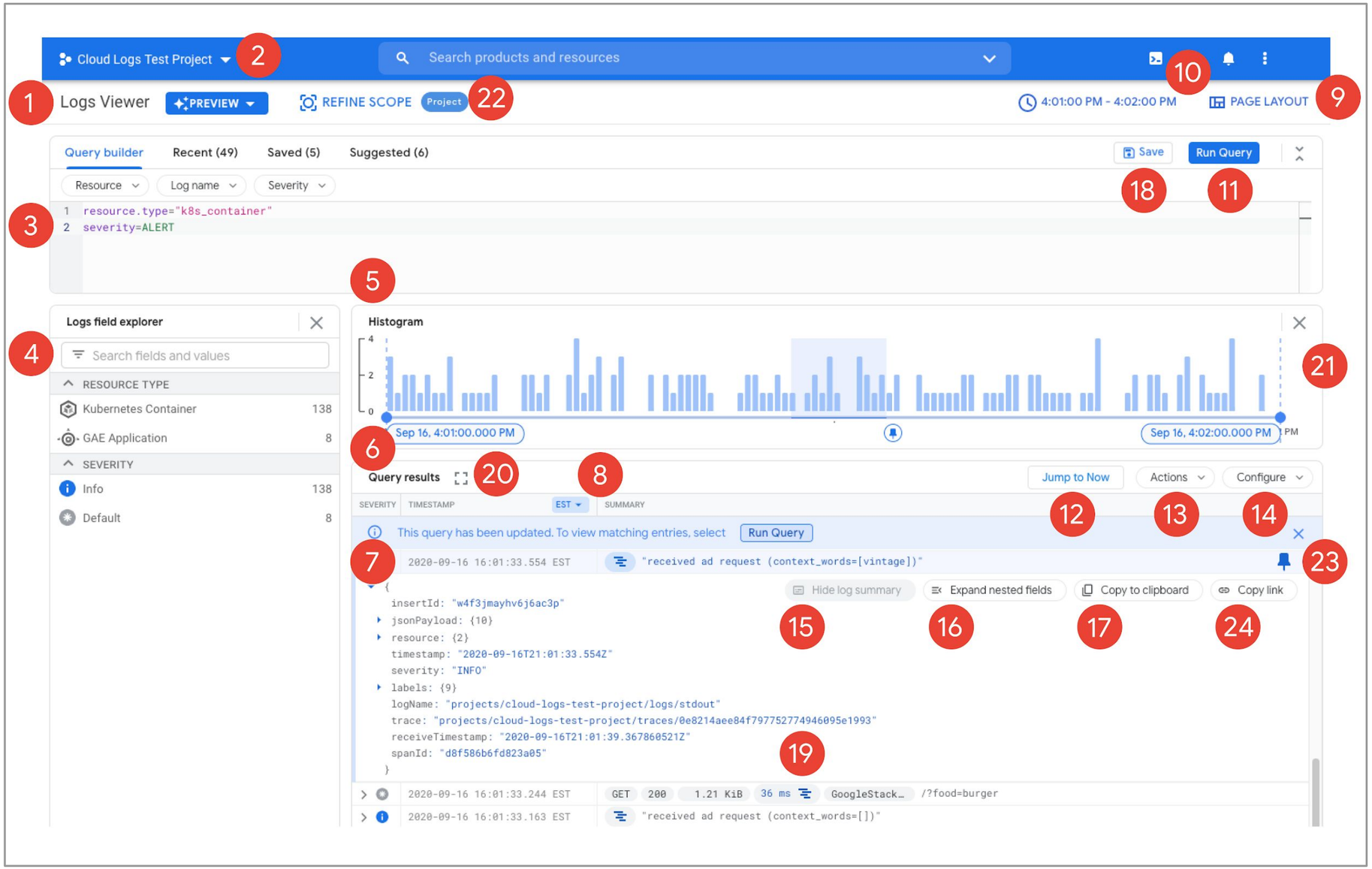
Advanced Logging and Analysis

The following course materials are copyright protected materials.

They may not be reproduced or distributed and may only be used by students attending this Google Cloud Partner Learning Services program.

Logs Viewer



Google Cloud

Entries are returned as LogEntry objects

Query results

Jump to Now | Actions | Configure

SEVERITY	TIMESTAMP (CDT)	SUMMARY
	2020-09-16 11:49:38.815 CDT	run.googleapis.com google.cloud.run.v1.Services.CreateService namespaces/velossandbox/services/demo patrick.haggerty@roitraining.com audit_log, method: "google.cloud.run.v1.Services.CreateService", principal_email: "patrick.haggerty@roitraining.com"

Hide log summary | Collapse nested fields | Copy to clipboard | Copy link


```
{
 protoPayload: {
  @type: "type.googleapis.com/google.cloud.audit.AuditLog"
  authenticationInfo: {
   principalEmail: "patrick.haggerty@roitraining.com"
  }
  requestMetadata: {
   callerIp: "72.24.18.24"
   callerSuppliedUserAgent:
   "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36,gzip(gfe),gzip(gfe)"
   requestAttributes: {
    time: "2020-09-16T16:49:39.035111Z"
    auth: {0}
   }
   destinationAttributes: {0}
  }
  serviceName: "run.googleapis.com"
  methodName: "google.cloud.run.v1.Services.CreateService"
  authorizationInfo: [
   0: {
    resource: "namespaces/velossandbox/services/demo"
    permission: "run.services.create"
    granted: true
    resourceAttributes: {0}
   }
  ]
  resourceName: "namespaces/velossandbox/services/demo"
  request: {
   service: {
    apiVersion: "serving.knative.dev/v1"
    kind: "Service"
```

Primary log fields

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)

Ultimately, it's the query that selects the entries

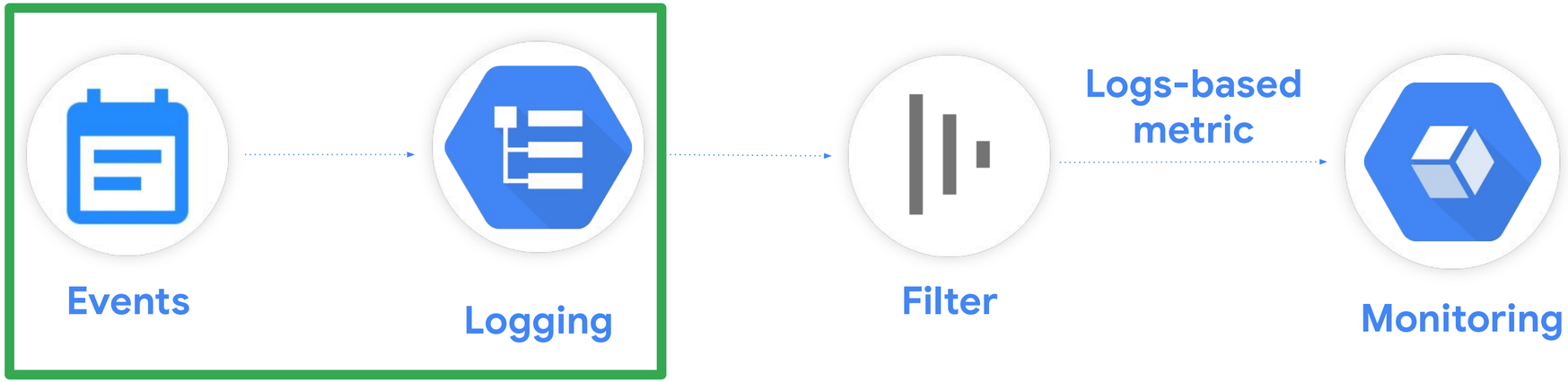
- Start with what you know about the entry you're trying to find
- If it belongs to a resource, a particular log file, or has a known severity, use the query builder drop-down menus

Using the query builder drop-down menu

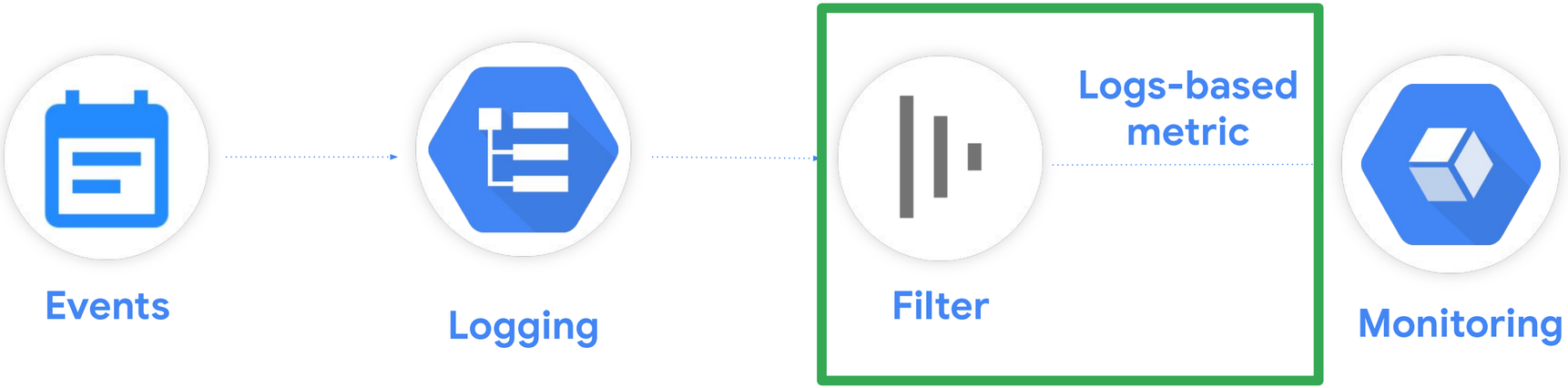
Key access control roles

- Logging/Logs Configuration Writer
  - List, create, get, update, and delete logs-based metrics
- Logging/Logs Viewer
  - View existing logs
- Monitoring Viewer
  - Read the time series in logs-based metrics
- Logging Admin, Editor, and Owner
  - Broad-level roles that can create logs-based metrics

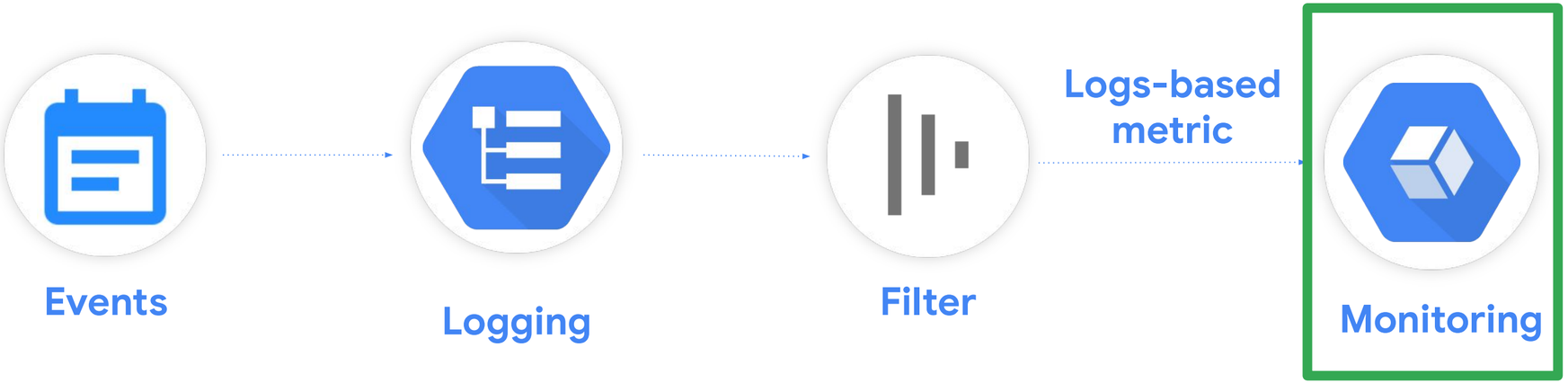
Logs-based metrics



Logs-based metrics



Logs-based metrics



Don’t reinvent the wheel!

- Google has a curated list of over 1,000 predefined metrics
  - Check there first!
- After that, can metrics be created from application logs?
  - Logs-based metrics
- Only create custom metrics when it makes sense
  - Remember, they are also charged differently

Logs-based metrics

Google Cloud Platform | patrick-haggerty

Stackdriver Logging

- Logs Viewer
- Logs-based metrics
- Logs Router
- Resource usage

Logs-based metrics

CREATE METRIC | DELETE

System Metrics

Predefined logs-based system metrics for your project. These metrics record the number of events that occurred within a specific time period.

Name	Description
billing/bytes_ingested	The total number of billable bytes received in log entries.
billing/monthly_bytes_ingested	The total number of billable bytes received in log entries since the start of the month.
byte_count	The total number of bytes received in log entries.
excluded_byte_count	The total number of bytes excluded from log entries
excluded_log_entry_count	The total number of log entries that were not counted because they are being excluded by a resource type exclusion or an exclusion filter.
exports/byte_count	The total number of bytes exported using sinks.
exports/error_count	The total number of log entries that were not exported due to errors.
exports/log_entry_count	The total number of log entries that were exported using sinks.
log_entry_count	The total number of log entries received.
logs_based_metrics_error_count	The total number of log entries that were not counted due to their timestamp being too old.
metric_throttled	The throttling status for logs-based metrics.
time_series_count	The estimated number of active time series for logs-based metrics.

User-defined Metrics

User defined logs-based metrics that count the number of log entries that match a given filter.

Filter Metrics

Name	Type	Description	Previous Month Usage	Usage (MTD)	Filter
user/score-fun	Distribution		0 B	7.89 KiB	resource.type="global"

- Edit metric
- Delete metric
- View logs for metric
- View in Metrics Explorer

Google Cloud

Logs-based metrics

Google Cloud Platform | patrick-haggerty

Stackdriver Logging

- Logs Viewer
- Logs-based metrics
- Logs Router
- Resource usage

Logs-based metrics | CREATE METRIC | DELETE

System Metrics

Predefined logs-based system metrics for your project. These metrics record the number of events that occurred within a specific time period.

Name	Description
billing/bytes_ingested	The total number of billable bytes received in log entries.
billing/monthly_bytes_ingested	The total number of billable bytes received in log entries since the start of the month.
byte_count	The total number of bytes received in log entries.
excluded_byte_count	The total number of bytes excluded from log entries
excluded_log_entry_count	The total number of log entries that were not counted because they are being excluded by a resource type exclusion or an exclusion filter.
exports/byte_count	The total number of bytes exported using sinks.
exports/error_count	The total number of log entries that were not exported due to errors.
exports/log_entry_count	The total number of log entries that were exported using sinks.
log_entry_count	The total number of log entries received.
logs_based_metrics_error_count	The total number of log entries that were not counted due to their timestamp being too old.
metric_throttled	The throttling status for logs-based metrics.
time_series_count	The estimated number of active time series for logs-based metrics.

User-defined Metrics

User defined logs-based metrics that count the number of log entries that match a given filter.

Filter Metrics

Name	Type	Description	Previous Month Usage	Usage (MTD)	Filter
user/score-fun	Distribution		0 B	7.89 KiB	resource.type="global"

- Edit metric
- Delete metric
- View logs for metric
- View in Metrics Explorer

Google Cloud

Logs-based metrics

Google Cloud Platform | patrick-haggerty

Stackdriver Logging

- Logs Viewer
- Logs-based metrics
- Logs Router
- Resource usage

Logs-based metrics

CREATE METRIC | DELETE

System Metrics

Predefined logs-based system metrics for your project. These metrics record the number of events that occurred within a specific time period.

Name	Description
billing/bytes_ingested	The total number of billable bytes received in log entries.
billing/monthly_bytes_ingested	The total number of billable bytes received in log entries since the start of the month.
byte_count	The total number of bytes received in log entries.
excluded_byte_count	The total number of bytes excluded from log entries
excluded_log_entry_count	The total number of log entries that were not counted because they are being excluded by a resource type exclusion or an exclusion filter.
exports/byte_count	The total number of bytes exported using sinks.
exports/error_count	The total number of log entries that were not exported due to errors.
exports/log_entry_count	The total number of log entries that were exported using sinks.
log_entry_count	The total number of log entries received.
logs_based_metrics_error_count	The total number of log entries that were not counted due to their timestamp being too old.
metric_throttled	The throttling status for logs-based metrics.
time_series_count	The estimated number of active time series for logs-based metrics.

User-defined Metrics

User defined logs-based metrics that count the number of log entries that match a given filter.

Filter Metrics

Name	Type	Description	Previous Month Usage	Usage (MTD)	Filter
user/score-fun	Distribution		0 B	7.89 KiB	resource.type="global"

- Edit metric
- Delete metric
- View logs for metric
- View in Metrics Explorer

Google Cloud

Logs-based metrics

Google Cloud Platform | patrick-haggerty

Stackdriver Logging

- Logs Viewer
- Logs-based metrics
- Logs Router
- Resource usage

Logs-based metrics

CREATE METRIC | DELETE

System Metrics

Predefined logs-based system metrics for your project. These metrics record the number of events that occurred within a specific time period.

Name	Description
billing/bytes_ingested	The total number of billable bytes received in log entries.
billing/monthly_bytes_ingested	The total number of billable bytes received in log entries since the start of the month.
byte_count	The total number of bytes received in log entries.
excluded_byte_count	The total number of bytes excluded from log entries
excluded_log_entry_count	The total number of log entries that were not counted because they are being excluded by a resource type exclusion or an exclusion filter.
exports/byte_count	The total number of bytes exported using sinks.
exports/error_count	The total number of log entries that were not exported due to errors.
exports/log_entry_count	The total number of log entries that were exported using sinks.
log_entry_count	The total number of log entries received.
logs_based_metrics_error_count	The total number of log entries that were not counted due to their timestamp being too old.
metric_throttled	The throttling status for logs-based metrics.
time_series_count	The estimated number of active time series for logs-based metrics.

User-defined Metrics

User defined logs-based metrics that count the number of log entries that match a given filter.

Filter Metrics

Name	Type	Description	Previous Month Usage	Usage (MTD)	Filter
user/score-fun	Distribution		0 B	7.89 KiB	resource.type="global"

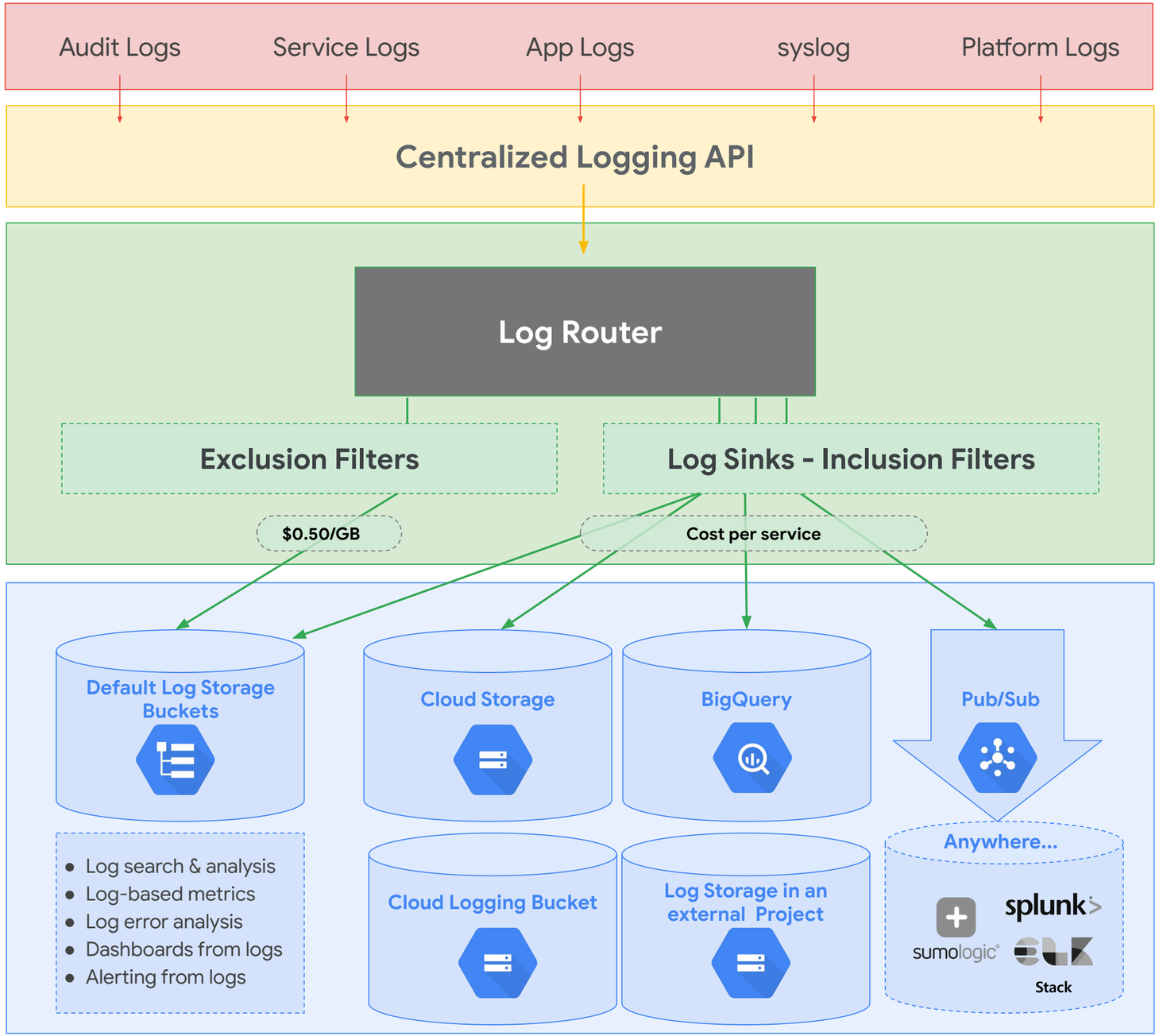
- Edit metric
- Delete metric
- View logs for metric
- View in Metrics Explorer

Google Cloud

Logs-based metric creation flow

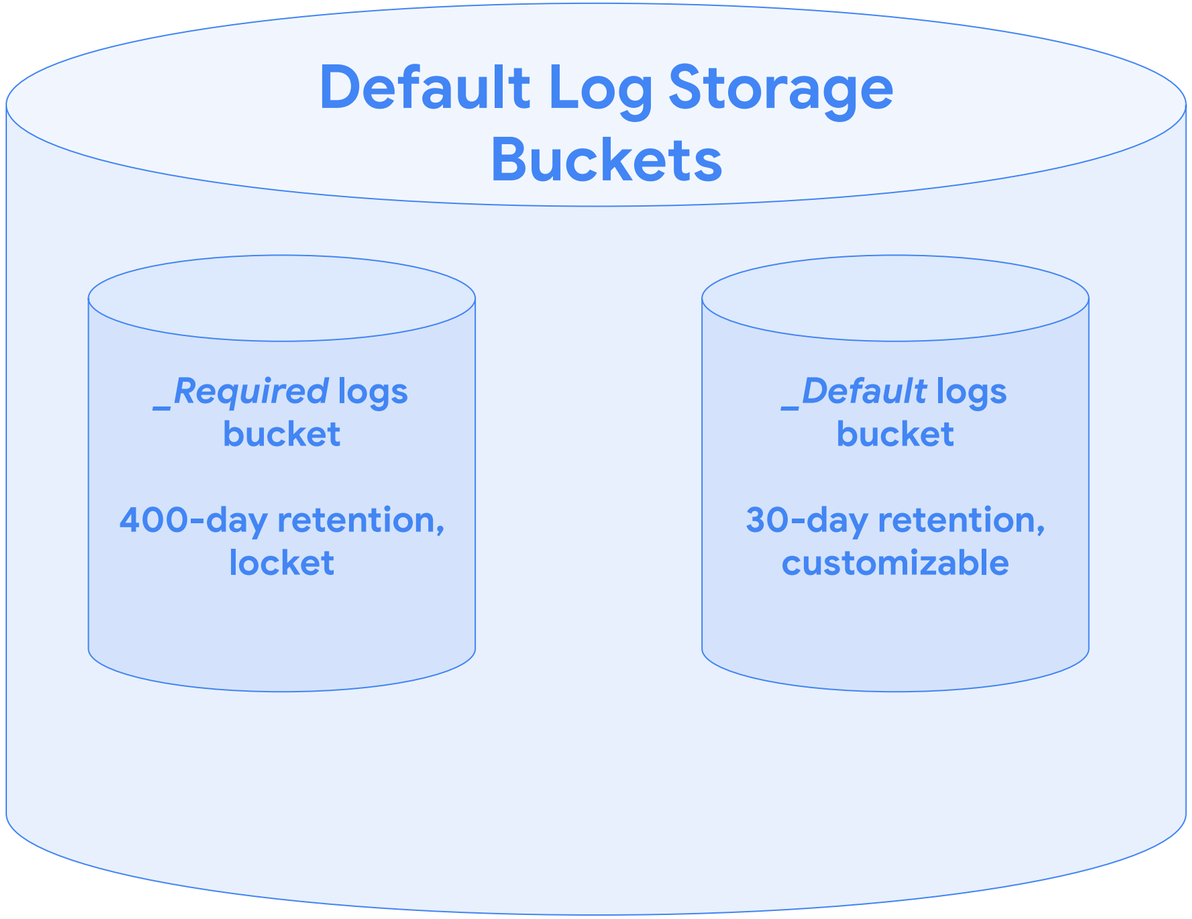
1. Find the log with the requisite data
2. Filter to the required entries
3. Pick a metric type (Counter or Distribution)
4. If Distribution, set configurations
5. Choose any secondary labels

Logging architecture

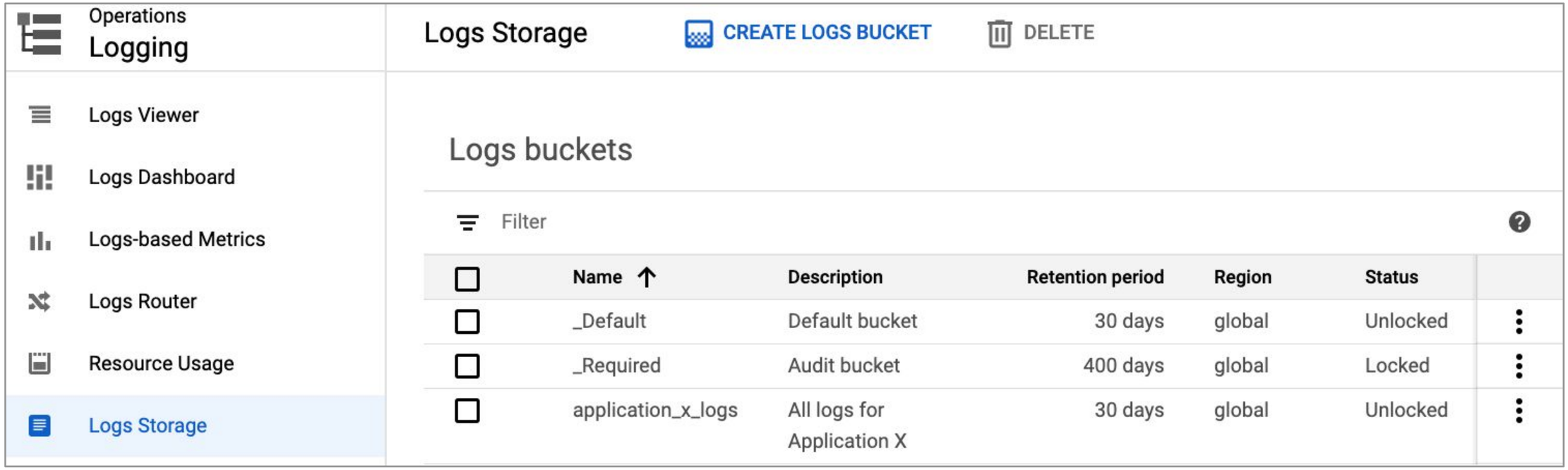


Google Cloud

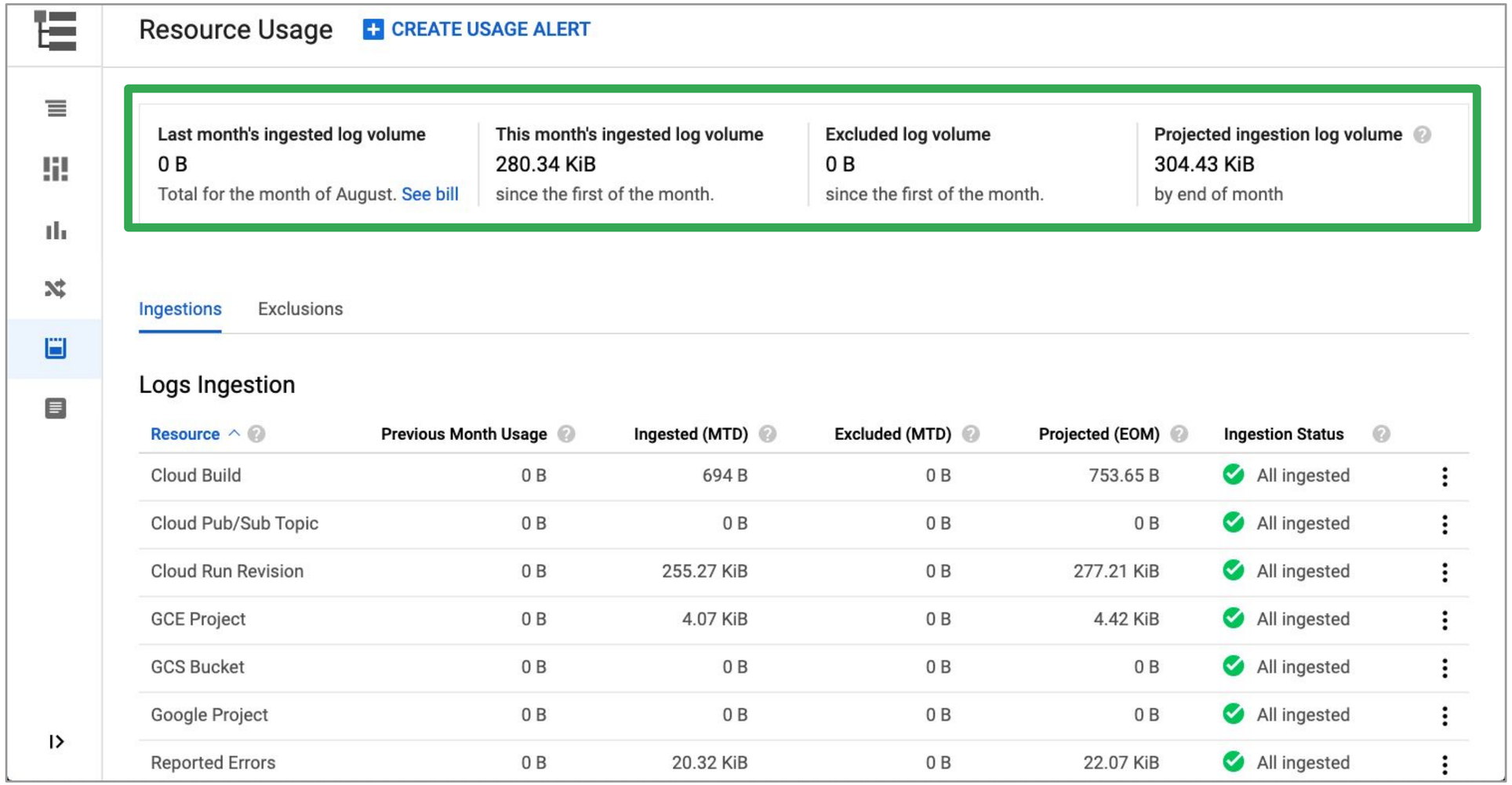
Default logs buckets



Create specialized buckets in current or remote projects:

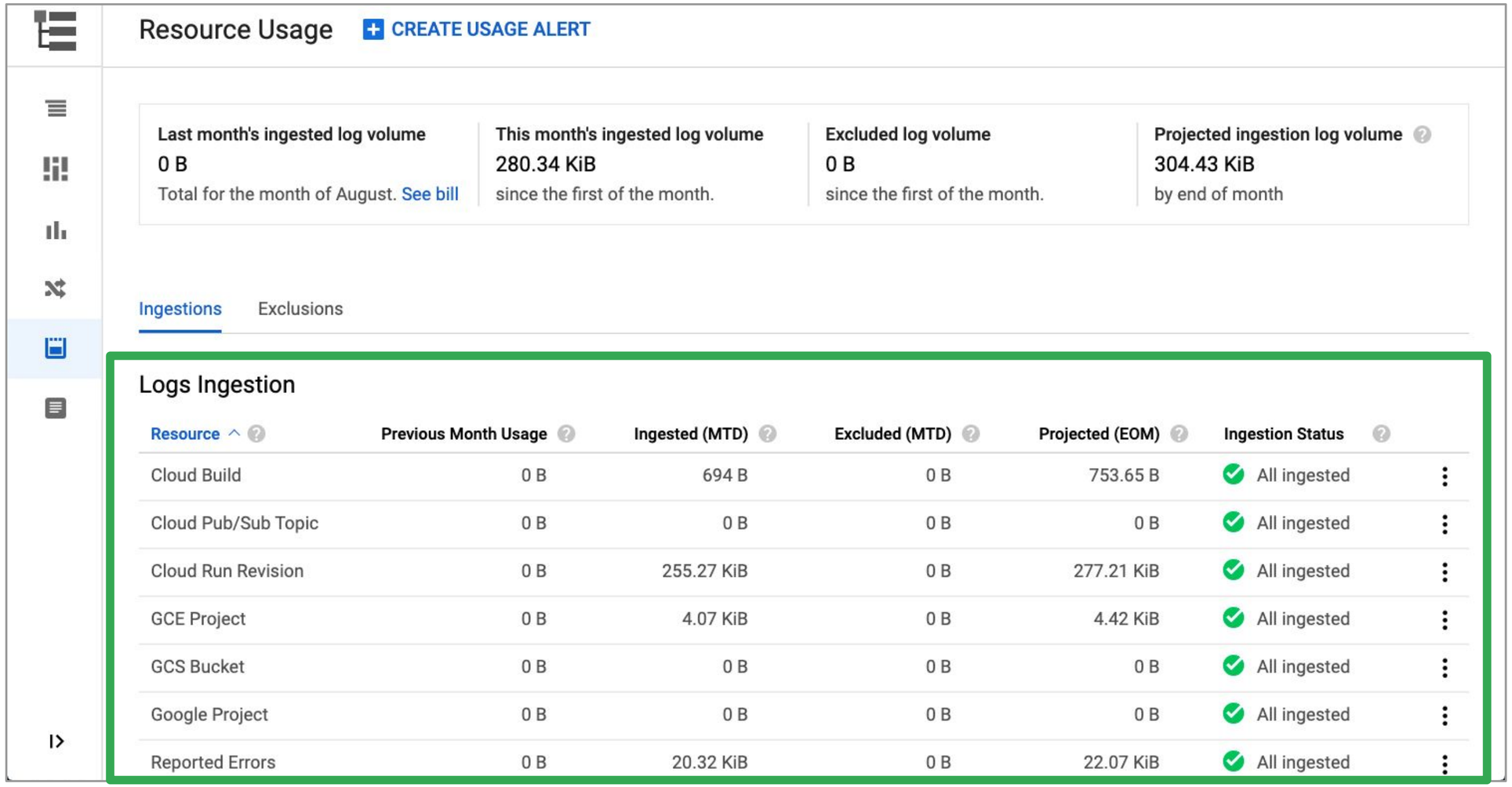


Resource usage



Resource	Previous Month Usage	Ingested (MTD)	Excluded (MTD)	Projected (EOM)	Ingestion Status
Cloud Build	0 B	694 B	0 B	753.65 B	All ingested
Cloud Pub/Sub Topic	0 B	0 B	0 B	0 B	All ingested
Cloud Run Revision	0 B	255.27 KiB	0 B	277.21 KiB	All ingested
GCE Project	0 B	4.07 KiB	0 B	4.42 KiB	All ingested
GCS Bucket	0 B	0 B	0 B	0 B	All ingested
Google Project	0 B	0 B	0 B	0 B	All ingested
Reported Errors	0 B	20.32 KiB	0 B	22.07 KiB	All ingested

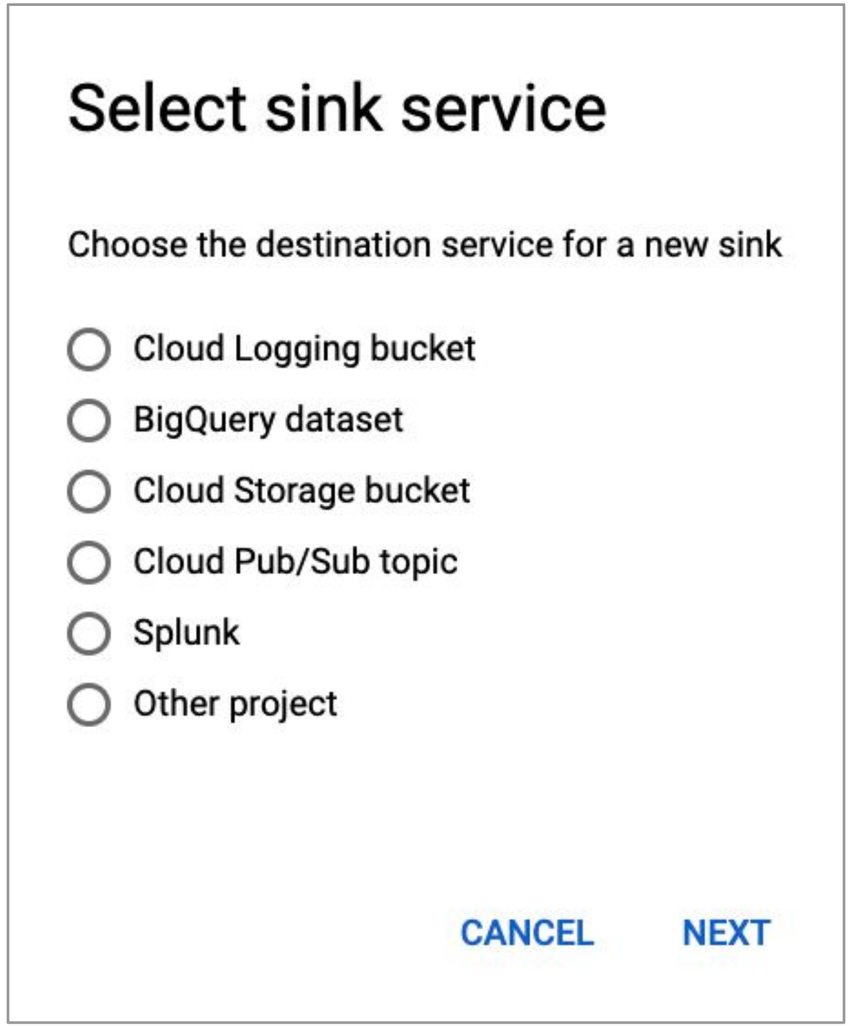
Resource usage



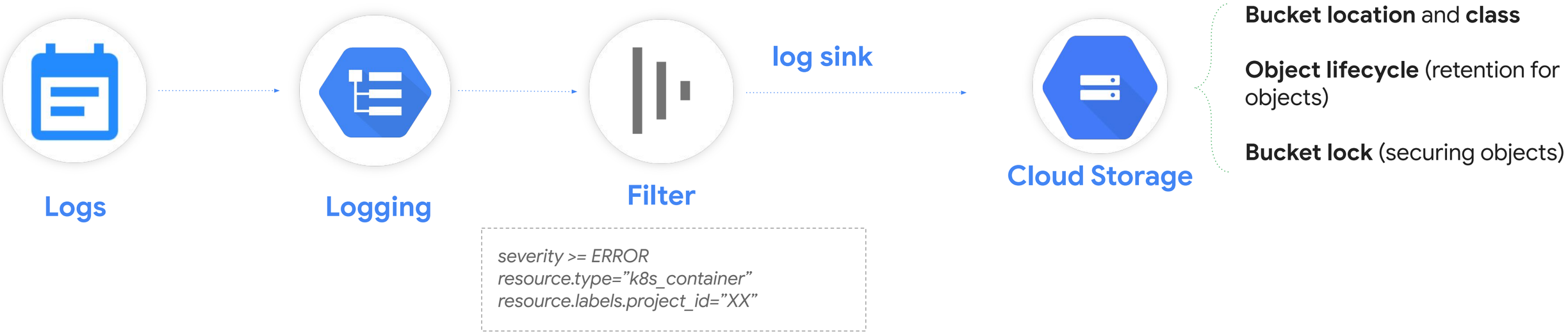
Resource	Previous Month Usage	Ingested (MTD)	Excluded (MTD)	Projected (EOM)	Ingestion Status
Cloud Build	0 B	694 B	0 B	753.65 B	All ingested
Cloud Pub/Sub Topic	0 B	0 B	0 B	0 B	All ingested
Cloud Run Revision	0 B	255.27 KiB	0 B	277.21 KiB	All ingested
GCE Project	0 B	4.07 KiB	0 B	4.42 KiB	All ingested
GCS Bucket	0 B	0 B	0 B	0 B	All ingested
Google Project	0 B	0 B	0 B	0 B	All ingested
Reported Errors	0 B	20.32 KiB	0 B	22.07 KiB	All ingested

Log router sinks

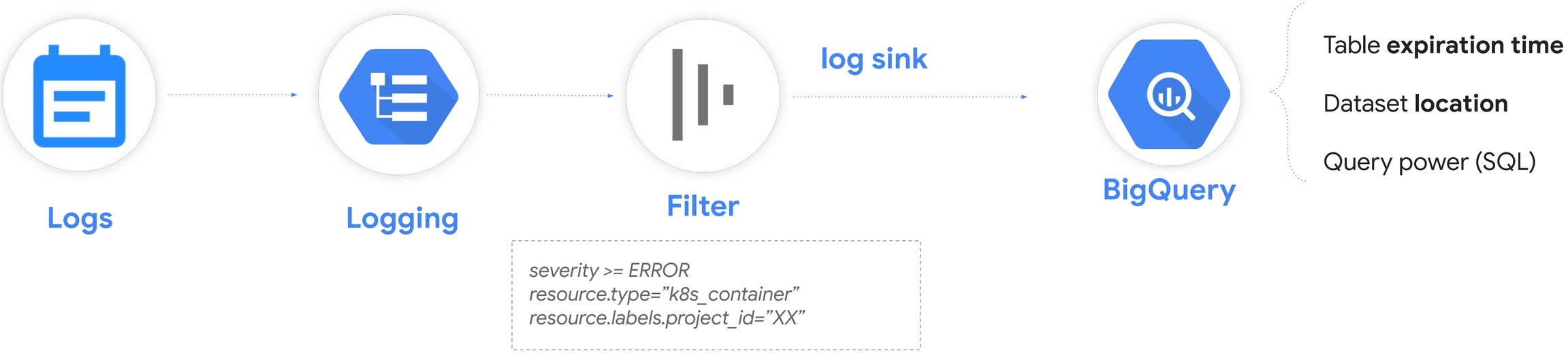
There are several sink locations, depending on need



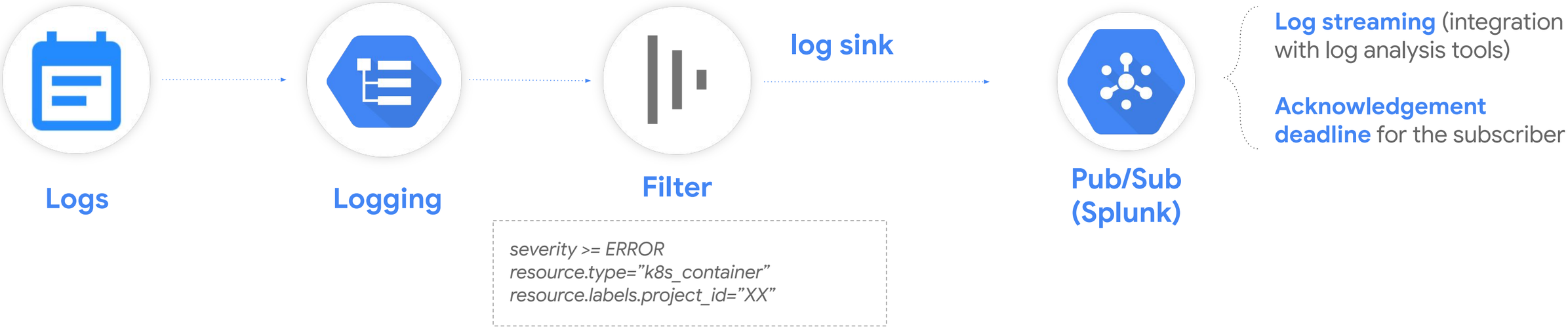
Cloud Storage works well for general storage:



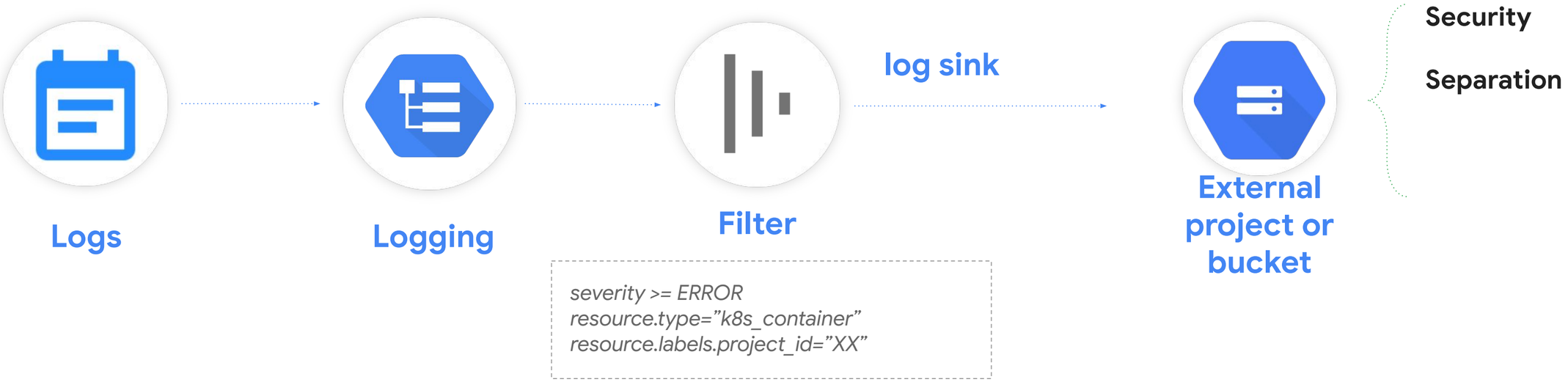
BigQuery for easy warehousing and analysis



Pub/Sub to connect with external systems and applications



Log exports


Logs
Logging
Filter
log sink
External project or bucket
Security
Separation
severity >= ERROR
resource.type="k8s_container"
resource.labels.project_id="XX"

Create a log sink

Google Cloud Platform | patrick-haggerty

Stackdriver Logging

CREATE METRIC | CREATE SINK | SAVE SEARCH | SHOW LIBRARY

- Logs Viewer
- Logs-based Metrics
- Logs Router
- Resource usage

Filter by label or text search

Cloud Run Revision, hello-logging | All logs | Any log level | Last hour | Jump to now

Showing logs from **the last hour** ending at **5:45 PM** (CST) — Download logs | View Options

No older entries found matching current filter in the last hour. Load older logs

```
2020-02-06 17:15:24.200 CST Cloud Run ReplaceService hello-logging …
2020-02-06 17:15:31.554 CST {"textPayload":"","insertId":"5e3c9e13000876b47417acef","resource"…
2020-02-06 17:15:31.554 CST > hello-logging-fun@1.0.0 start /usr/src/app
2020-02-06 17:15:31.554 CST > node index.js
2020-02-06 17:15:31.554 CST {"textPayload":"","insertId":"5e3c9e13000877020ba4e4b6","resource"…
2020-02-06 17:15:36.016 CST Hello world listening on port 8080
```

Edit Sink

Sink Name

Sink Name

Sink Service

Select des

Bigquery
Cloud Storage
Pub/Sub
Custom destination

Sink Destina

Creating a log sink will export future matching logs to the selected destination.

Create Sink | Cancel

Sink created

Export sink **fun_sink** was successfully created.

A unique service account, **p1055281703932-044810@gcp-sa-logging.iam.gserviceaccount.com**, has been created with permissions to write logs to the destination, **bigquery.googleapis.com/projects/patrick-haggerty/datasets/fun_sink_logs**.

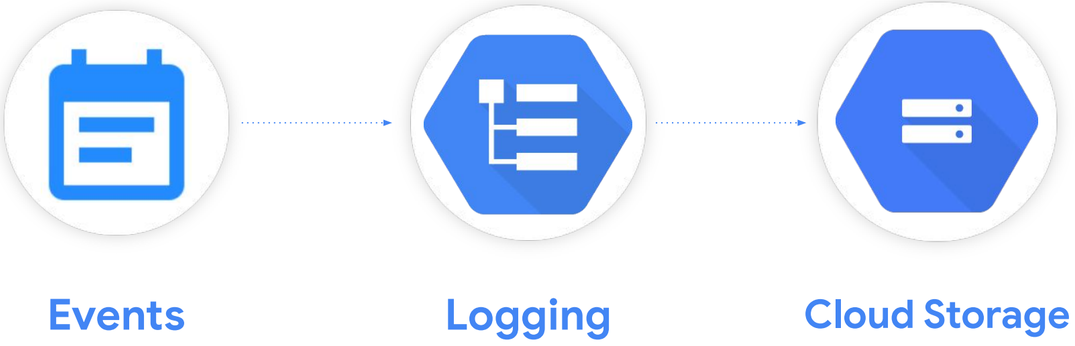
CLOSE

Log archiving and analysis

Example pipeline

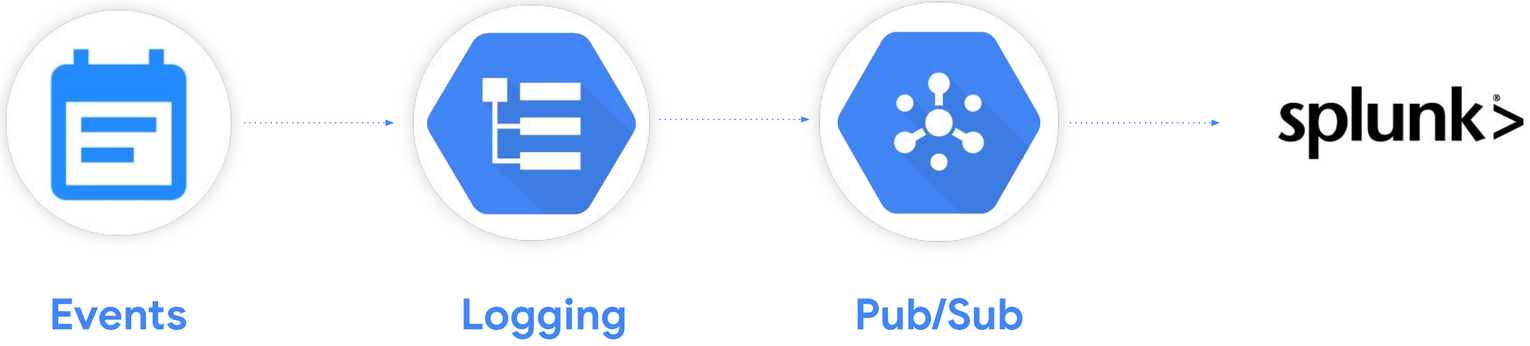
Archive logs for long-term storage

Example pipeline

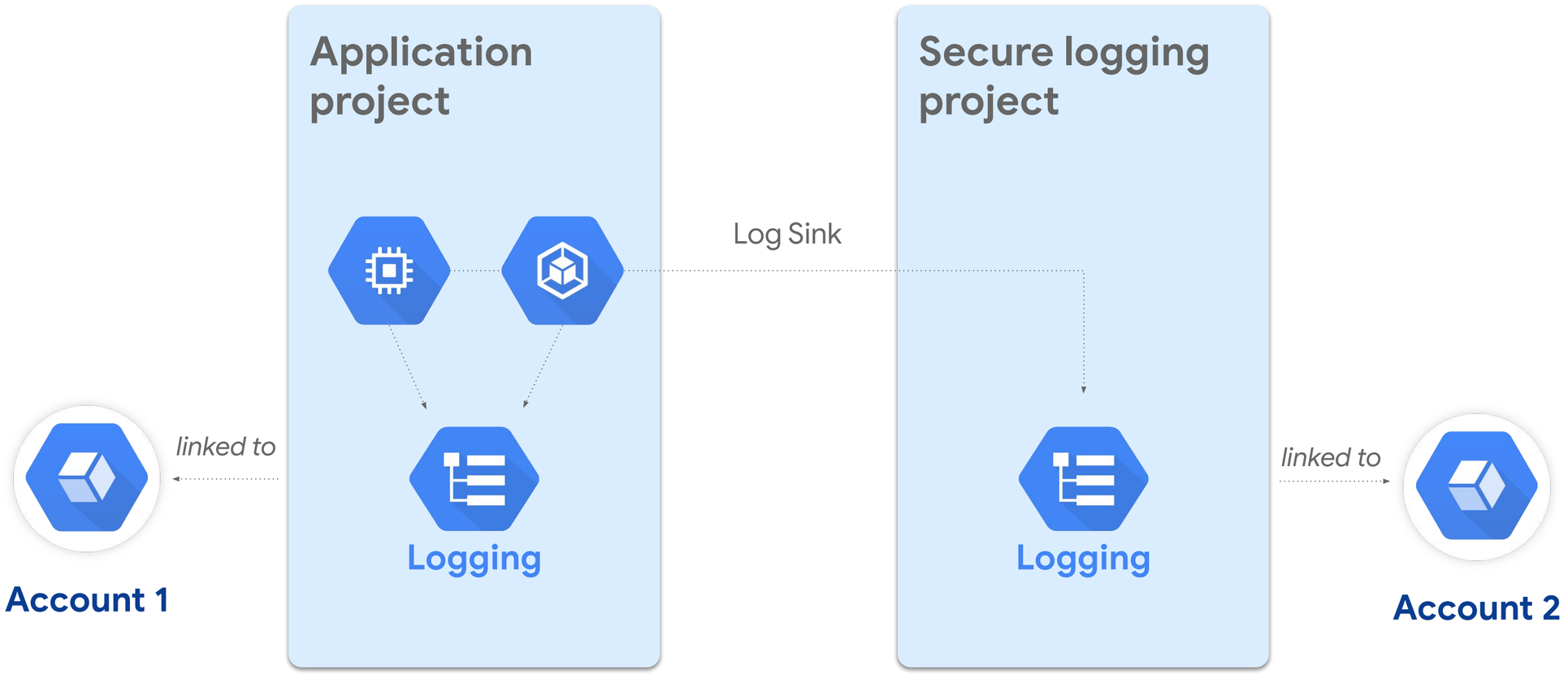


Exporting back to Splunk

Example pipeline



Security logging



Aggregation levels

Project

A **project-level log sink** exports all the logs for a **specific project**.

A **log filter** can be specified in the sink definition to include/exclude certain log types.

Folder

A **folder-level log sink** aggregates logs on the folder level.

You can also include logs from children resources (subfolders, projects).

Organization

An **organization-level log sink** aggregates logs on the organization level.

You can also include logs from children resources (subfolders, projects).

Aggregated sinks

- Export log entries for multiple projects, folders, up to the organization or billing account level

```
gcloud logging sinks create [SINK_NAME] \
storage.googleapis.com/[BUCKET_NAME] --include-children \
--folder=[FOLDER_ID] --log-filter="logName:activity"
```

- `--folder` could also be `--organization` and `--billing-account`
- Need *`Logs Configuration Writer`* IAM role for parent

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

Admin Activity

Record modifications to **configuration** or **metadata**

Retention is **400 days**

Immutable and available at **no charge**

Stored in the **_Required** log storage bucket

“Who added that VM?”

Always enabled

System Event

Record GCP **non-human** admin actions that modify **configurations**

Retention is **400 days**

Immutable and available at **no charge**

Stored in the **_Required** log storage bucket

“Did a live-migration event occur?”

Always enabled

Data Access

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

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

“Who modified that Cloud Storage file?”

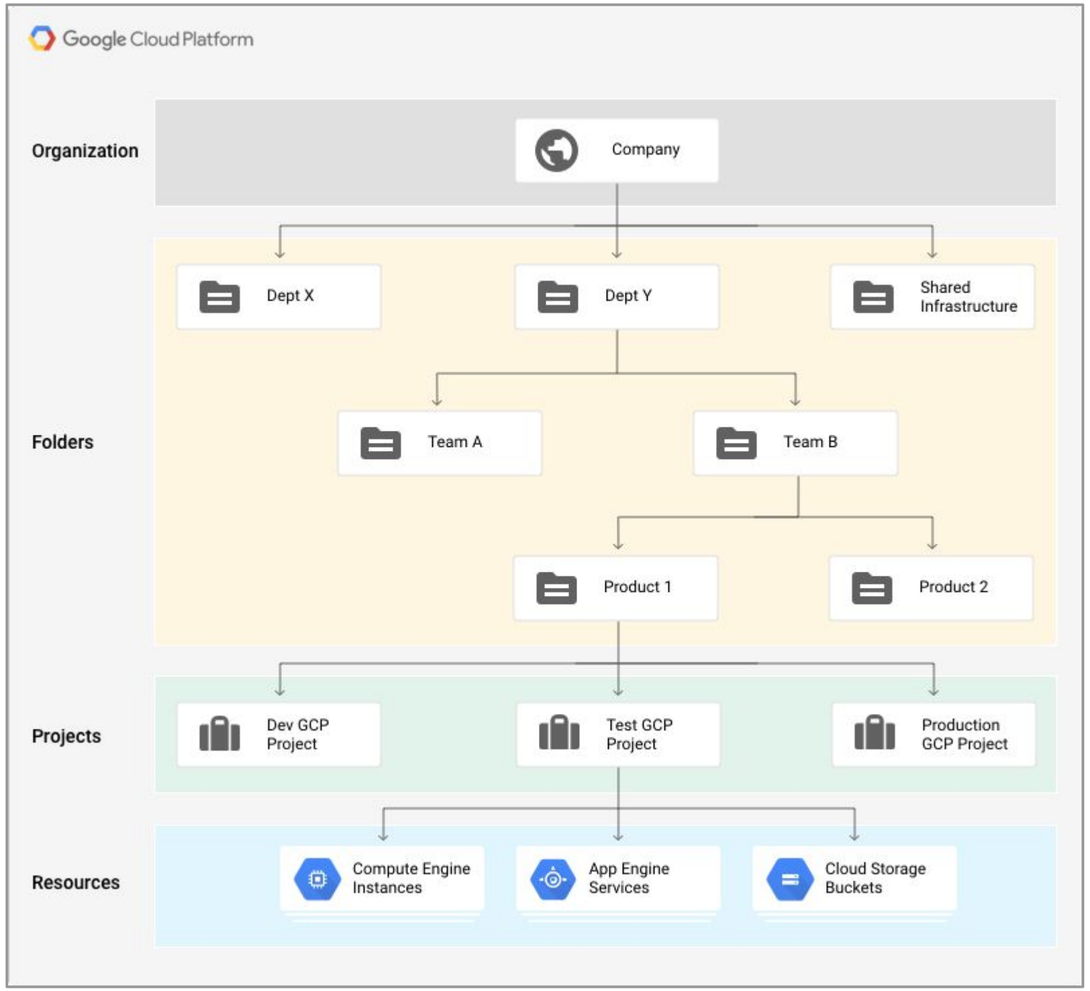
Needs to be enabled

Access Transparency logs

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

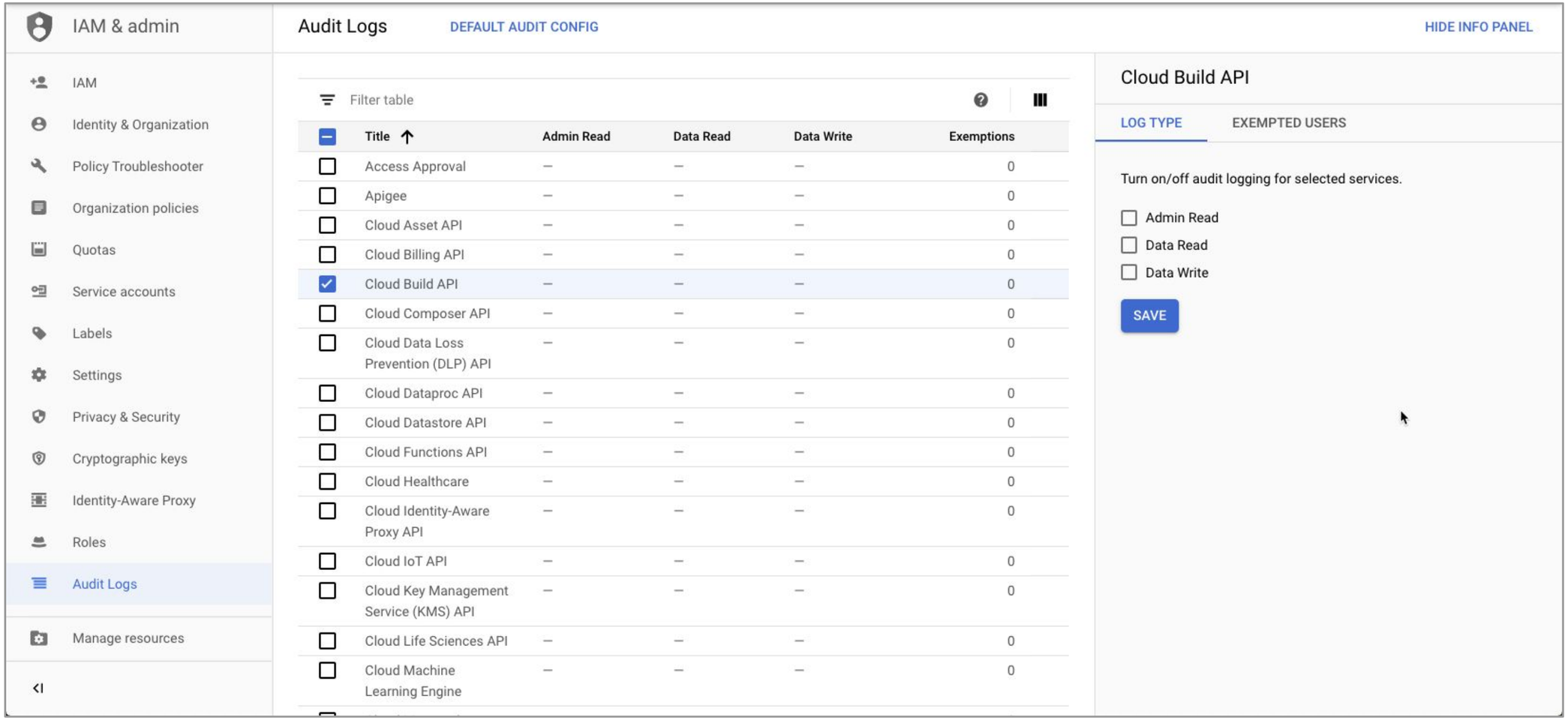
- Logs of accesses
- To Cloud and Apps customer data
- By human Googlers
- Provided to enterprises
- In near real time
- Supports approval and surfaced through App APIs and UIs, Security Command Center

Data Access log enablement scope



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

Enabling Data Access logging per Google Cloud service

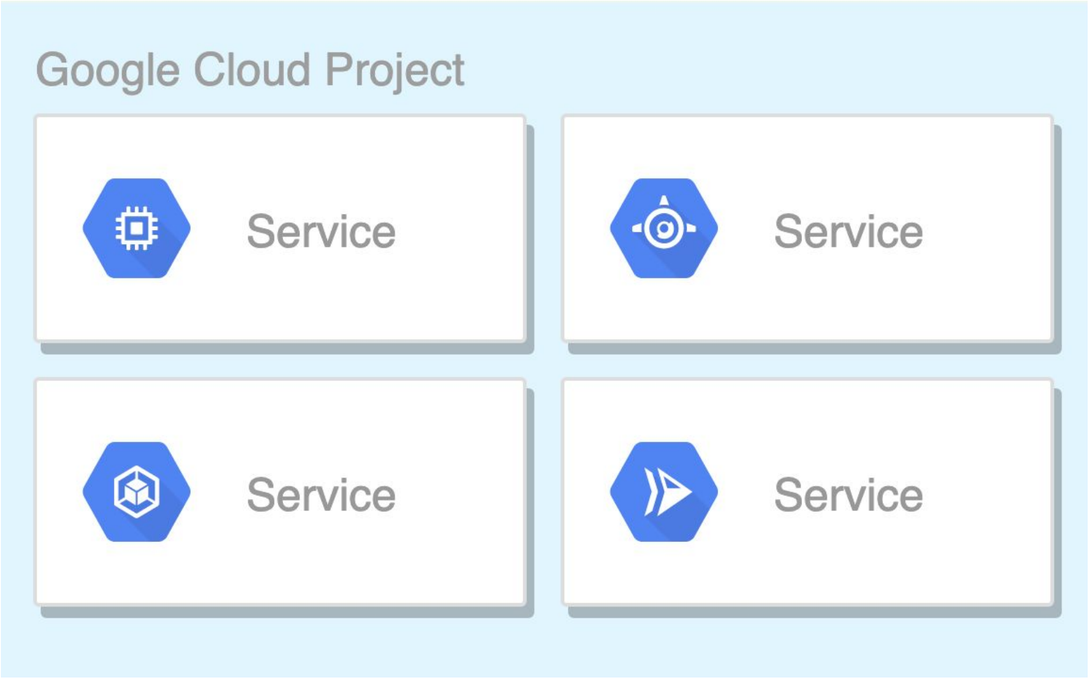


Google Cloud

Working with Audit Logs

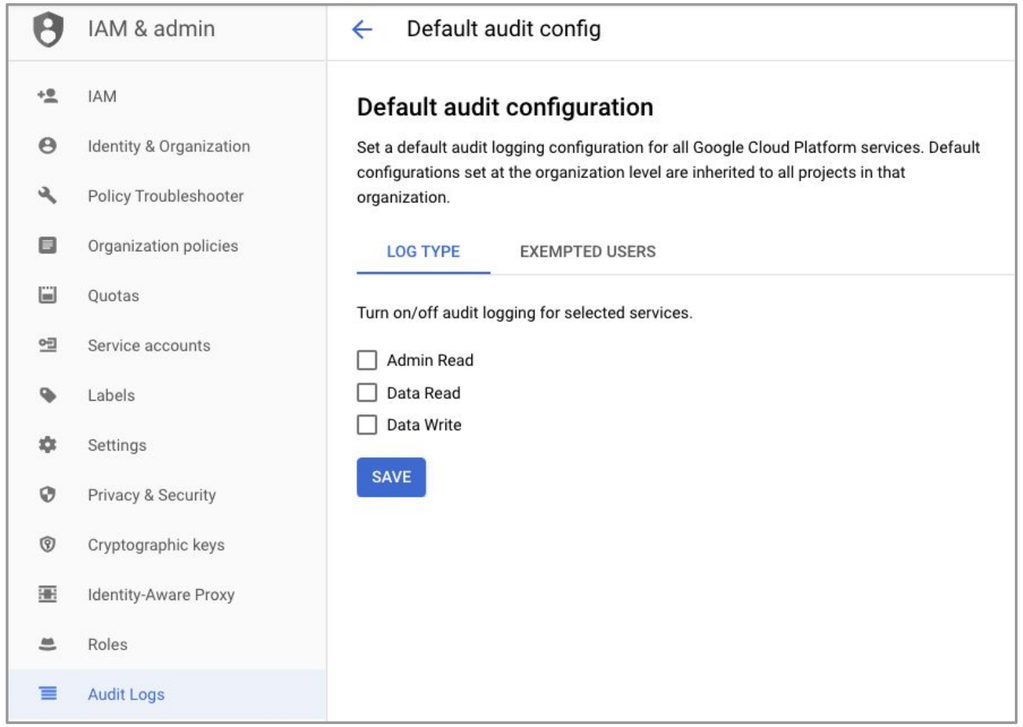
Plan and create test project

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



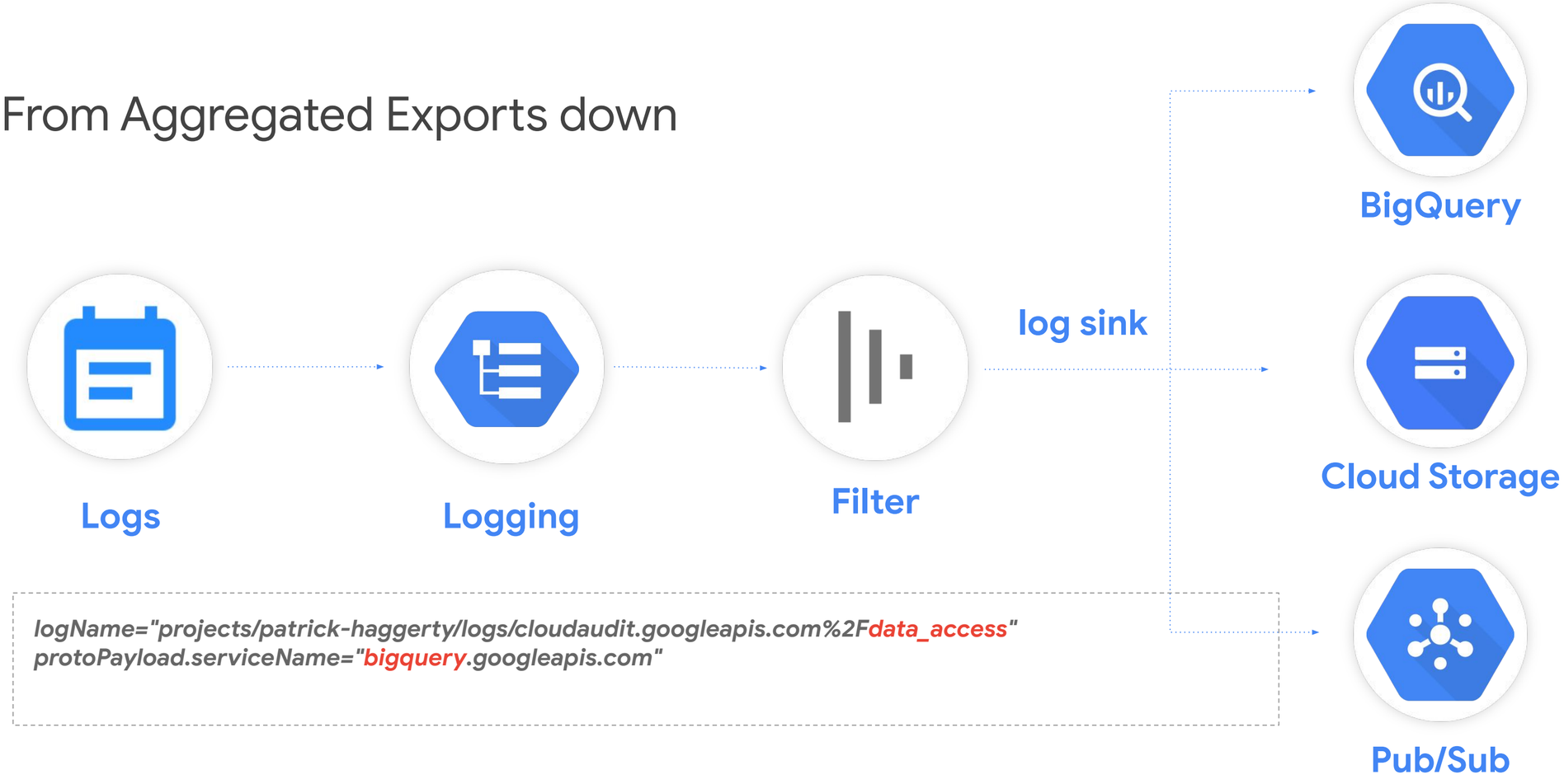
Decide and set org level data access

- 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



Plan and configure exports

- From Aggregated Exports down



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 Google Cloud-based and exported logs
- Data Access logs 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

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: **logging.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

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

Monitoring the Google Cloud VPC

Agenda

VPC Flow Logs

Firewall Rules Logging

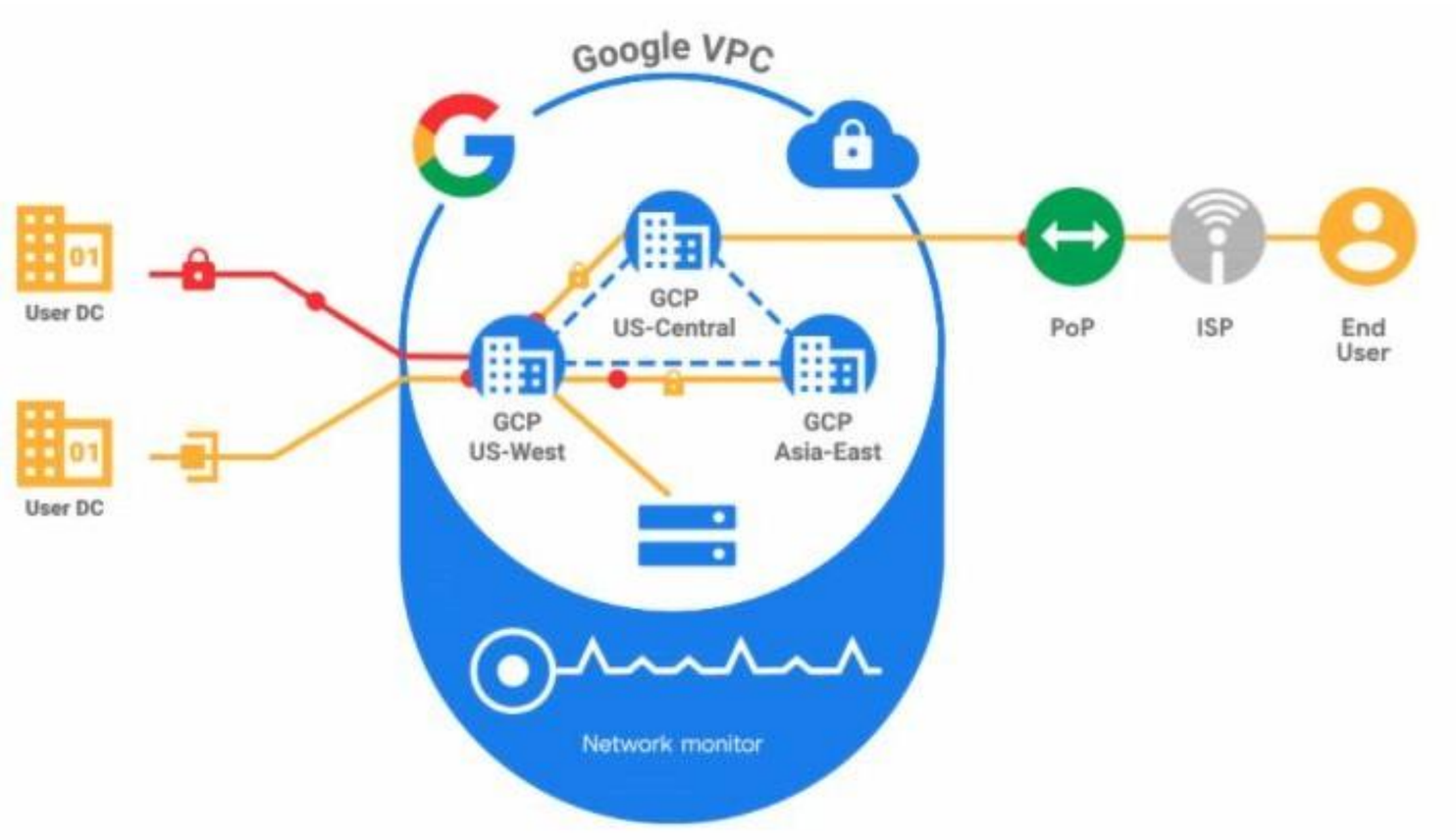
Load Balancer Logs

Cloud NAT Logs

Packet Mirroring

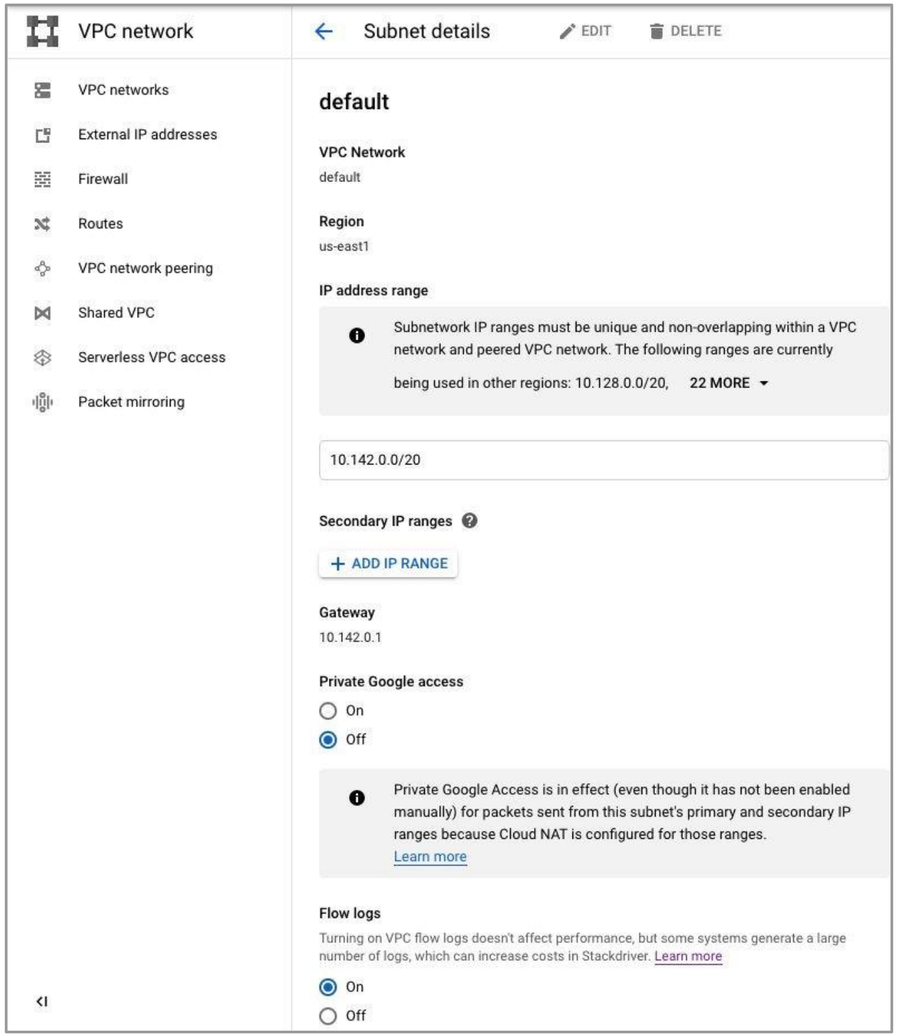
Network Intelligence Center

VPC Flow Logs record a sample of network flows



Enable VPC Flow Logs per VPC subnet

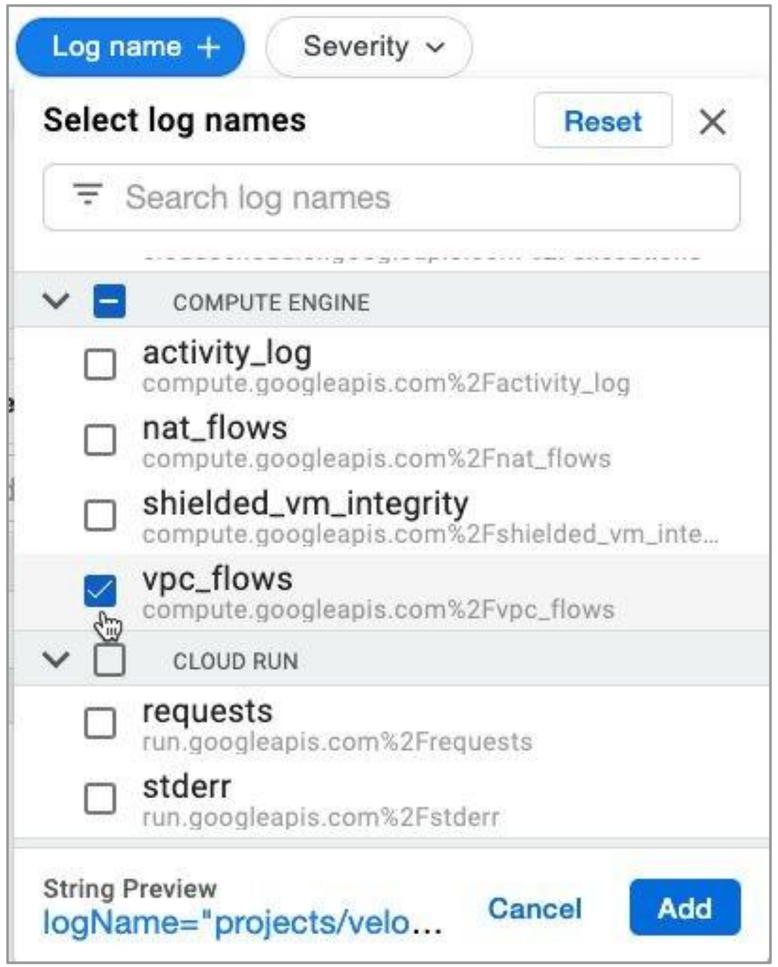
Logging



Google Cloud

Use Logging to review your VPC Flow Logs

Logging



Google Cloud

Analyze logs in BigQuery and visualize in Data Studio

BigQuery

Data Studio

RUN QUERY | Save Query | Save View | Format Query | Show Options

Results | Details | Download as CSV

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

Table | JSON

Firewall Rules Logging

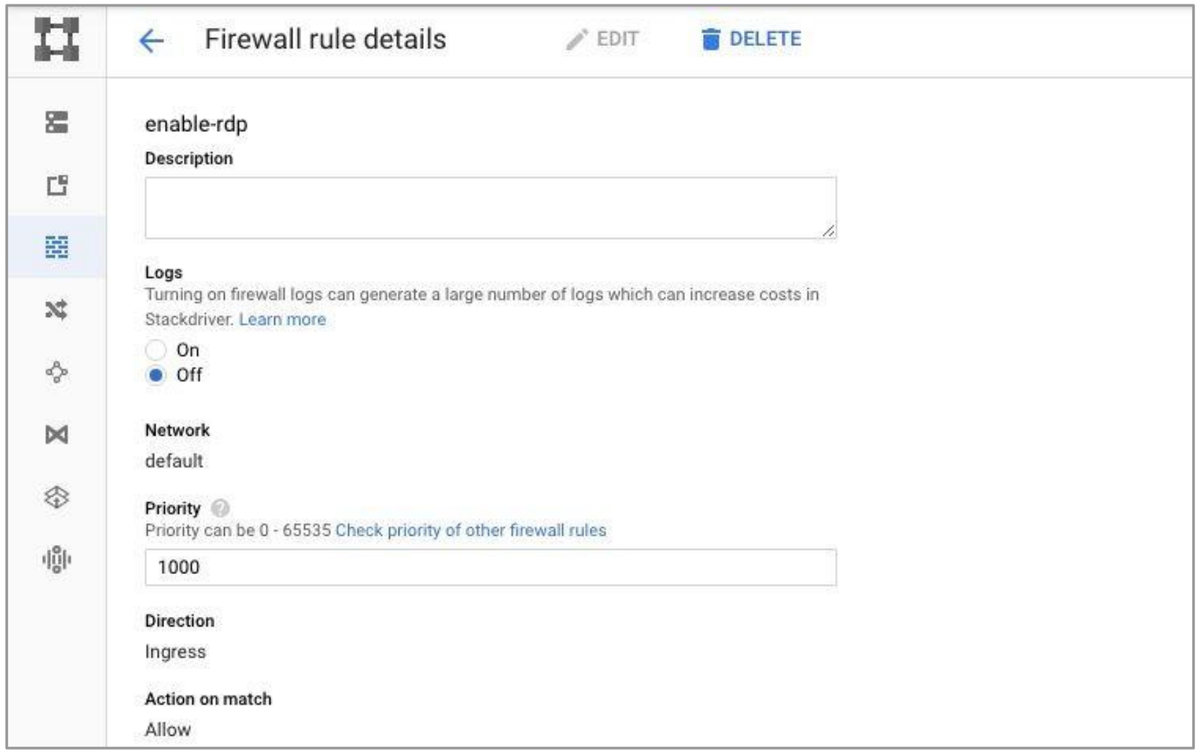
Did my firewall rules cause that application outage?

How many connections match the rule I just created?

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

Enabling Firewall Rules Logging in the console

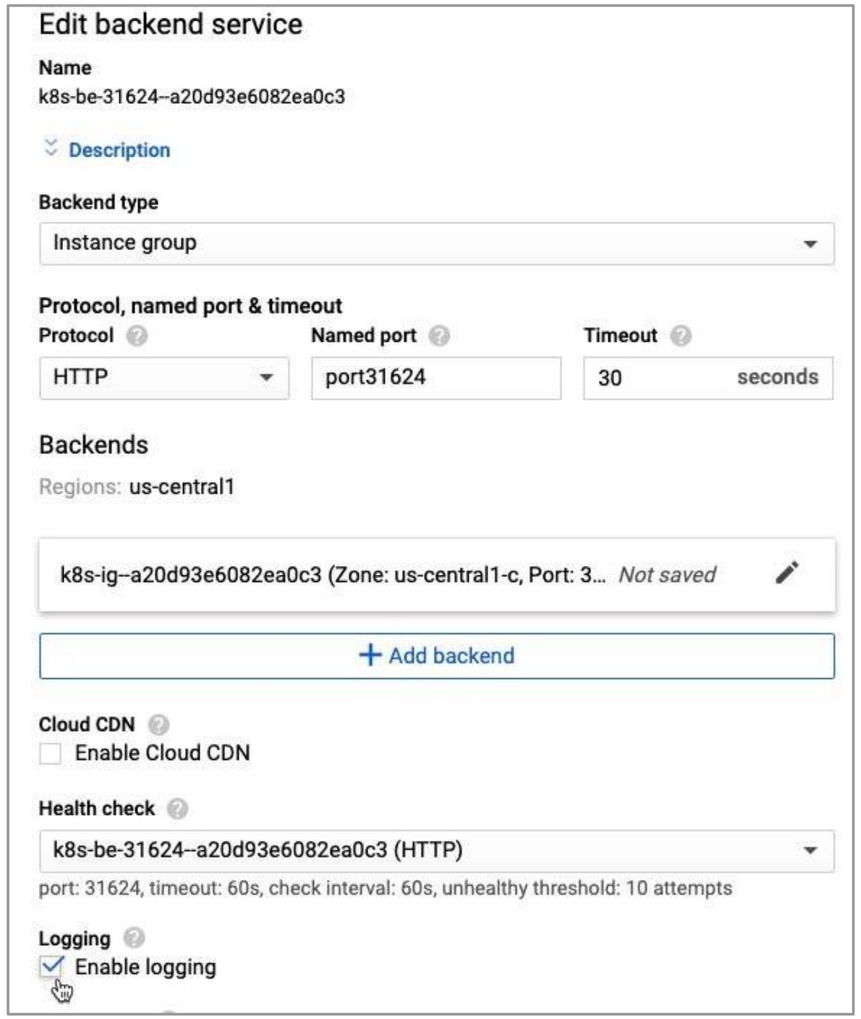
- Firewall Rules Logging is disabled by default
- You enable it on a per-rule basis



The internal and external HTTP(s) load balancers

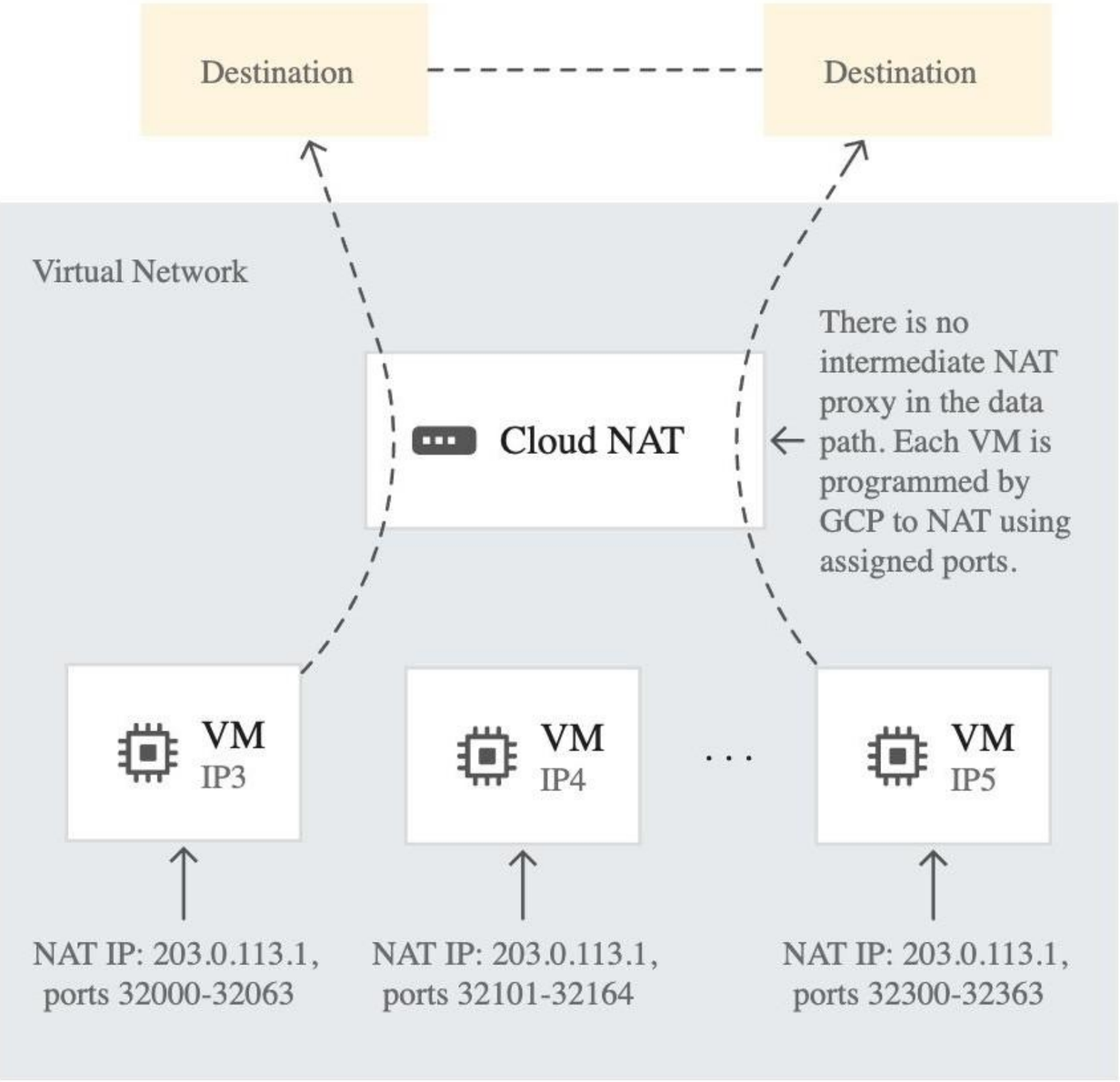
support logging

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



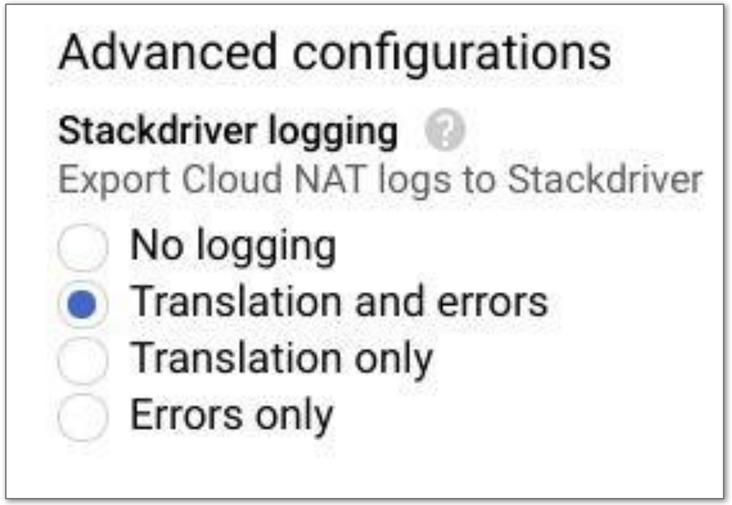
Cloud NAT overview

- 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



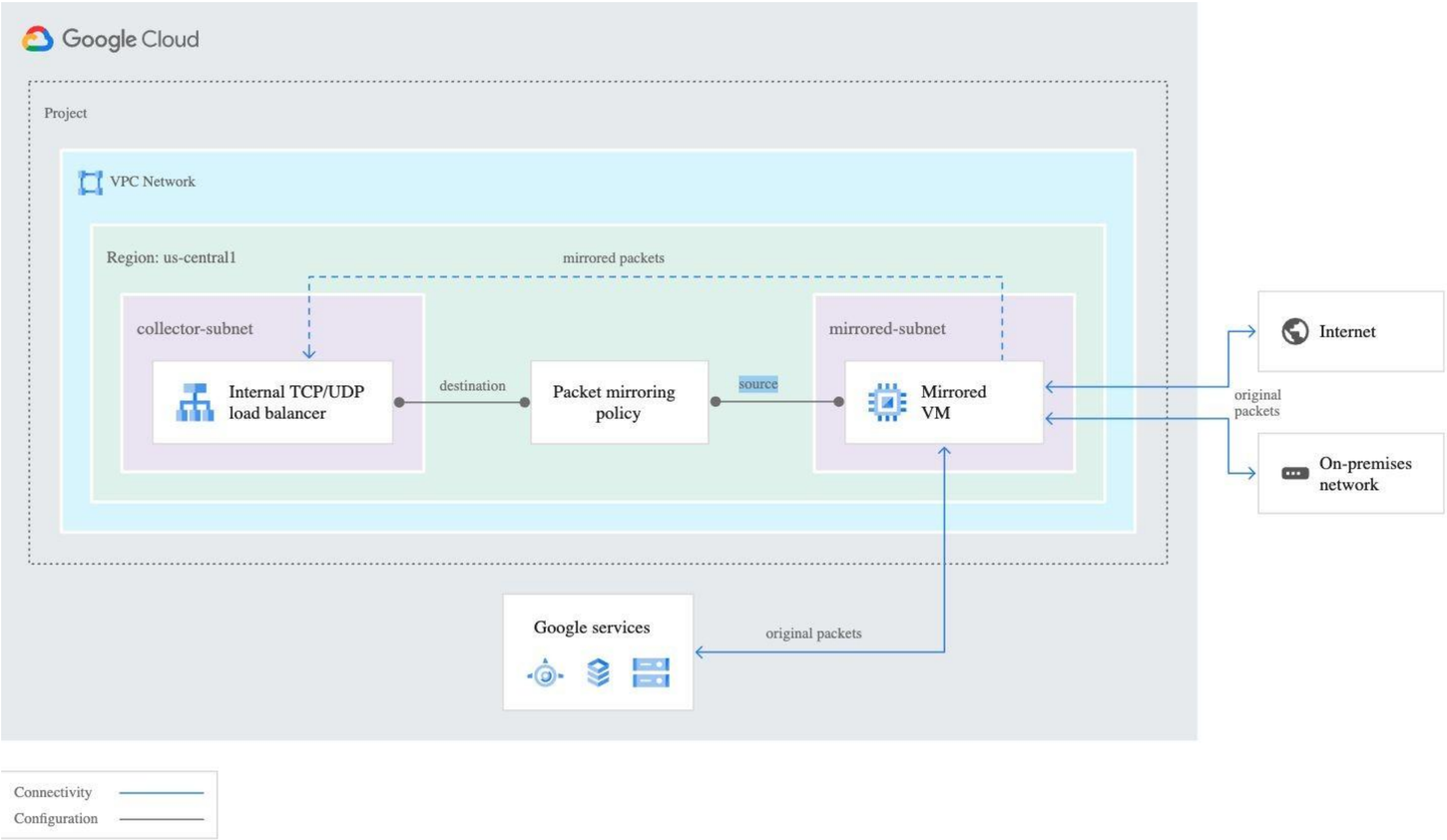
Cloud NAT logging

- 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



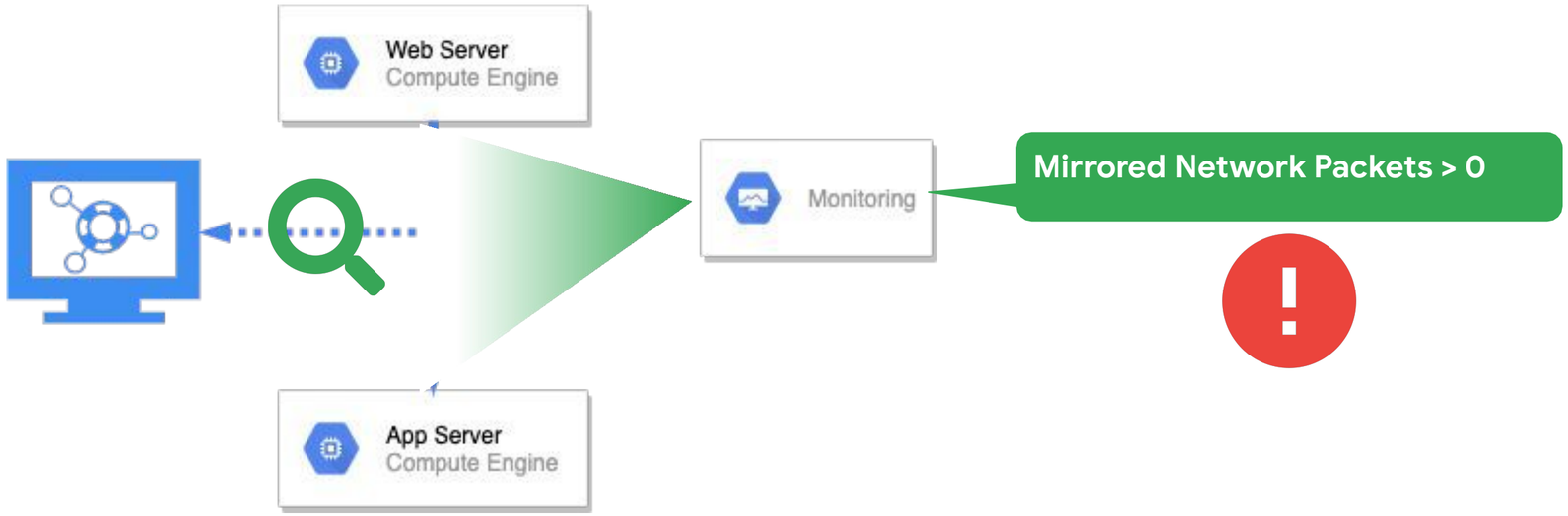
Packet Mirroring: visualize and protect your network

- 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



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



Google Cloud

Google Cloud