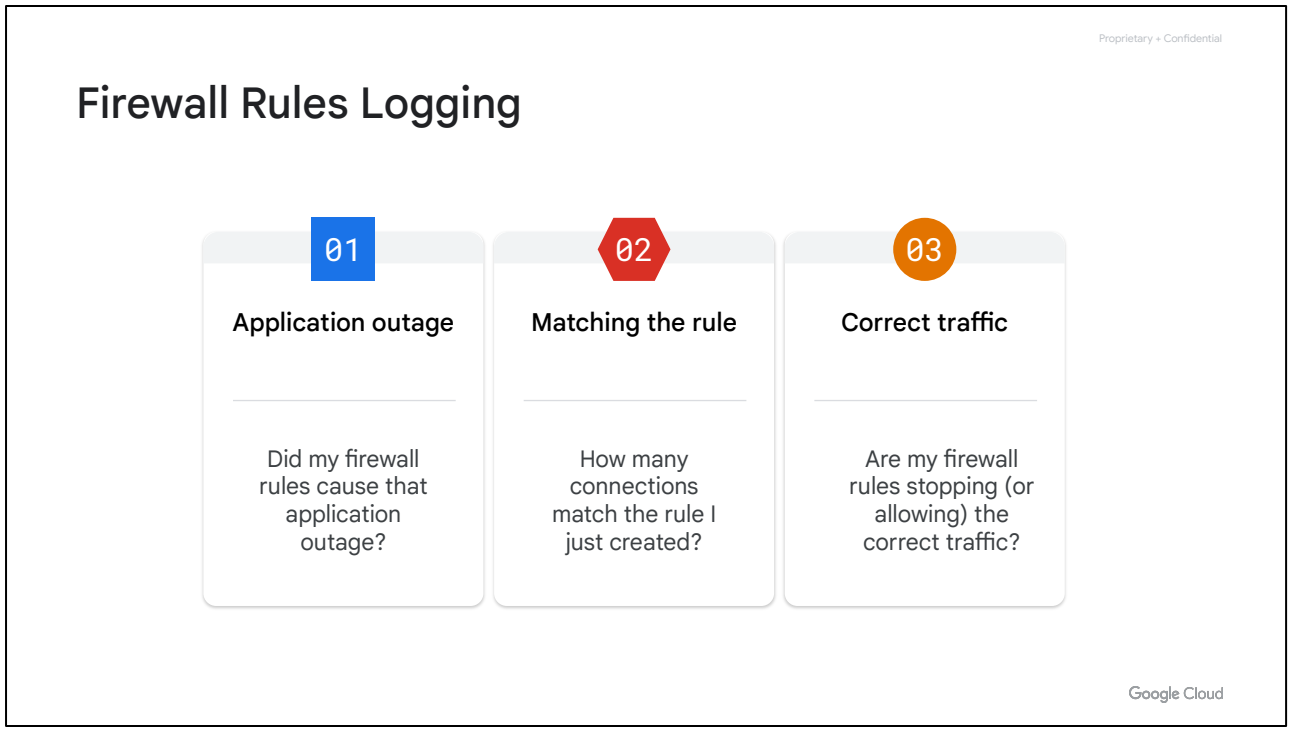
02 Firewall Rules Logging

03 Load Balancer Logs

04 Cloud NAT Logs

05 Packet Mirroring

06 Network Intelligence Center



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

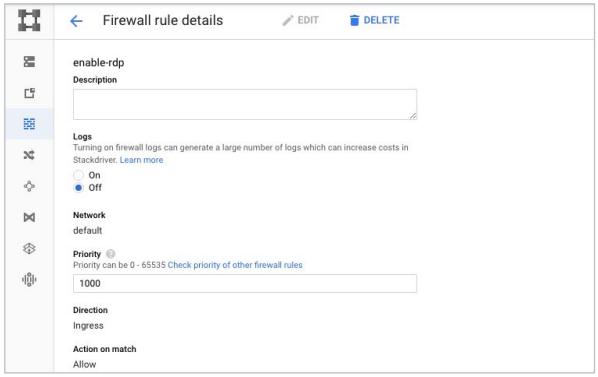
It can help answer questions like:

- 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 Rules Logging in the console

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

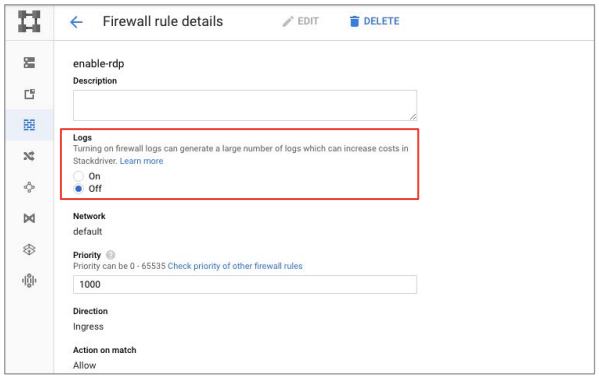


By default, Firewall Rules Logging is disabled.

You can enable it on a per-rule basis.

Enabling Firewall Rules Logging in the console

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



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

Caution: Firewall Rules Logging can generate a lot of data which may have a cost impact.

Enabling Firewall Rules Logging in the CLI

- Firewall Rules 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 Rules Logging can also be enabled on existing firewall rules using the CLI.

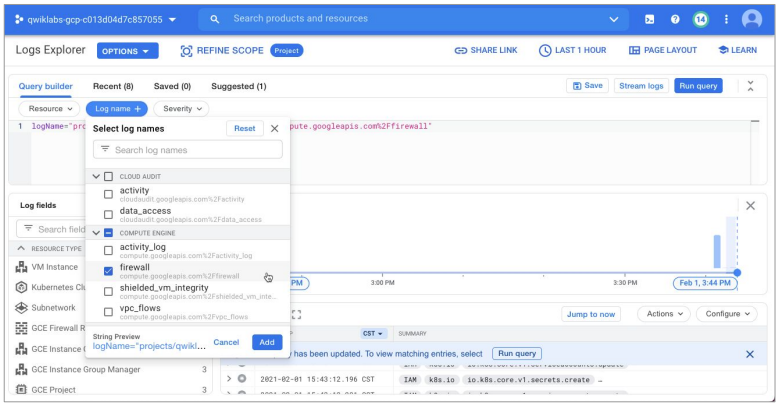
See these two examples on this slide. In both, [NAME] would be the name of your firewall rule.

Viewing the Firewall Rules logs

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

Cloud Logging

BigQuery



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

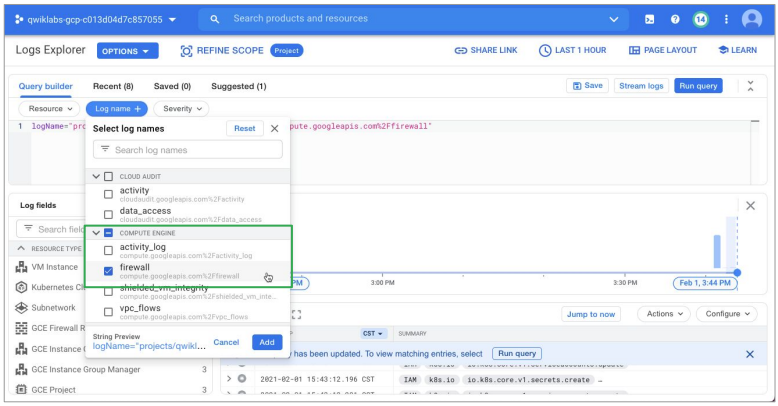
BigQuery is frequently used to simplify firewall rules log analysis.

Viewing the Firewall Rules logs

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

Cloud Logging

BigQuery

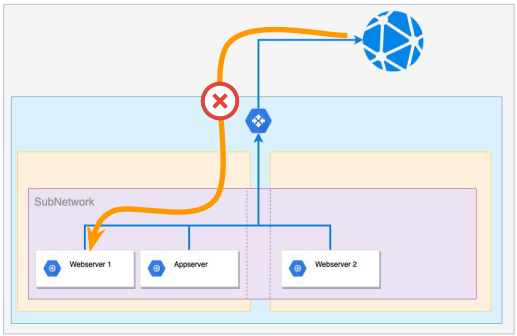


Like all Google Cloud Logs, use Logs Explorer to view logs in real time, or to configure exports.

BigQuery is frequently used to simplify firewall rules log analysis.

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.

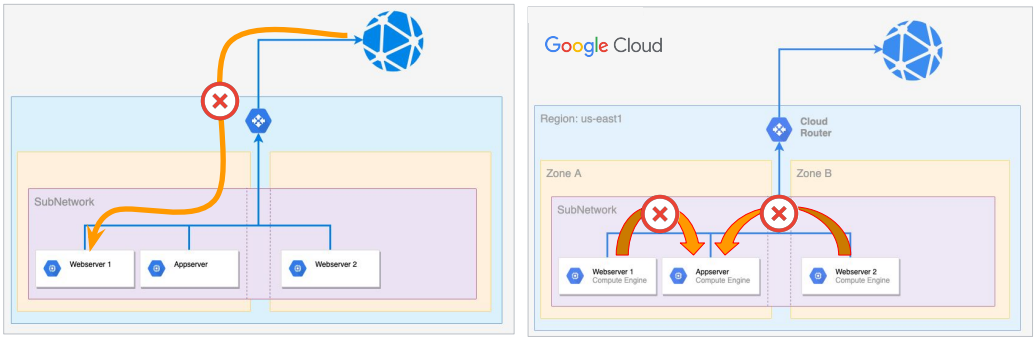
At the network boundary, where the private network meets the outside internet, sits a firewall.

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.

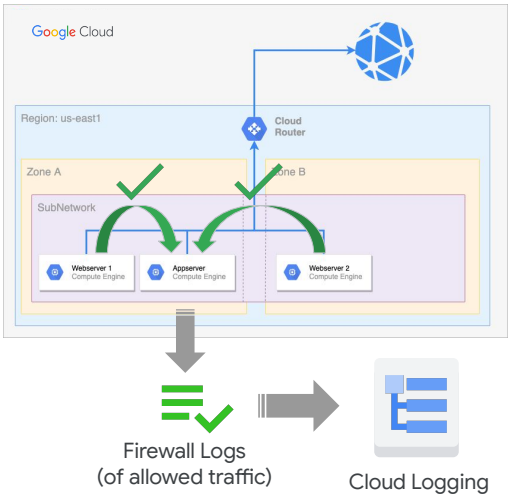
Now, imagine we have an issue.

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.

Firewall Rules

01 VPC Flow Logs

02 Firewall Rules Logging

03 Load Balancer Logs

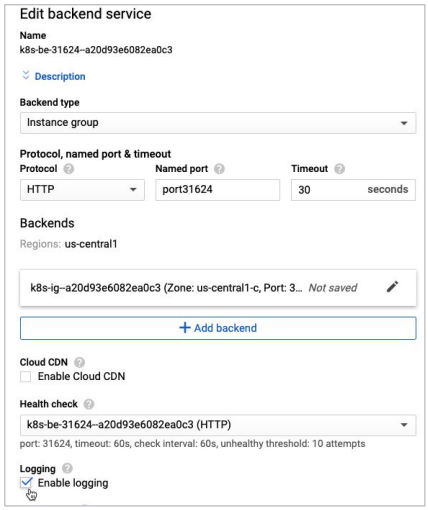
04 Cloud NAT Logs

05 Packet Mirroring

06 Network Intelligence Center

The internal and external HTTP(s) load balancers support logging

- Enabled on a per backend service basis
  - URL map may reference more than one
  - Will have to enable for each
- Enabled by default



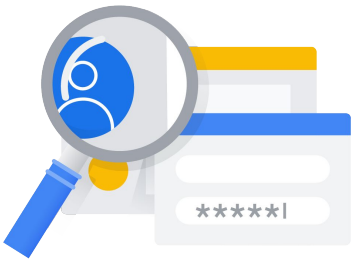
You can enable logging on a per backend service basis. A single internal HTTP(S) load balancer URL map can reference more than one backend service, so you might need to enable logging for more than one backend service, depending on your configuration. It will be enabled by default for all new load balancers backends, but backends created before the GA release of load balancer logging may require manual configuration.

Log entries

Types of information

Log entries contain the following types of information:

- General information including:
  - Severity, project ID, project number, and timestamp.
- HttpRequest log fields, including:
  - Method, URL, status, remote IP, and user agent.
- A *statusDetails* containing a string explaining why the load balancer returned the HTTP status that it did, cache and failure information.
- Redirects (HTTP response status code 302 found) issued from the load balancer are not logged. Redirects issued from the backend instances are logged.



HTTP(S) load balancing log entries contain information useful for monitoring and debugging your HTTP(S) traffic. Make sure to check the documentation for details.

Log entries contain the following types of information:

- General information shown in most logs, such as severity, project ID, project number, timestamp, and so on.
- HttpRequest log fields. However, *HttpRequest.protocol* is not populated for HTTP(S) load balancing Cloud Logging logs.
- A *statusDetails* field inside the *structPayload*. This field holds a string that explains why the load balancer returned the HTTP status that it did.
- Redirects (HTTP response status code 302 Found) issued from the load balancer are *not* logged. Redirects issued from the backend instances *are* logged.

Firewall Rules

01 VPC Flow Logs

02 Firewall Rules Logging

03 Load Balancer Logs

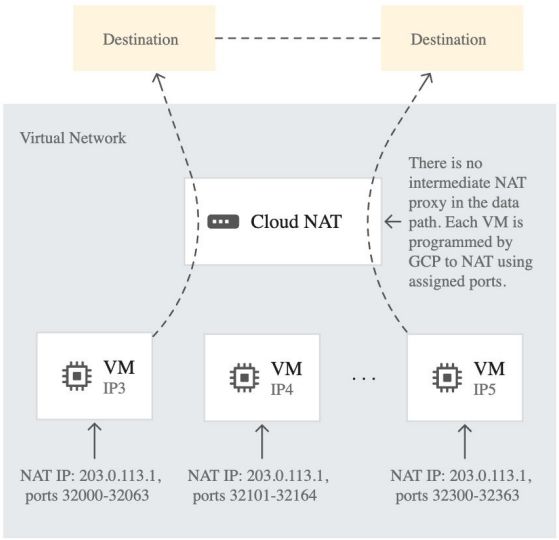
04 Cloud NAT Logs

05 Packet Mirroring

06 Network Intelligence Center

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



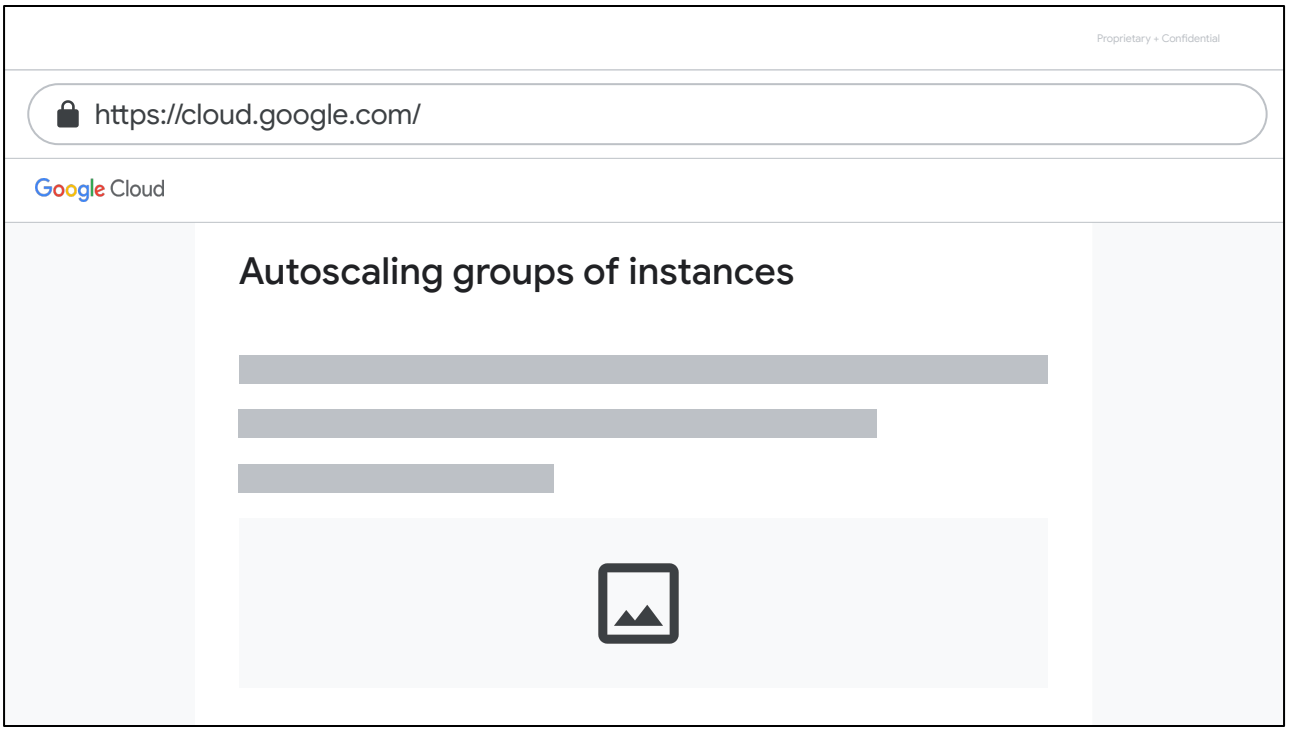
Cloud NAT (network address translation) allows Google Cloud virtual machine (VM) instances without external IP addresses and private Google Kubernetes Engine (GKE) clusters to send outbound packets to the internet and receive any corresponding established inbound response packets.

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

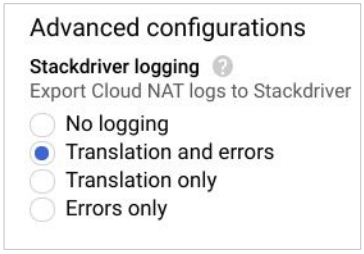
- networking.



For more information about autoscaling, visit the guide titled ‘Autoscaling groups of instance’ in the official Google Cloud documentation.

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



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"

Firewall Rules

01 VPC Flow Logs

02 Firewall Rules Logging

03 Load Balancer Logs

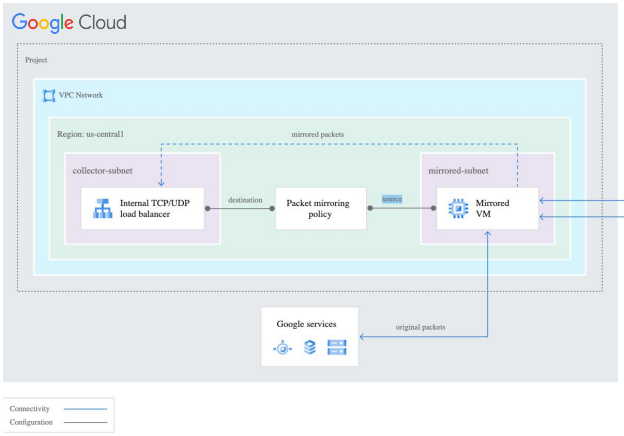
04 Cloud NAT Logs

05 Packet Mirroring

06 Network Intelligence Center

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.

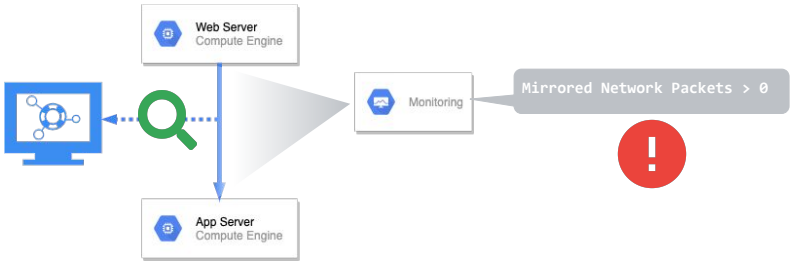
Packet Mirroring is useful when you need to monitor and analyze your security status. It exports all traffic, not only the traffic between sampling periods. For example, you can use security software that analyzes mirrored traffic to detect all threats or anomalies.

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



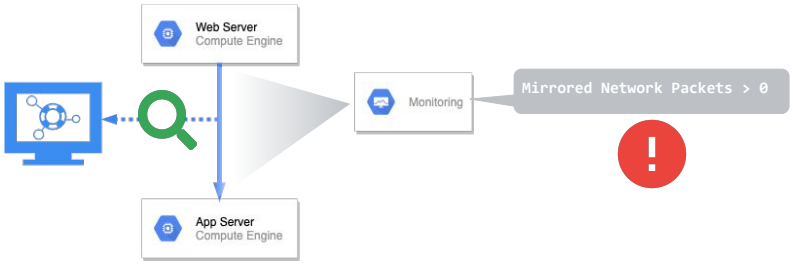
Packet Mirroring exports monitoring data about mirrored traffic to Cloud Monitoring.

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

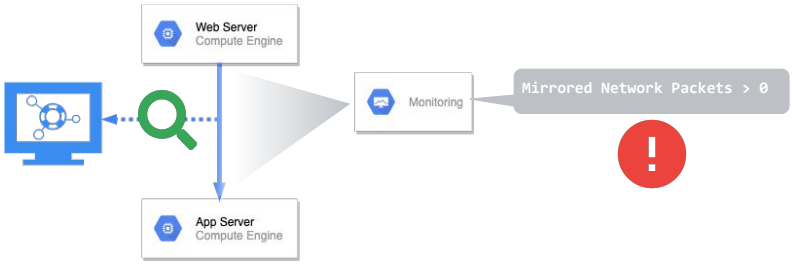


You can view the monitoring metrics of mirrored VM instances or instances that are part of the collector destination (internal load balancer).

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.

Firewall Rules

01 VPC Flow Logs

02 Firewall Rules Logging

03 Load Balancer Logs

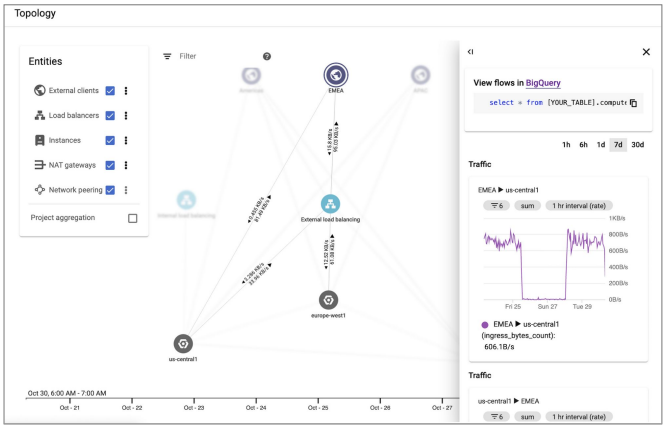
04 Cloud NAT Logs

05 Packet Mirroring

06 Network Intelligence Center

Network Intelligence Center

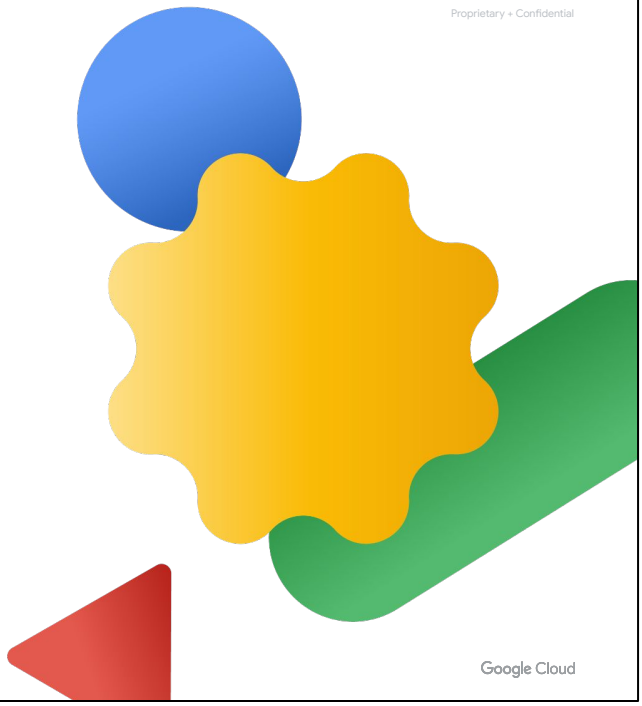
Centralized Network monitoring and visibility



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.

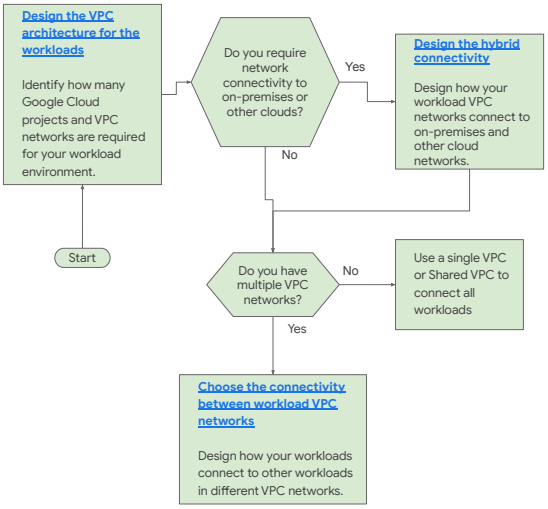
Currently, it offers four modules: network topology, connectivity testing, a performance dashboard, and firewall insights.

Network Architecture Design Approach



BREAK SLIDE

Network architecture design approach



This slide deck introduces a design approach for cloud network architecture in Google Cloud. The goal is to design a foundational network topology that supports the deployment of future workloads. The network design can be approached in three distinct phases.

1) Designing the workload VPC architecture

It is important to identify at an early stage, how many projects and Virtual Private Cloud (VPC) networks are required to host your workloads.

Projects are fundamental grouping mechanisms in Google Cloud. A project contains related services and workloads that have a single administrative domain. A project is required to use Google Cloud, and forms the basis for creating, enabling, and using all Google Cloud services, managing APIs, enabling billing, adding and removing collaborators, and managing permissions.

Enterprises may have different administrative domains for their workload environments. For example, the Development team may manage all workloads in one project, and the Production team may manage their workloads in a separate project.

A projects contains one or more VPC networks. A VPC network provides connectivity between Google Cloud workloads, and to external networks.

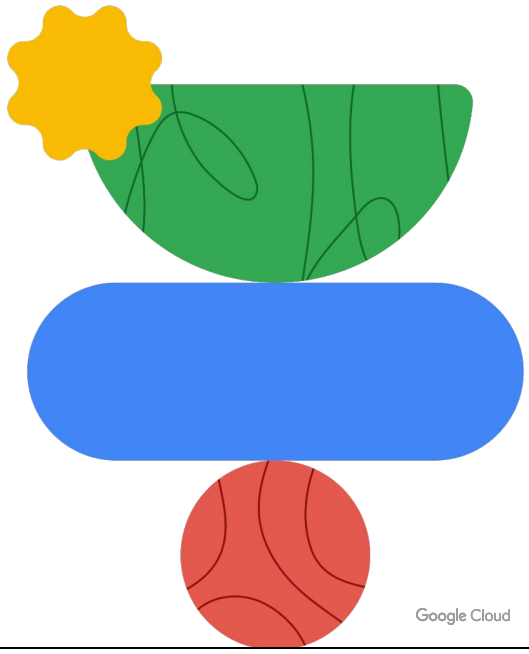
2) Designing the hybrid network connectivity

It is important to design a robust hybrid network topology that allows workload VPC networks to connect to on-premises networks, and other cloud networks. Many enterprises require hybrid connectivity to their on-premises datacenter workloads via an Cloud Interconnect or VPN. Many enterprises also require multi-cloud connectivity to workloads running on other clouds.

3) Designing the connectivity between workload VPC networks

Multiple workload VPC networks in Google Cloud may require connectivity between each other. There are different ways to connect workloads depending on the workload type (i.e., IaaS, serverless or managed services). Learn more about connecting multiple VPC networks.

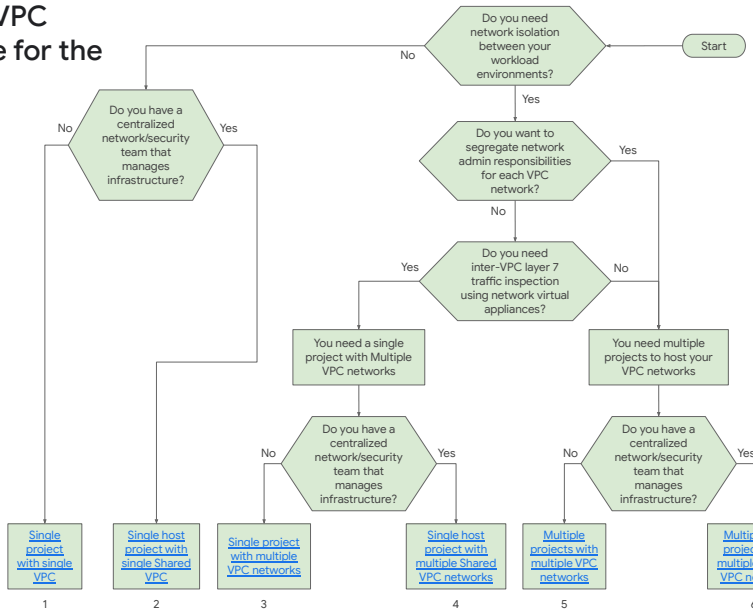
Designing the VPC Architecture for the Workloads



~~Note: These slides are sourced from the Partner Advantage document Google Cloud Networking Design Patterns | Technical | Y22~~

Welcome to this section: Design the VPC Architecture for the Workloads.

Design the VPC architecture for the workloads



Google Cloud

Identify how many Google Cloud projects and VPC networks are required for your workloads.

The number of projects and VPC networks depends on factors such as:

- ✓ The need for layer 7 traffic inspection of network traffic using third-party VM appliances
- ✓ The need for mitigation of data exfiltration (using VPC Service Control perimeters)
- ✓ The need for central network resource configuration and management

Use the decision tree to select the appropriate workload VPC architecture from the following options:

1. Single project with single VPC
2. Single host project with single Shared VPC

Designing the VPC Architecture for the Workloads

01 Single project with single VPC

02 Single host project with single Shared VPC

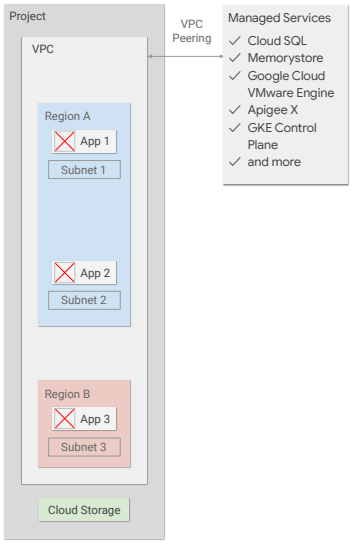
03 Single project with multiple VPC networks

04 Single host project with multiple Shared VPC networks

05 Multiple projects with multiple VPC networks

06 Multiple host projects with multiple Shared VPC networks

1. Single project with single VPC



Recommended to use when

Network Security

1. You **do not need network isolation between applications**. All applications can reside in a single network.

2. Firewall rules inside a VPC network are sufficient to control network access between applications.

3. Identity and Access Management (IAM) permissions are sufficient to control access to cloud services.

Network Operations

4. In a multi-team environment, application teams want **autonomy over the configuration of network resources** for their applications. A standalone VPC (rather than Shared VPC) can be used.

Recommended hybrid connectivity

Use the following hybrid connectivity for connecting to on-premises or other clouds:

Designing the VPC Architecture for the Workloads

01 Single project with single VPC

02 Single host project with single Shared VPC

03 Single project with multiple VPC networks

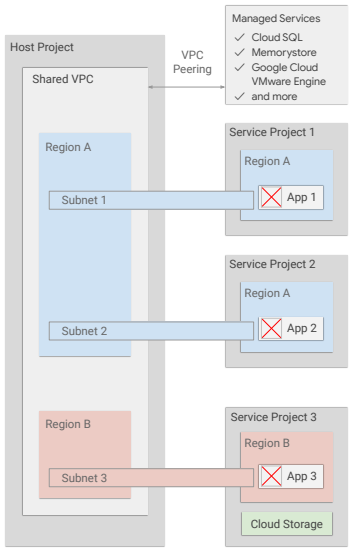
04 Single host project with multiple Shared VPC networks

05 Multiple projects with multiple VPC networks

06 Multiple host projects with multiple Shared VPC networks

Proprietary + Confidential

2. Single host project with single Shared VPC



Google Cloud

Recommended to use when

Network Security

1. You **do not need network isolation between applications**. All applications can reside in a single network.

2. Firewall rules inside a VPC network are sufficient to control network access between applications.

3. IAM permissions are sufficient to control access to cloud services

Network Operations

4. In a multi-team environment, you want a network team to **centrally manage network resources in a common network**. Shared VPC allows application teams to deploy their applications in projects (Service Projects) that use network resources in a centrally managed network (Shared VPC).

Recommended hybrid connectivity

Use the following hybrid connectivity for connecting to on-premises or to other clouds:

Designing the VPC Architecture for the Workloads

01 Single project with single VPC

02 Single host project with single Shared VPC

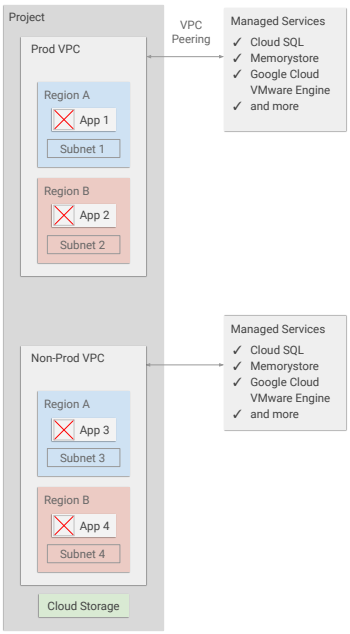
03 Single project with multiple VPC networks

04 Single host project with multiple Shared VPC networks

05 Multiple projects with multiple VPC networks

06 Multiple host projects with multiple Shared VPC networks

3. Single project with multiple VPC networks



Recommended to use when

Network Security

1. You need **network isolation between workload environments** (typically required as part of network security compliance). For example, network isolation between Prod and Non-Prod workloads requires the workload applications to be deployed in separate VPC networks.

2. You may need a network virtual appliance (NVA) for **layer 7 traffic inspection between workload environments**. For example, layer 7 traffic inspection between Prod and Non-prod applications requires that the applications are in separate VPC networks.

Network Operations

3. Application teams want **autonomy over network resource configuration** for their applications. For example, if the Prod application team requires autonomy over network resource configuration, they can deploy their application and all associated networking configuration directly in the Prod VPC and not a Shared VPC.

Recommended hybrid connectivity

- B. Hybrid connectivity to multiple VPC (or Shared VPC) networks)

If you require layer 7 traffic inspection between the VPC networks, use the following:

- C. Hybrid connectivity using appliances

Designing the VPC Architecture for the Workloads

01 Single project with single VPC

02 Single host project with single Shared VPC

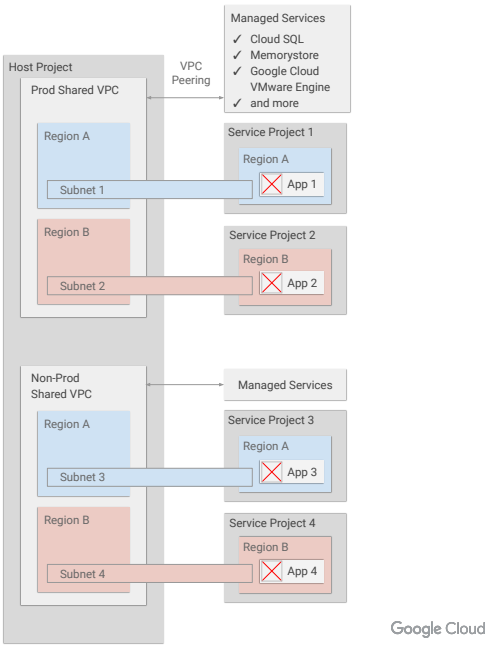
03 Single project with multiple VPC networks

04 Single host project with multiple Shared VPC networks

05 Multiple projects with multiple VPC networks

06 Multiple host projects with multiple Shared VPC networks

4. Single host project with multiple Shared VPC networks



Recommended to use when

Network Security

1. You need **network isolation between workload environments** (typically required as part of network security compliance). For example, network isolation between Prod and Non-Prod workloads requires the workload applications to be deployed in separate VPC networks.

2. You may need a network virtual appliance (NVA) for **layer 7 traffic inspection between workload environments**. For example, layer 7 traffic inspection between Prod and Non-prod applications requires that the applications are in separate VPC networks.

Network Operations

3. You require a network team to **centrally manage network resources in a common network**. Shared VPC allows application teams to deploy their applications in projects (Service Projects) that use network resources in a centrally managed network (Shared VPC).

Recommended hybrid connectivity

If you require layer 7 traffic inspection between the VPC networks, use the following:

- C. Hybrid connectivity using appliances

Designing the VPC Architecture for the Workloads

01 Single project with single VPC

02 Single host project with single Shared VPC

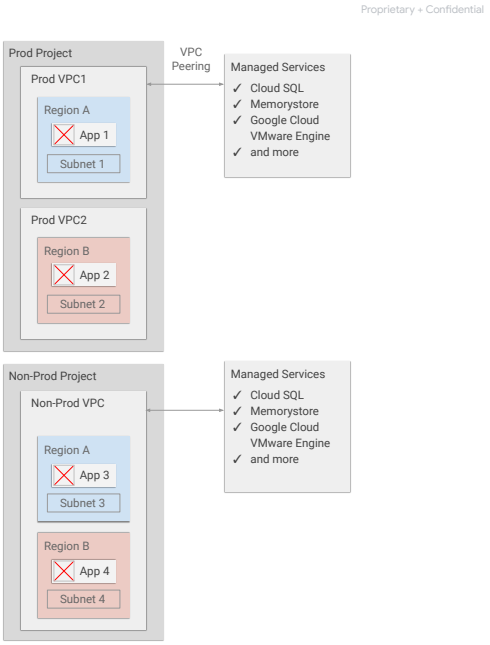
03 Single project with multiple VPC networks

04 Single host project with multiple Shared VPC networks

05 Multiple projects with multiple VPC networks

06 Multiple host projects with multiple Shared VPC networks

5. Multiple projects with multiple VPC networks



Recommended to use when

Network Security

1. You need **network isolation between workload environments** (typically required as part of network security compliance). For example, network isolation between Prod and Non-Prod workloads requires the workload applications to be deployed in separate VPC networks.

2. You may need a network virtual appliance (NVA) for **layer 7 traffic inspection between application environments**. For example, layer 7 traffic inspection between Prod and Non-prod applications requires that the applications are in separate VPC networks.

3. You want to **segregate network IAM admin per environment**. For example, when a user requires project viewer role on all resources in Prod, and project editor role on all resources in Non-prod, then the Prod and Non-prod applications (and their VPC networks) should be in separate projects.

Network Operations

4. Application teams want **autonomy over network resource configuration** for

Recommended hybrid connectivity

Use the following recommended hybrid connectivity for connecting your VPC networks to on-premises or other clouds:

- B. Hybrid connectivity to multiple VPC (or Shared VPC) networks)

If you require layer 7 traffic inspection between the VPC networks, use the following:

- C. Hybrid connectivity using appliances

Designing the VPC Architecture for the Workloads

01 Single project with single VPC

02 Single host project with single Shared VPC

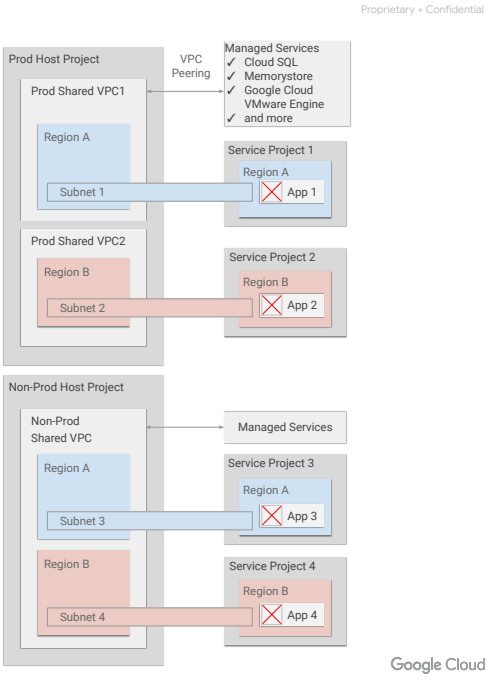
03 Single project with multiple VPC networks

04 Single host project with multiple Shared VPC networks

05 Multiple projects with multiple VPC networks

06 Multiple host projects with multiple Shared VPC networks

6. Multiple host projects with multiple Shared VPC networks



Recommended to use when

Network Security

1. You need **network isolation between workload environments** (typically required as part of network security compliance). For example, network isolation between Prod and Non-Prod workloads requires the workload applications to be deployed in separate VPC networks.

2. You may need a network virtual appliance (NVA) for **layer 7 traffic inspection between application** environments. For example, layer 7 traffic inspection between Prod and Non-prod applications requires that the applications are in separate Shared VPC networks.

3. You want to **segregate network IAM admin per environment**. For example, when a user requires project viewer role on all resources in Prod, and project editor role on all resources in Non-prod, then Prod and Non-prod applications (and their VPC networks) should be in separate projects.

Network Operations

4. You require a network team to **centrally manage network resources in a**

Recommended hybrid connectivity

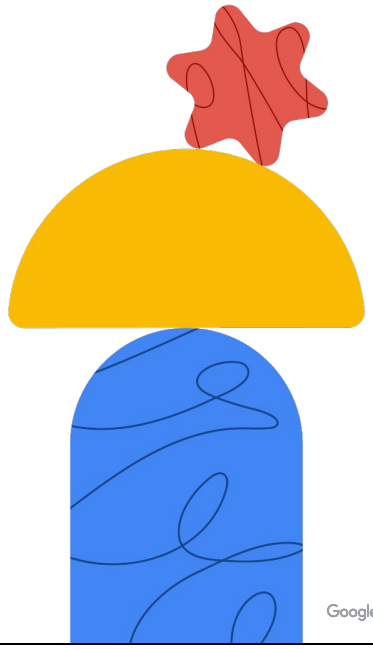
Use the following recommended hybrid connectivity for connecting your VPC networks to on-premises or other clouds:

- B. Hybrid connectivity to multiple VPC (or Shared VPC) networks

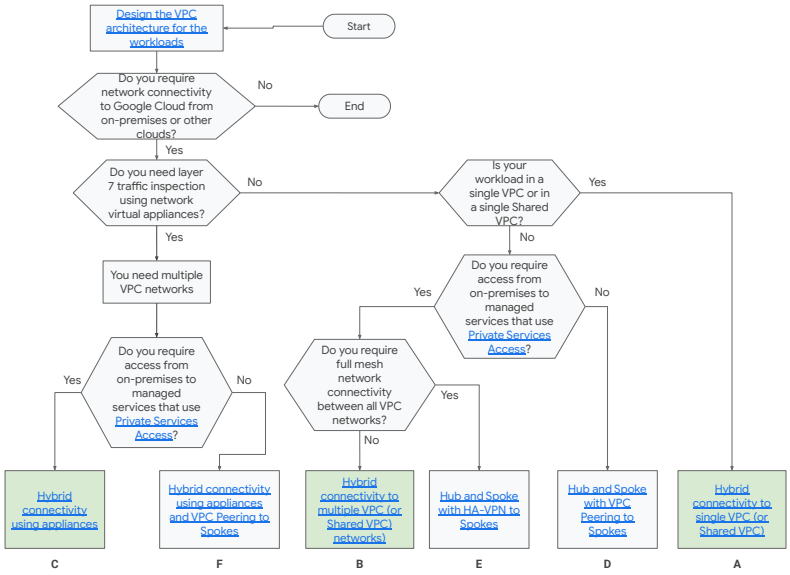
If you require layer 7 traffic inspection between the VPC networks, use the following:

- C. Hybrid connectivity using appliances

Designing the Hybrid Connectivity



Design the hybrid connectivity



Design the hybrid network topology for connecting workloads in your VPC network(s) to on-premises and other clouds.

The hybrid connectivity design depends on factors such as:

- ✓ The number of VPC networks used for the workloads
- ✓ The need for layer 7 traffic inspection of network traffic using network virtual appliances (NVA) appliances
- ✓ Access to Google-managed services that use Private Services Access

Use the decision tree as a quick guide in selecting the appropriate network topology. The following network topology patterns are recommended:

A. Hybrid connectivity to single VPC (or Shared VPC)

B. Hybrid connectivity to multiple VPC (or Shared VPC) networks

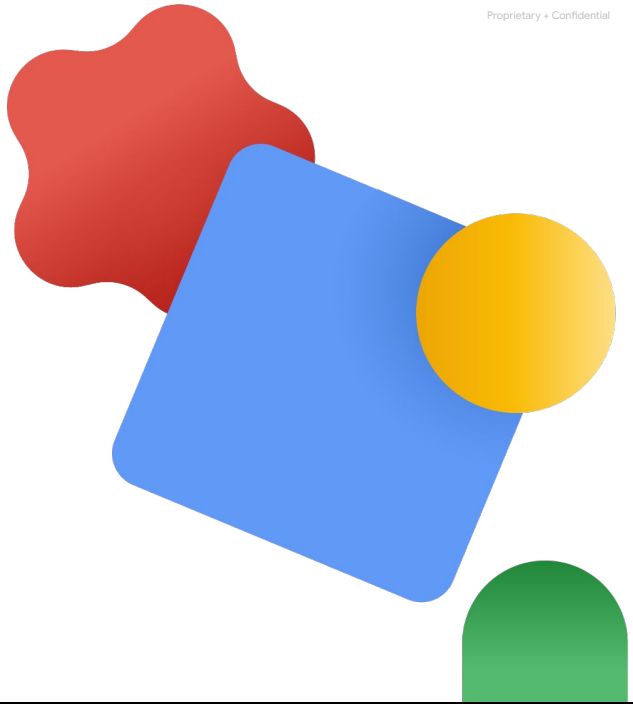
C. Hybrid connectivity using appliances

When you have a large number of workload VPC networks, you might need a hub and spoke architecture that supports a large number of VPC networks. This involves connecting multiple workload VPC networks to a transit Hub VPC that has connectivity to on-premises and other clouds. Consider the following network topology patterns and their associated pros and cons:

D. Hub and Spoke with VPC Peering to Spokes

E. Hub and Spoke with HA-VPN to Spokes

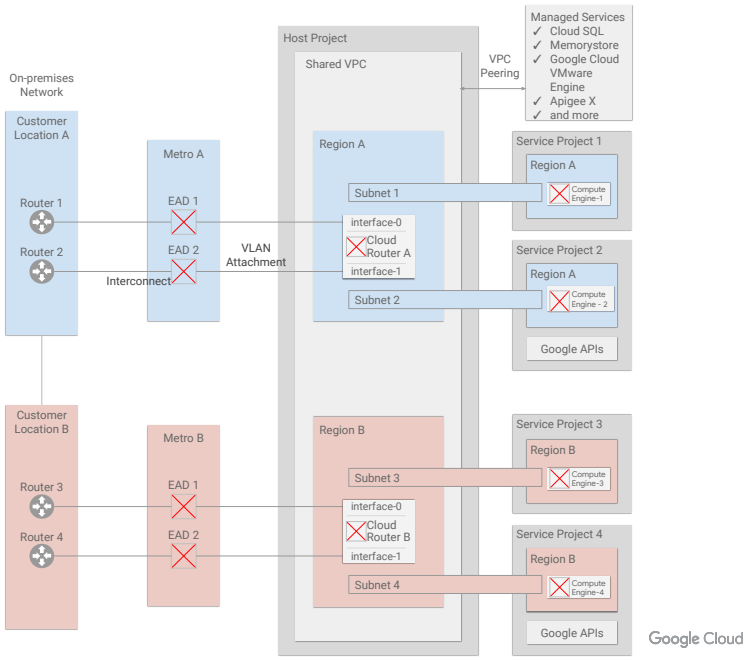
Hybrid Connectivity to a Single VPC (for Shared VPC



BREAK SLIDE

A. Hybrid connectivity to single VPC (or Shared VPC)

A1: Summary



Abbreviation
EAD = Edge Availability Domain
Metro = Metropolitan Area

Overview

The network design patterns in **Section A** apply to the following workload environments:

- ✓ Single project with single VPC
- ✓ Single host project with single Shared VPC (shown here)

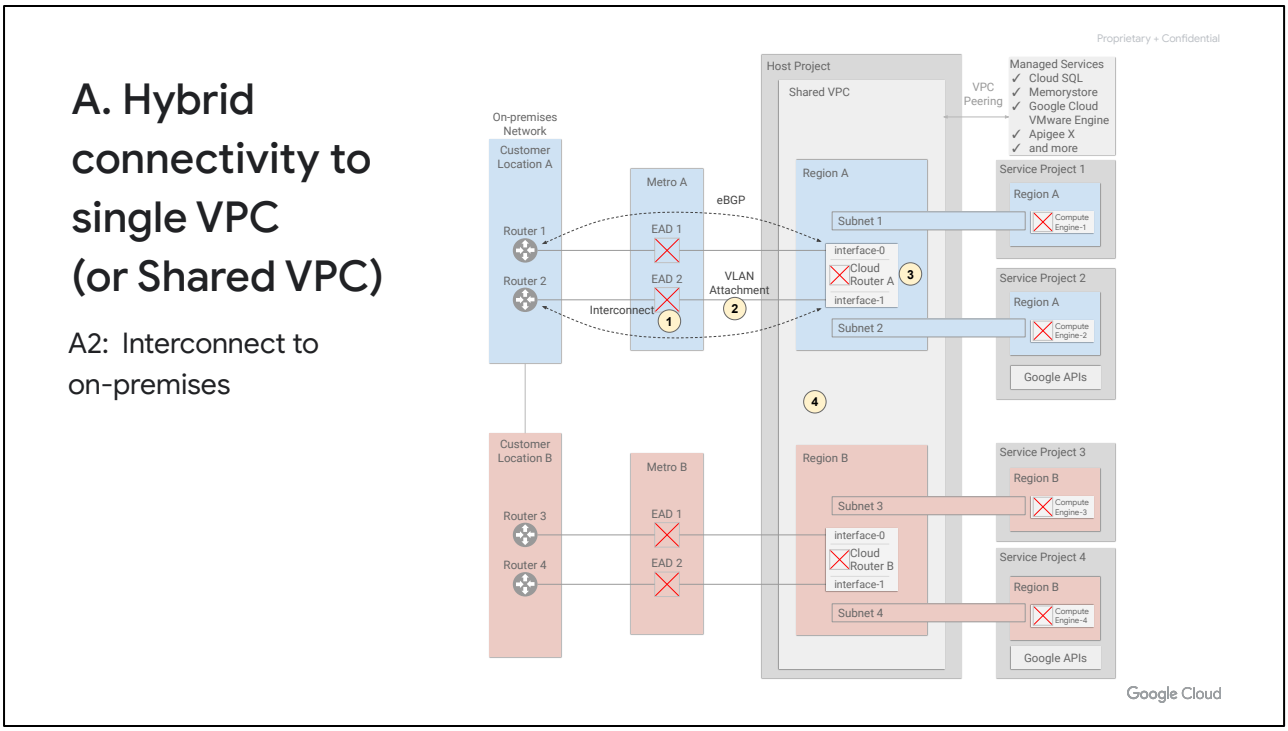
In this network topology, Interconnect (or HA-VPN) from on-premises (or other clouds) terminates directly into a single Shared VPC.

This pattern provides hybrid connectivity to

- ✓ IaaS resources in the workload Shared VPC
- ✓ Google APIs and services (for example, storage.googleapis.com , *.run.app) in the service projects
- ✓ Google Cloud managed services that use Private Services Access

Scaling Out

If your workload environment grows and you require more Host Projects and Shared VPC networks, you can expand this architecture as illustrated in **Section B** - Hybrid connectivity to multiple VPC (or Shared VPC) networks.



1) Cloud Interconnect

Set up Dedicated Interconnect or Partner Interconnect to Google Cloud. Connect to two Edge Availability Domains (EAD) in the same Metro in order to achieve 99.99% SLA. You can connect your Cloud Interconnects to multiple regions in the same Shared VPC. This diagram shows Dedicated Interconnect in two regions.

2) VLAN Attachment

A VLAN attachment connects your interconnect in a Google point of presence (PoP) to a Cloud Router in a specified Google Cloud region.

3) Cloud Router

A Cloud Router exchanges dynamic (BGP) routes between your VPC networks and on-premises routers. You can configure dynamic routing between your on-premises routers and a cloud router in a particular region. Each cloud router is implemented by two software tasks that provide two interfaces for high availability. Configure BGP routing to each of the cloud router's interfaces.

4) VPC Global Dynamic Routing

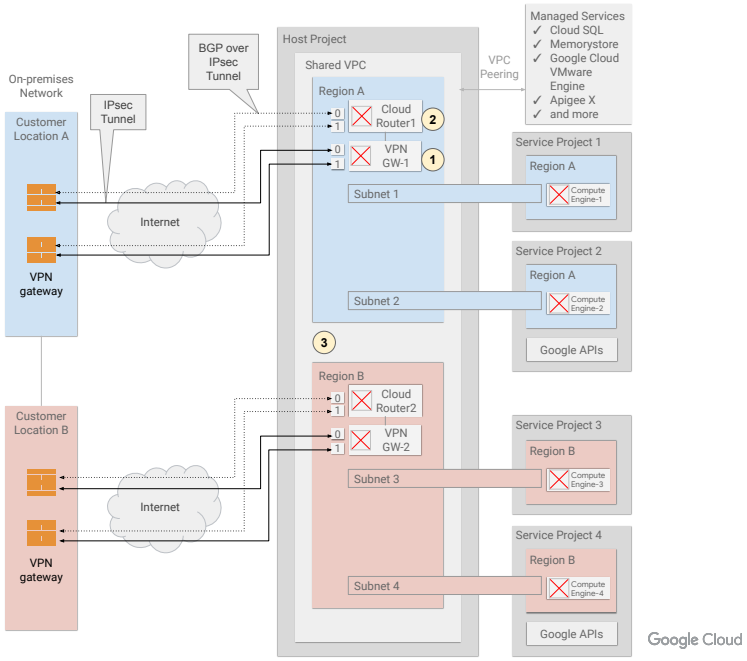
Configure global dynamic routing in the Shared VPC to allow exchange of dynamic routes between all regions.

Abbreviation
EAD = Edge Availability Domain
Metro = Metropolitan Area

Useful links
- Cloud Interconnect FAQ
- Best practices for Cloud Interconnect
- Cloud Interconnect tutorials

A. Hybrid connectivity to single VPC (or Shared VPC)

A3: HA-VPN to on-premises



1) Cloud HA-VPN

The Cloud HA-VPN gateway is used to establish IPsec tunnels to the on-premises VPN gateway over the Internet. HA-VPN offers a 99.99% SLA. You can have multiple HA-VPN tunnels into different regions in the Shared VPC.

2) Cloud Routers

Configure dynamic routing between the on-premises routers and a cloud router in each region. Each cloud router is implemented by two software tasks that provide two interfaces for high availability. Configure BGP routing to each of the cloud router's interfaces.

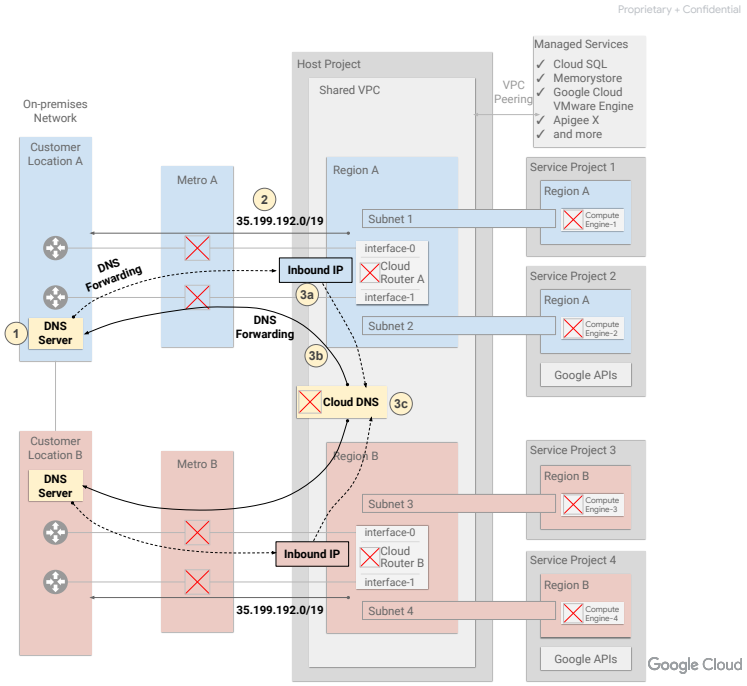
3) VPC Global Dynamic Routing

Configure global dynamic routing in the Shared VPC to allow exchange of dynamic routes between all regions.

Further reading
Best practices for Cloud VPN
Cloud HA-VPN Tutorials

A. Hybrid connectivity to single VPC (or Shared VPC)

A4: DNS



Overview

In a hybrid environment, DNS resolution can be performed in Google Cloud or on-premises. Let's consider a use case where on-premises DNS servers are authoritative for on-premises DNS zones, and Cloud DNS is authoritative for Google Cloud zones.

For more information, refer to the DNS best practice documentation at [Hybrid architecture using a single Shared VPC network].

1) On-premises DNS

Configure your on-premises DNS server to be authoritative for on-premises DNS zones. Configure DNS forwarding (for Google Cloud DNS names) by targeting the Cloud DNS inbound forwarding IP address, which is created via the [Inbound Server Policy] configuration in the Shared VPC. This allows on-premises network to resolve Google Cloud DNS names.

2) Host Project (Shared VPC) - DNS Egress Proxy

Advertise the Google [DNS Egress Proxy] range 35.199.192.0/19 to the on-premises network via the cloud routers. Outbound DNS requests from Google to on-premises

are sourced from this IP address range.

3) Host Project (Shared VPC) - Cloud DNS

a. Configure an Inbound Server Policy for inbound DNS requests from on-premises.

b. Configure DNS forwarding zone (for on-premises DNS zones) targeting the on-premises DNS resolvers.

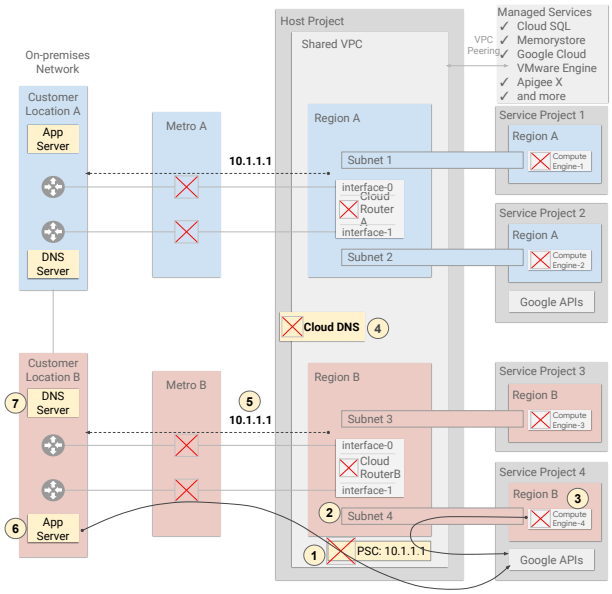
c. Configure DNS Private Zones in the ***Host Project*** and attach ***Shared VPC*** to the zone. This allows hosts (on-premises and all service projects) to resolve the Prod DNS names.

Abbreviation
Metro = Metropolitan Area

Useful links
DNS - Hybrid architecture using a single Shared VPC network
Cloud DNS - Forwarding Targets Selection

A. Hybrid Connectivity to Single VPC (or Shared VPC)

A5: Private Service Connect (PSC) for Google APIs



Access to all supported APIs and services

Overview

You can use Private Service Connect (PSC) to access all supported Google APIs and services from Compute Engine hosts and on-premises hosts; using the internal IP address of a PSC endpoint in the Shared VPC. Let's consider PSC access to a service in ***Service Project 4*** via the Shared VPC.

Create a PSC Endpoint

1)Choose a PSC endpoint address (for example,10.1.1.1) and create a PSC endpoint in the Shared VPC with a target of **"all-apis"**- which gives access to all supported Google APIs and services. Service Directory automatically creates a DNS record (with DNS name of **p.googleapis.com**) linked to the PSC endpoint IP address.

Access from Compute Engine Hosts

Compute Engine-4 host in ***Service Project 4*** can access all supported Google APIs and services via the PSC endpoint in the Shared VPC. Read more about using an endpoint.

2)Enable Private Google Access on all subnets with compute instances that require access to Google APIs via PSC.

3)If your Compute Engine clients can use custom DNS names (for example,

1)**storage-xyz.p**.googlepapis.com), you can use the auto-created **p.googleapis.com** DNS name. Read more about using p.googleapis.com DNS names.

2)If your Compute Engine clients cannot use custom DNS names, you can create Cloud DNS records using the default DNS names (for example,**storage**.googleapis.com). Read more about creating DNS records using default DNS names.

Access from On-premises Hosts

On-premises hosts can access all supported Google APIs and services via the PSC endpoint in the Shared VPC. Read more about using Private Service Connect from on-premises hosts.

5)Advertise the PSC endpoint address to the on-premises network.

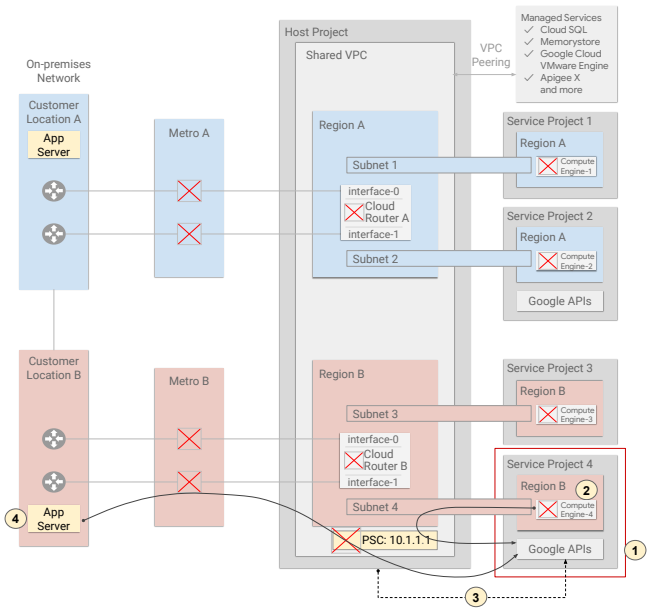
6)If your on-premises clients can use custom DNS names (for example, **storage-xyz.p.**googlepapis.com), you can create A records mapping the custom DNS names to the PSC endpoint address.

7)If your on-premises clients cannot use custom DNS names, you can create A records mapping the default DNS names (for example,**storage.**googleapis.com) to the PSC endpoint address.

Abbreviation
Metro = Metropolitan Area
PSC = Private Service Connect

A. Hybrid connectivity to single VPC (or Shared VPC)

A7: VPC Service Control



Overview

You can use Private Service Connect (PSC) to access all supported secure Google APIs and services from Compute Engine hosts and on-premises hosts; using the internal IP address of a PSC endpoint in the Shared VPC. Let's consider PSC access to a service in ***Service Project 4*** via the Shared VPC.

Create a PSC endpoint

1) Choose a PSC endpoint address (for example, 10.1.1.1) and create a PSC endpoint in the Shared VPC with a target of **"vpc-sc"**- which gives access to Google APIs and services that are supported under VPC Service Control. Service Directory automatically creates a DNS record (with DNS name of **p.googleapis.com**) linked to the PSC endpoint IP address.

Access from Compute Engine hosts

Compute Engine-4 host in ***Service Project 4*** can access (VPC service control) supported Google APIs and services via the PSC endpoint in the Shared VPC. Read more about using an endpoint.

2) Enable Private Google Access on all subnets with compute instances that require access to Google APIs via PSC.

1) If your Compute Engine clients can use custom DNS names (for example, **storage-xyz.p**.googlepapis.com), you can use the auto-created **p.googleapis.com** DNS name. Read more about using p.googleapis.com DNS names.

2) If your Compute Engine clients cannot use custom DNS names, you can create Cloud DNS records using the default DNS names (for example, **storage**.googleapis.com). Read more about creating DNS records using default DNS names.

Access from on-premises hosts

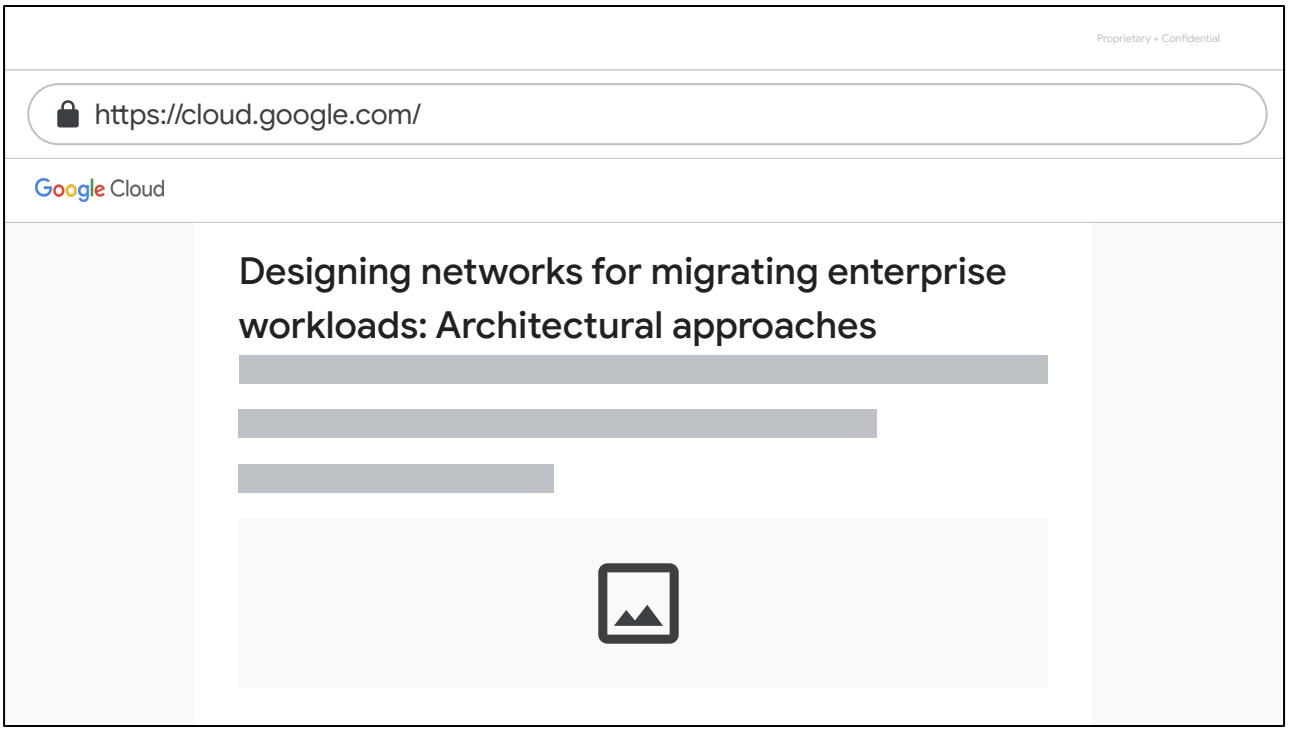
On-premises hosts can access all secure Google APIs and services via the PSC endpoint in the Shared VPC. Read more about using Private Service Connect from on-premises hosts.

5) Advertise the PSC endpoint address to the on-premises network.

6) If your on-premises clients can use custom DNS names (for example, **storage-xyz.p.**googlepapis.com), you can create A records mapping the custom DNS names to the PSC endpoint address.

7) If your on-premises clients cannot use custom DNS names, you can create A records mapping the default DNS names (for example, **storage.**googleapis.com) to the PSC endpoint address.

Abbreviation
Metro = Metropolitan Area
PSC = Private Service Connect



For more information about network design, visit the Cloud Architecture Center and access the documentation titled ‘Designing networks for migrating enterprise workloads: Architectural approaches’.

Congratulations. You have completed the Advanced Logging and Analysis module.