



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

The screenshot displays the Google Cloud Logs Viewer interface for the 'Cloud Logs Test Project'. The interface is divided into several sections, each with a numbered callout:


- 1**: Logs Viewer header.
- 2**: Project dropdown menu.
- 3**: Query builder input area.
- 4**: Logs field explorer sidebar.
- 5**: Histogram chart showing log frequency over time.
- 6**: Time range selector for the histogram.
- 7**: Query results table header.
- 8**: Query results table body.
- 9**: Page layout settings.
- 10**: Search products and resources bar.
- 11**: Run Query button.
- 12**: Jump to Now button.
- 13**: Actions dropdown menu.
- 14**: Configure dropdown menu.
- 15**: Hide log summary button.
- 16**: Expand nested fields button.
- 17**: Copy to clipboard button.
- 18**: Save button.
- 19**: Copy link button.
- 20**: Run Query button (in results table).
- 21**: Close button for histogram.
- 22**: Project dropdown menu (in refine scope).
- 23**: Close button for query results.
- 24**: Close button for log details.


The interface also shows a 'Query builder' section with filters for Resource, Log name, and Severity. The 'Logs field explorer' lists fields like 'RESOURCE TYPE' and 'SEVERITY'. The 'Query results' table displays log entries with columns for SEVERITY, TIMESTAMP, and SUMMARY. The log details view shows a JSON payload with fields like 'insertId', 'jsonPayload', 'resource', 'timestamp', 'severity', 'labels', 'logName', 'trace', 'receiveTimestamp', and 'spanId'.

Entries are returned as LogEntry objects

Query results 

[Jump to Now](#) [Actions](#) [Configure](#)

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

 {

```
{
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {
      principalEmail: "patrick.haggerty@roittraining.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: {}
      }
      destinationAttributes: {}
    }
    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: {}
      }
    ]
    resourceName: "namespaces/velossandbox/services/demo"
    request: {
      service: {
        apiVersion: "serving.knative.dev/v1"
        kind: "Service"
      }
    }
  }
}
```

[Hide log summary](#) [Collapse nested fields](#) [Copy to clipboard](#) [Copy link](#)

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

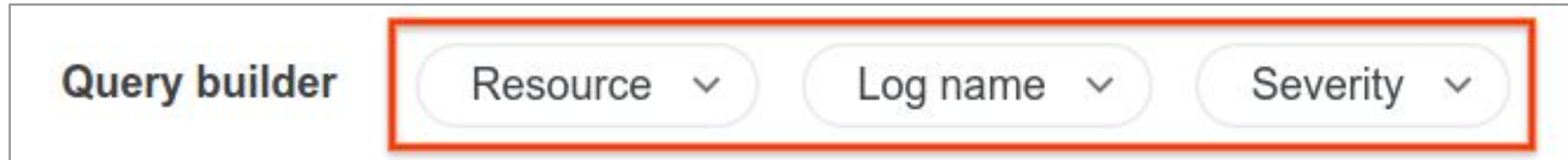


The screenshot shows the Google Cloud Query Builder interface. At the top, there are tabs for 'Query builder', 'Recent (2)', 'Saved (0)', and 'Suggested (0)'. To the right of these tabs are buttons for 'Save' and 'Run Query'. Below the tabs, there are three dropdown menus labeled 'Resource', 'Log name', and 'Severity'. The main area of the interface contains a query editor with two lines of text:

```
1 logName="projects/velossandbox/logs/cloudaudit.googleapis.com%2Factivity"  
2 resource.type="cloud_run_revision"
```

- 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

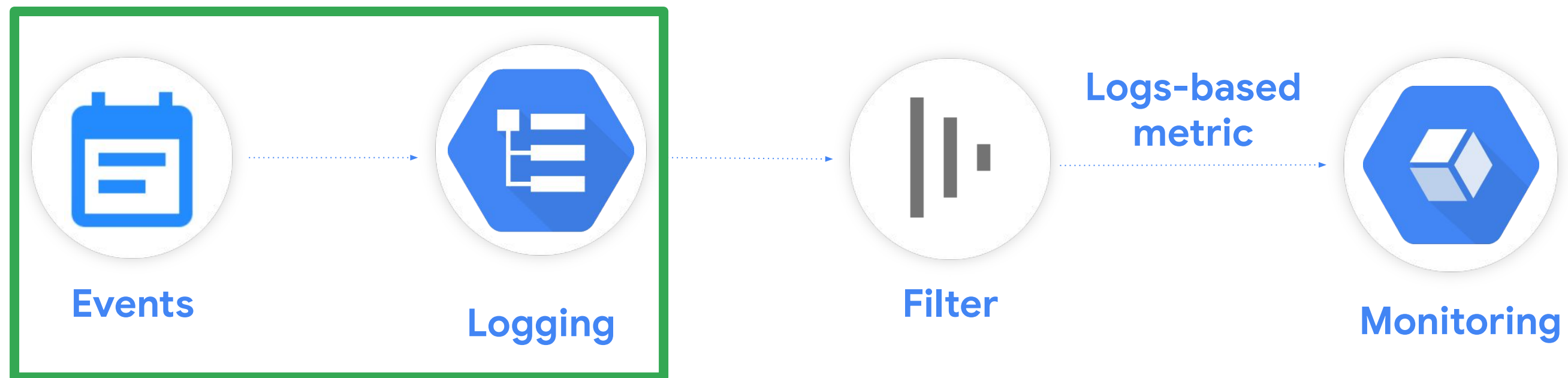


The image shows a query builder interface. On the left, the text "Query builder" is displayed. To its right, there is a horizontal container with three filter buttons: "Resource", "Log name", and "Severity". Each button has a downward-pointing chevron icon. A red rectangular box highlights the three filter buttons.

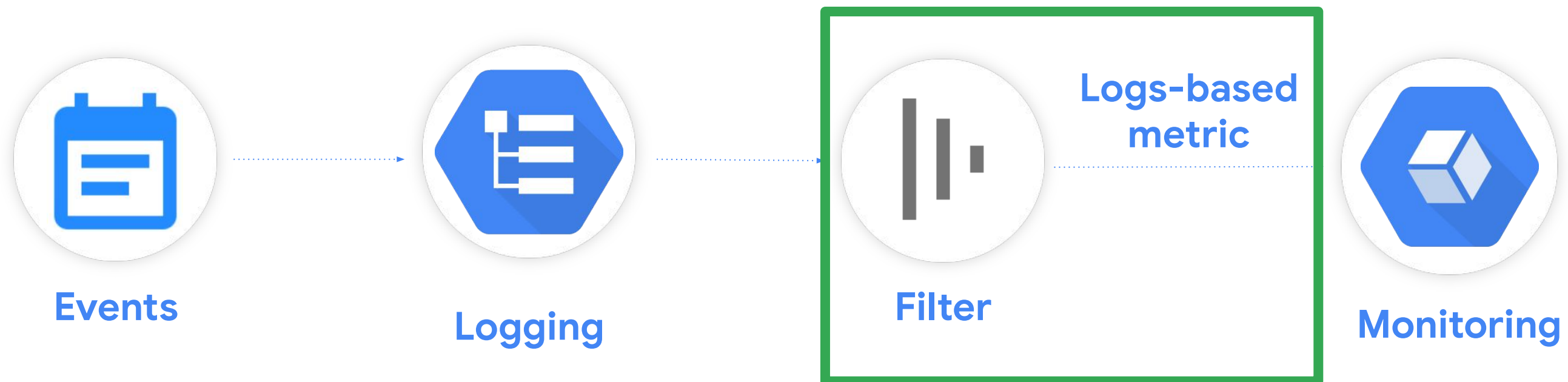
Key access control roles

- **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

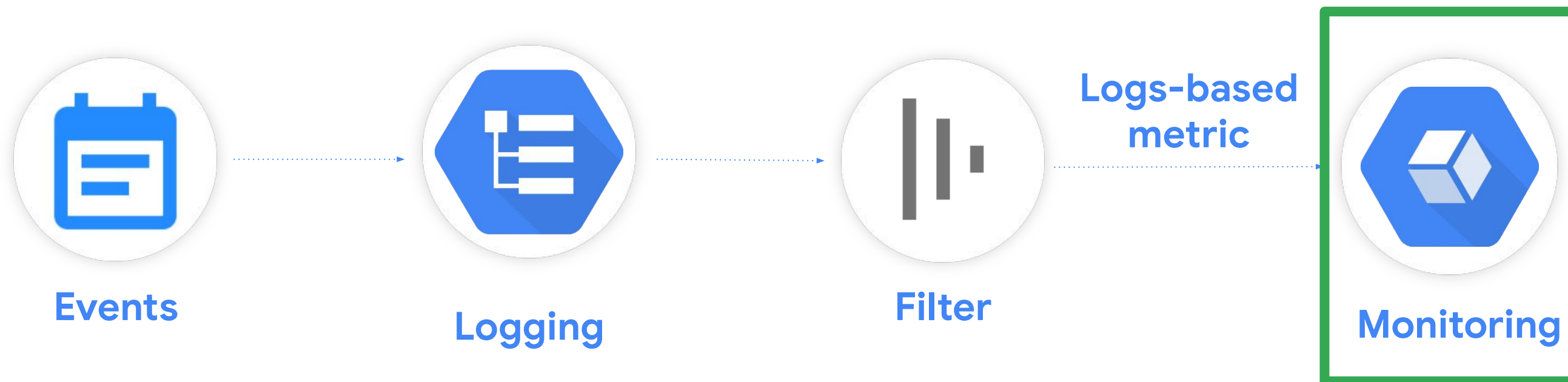
Logs-based metrics



Logs-based metrics

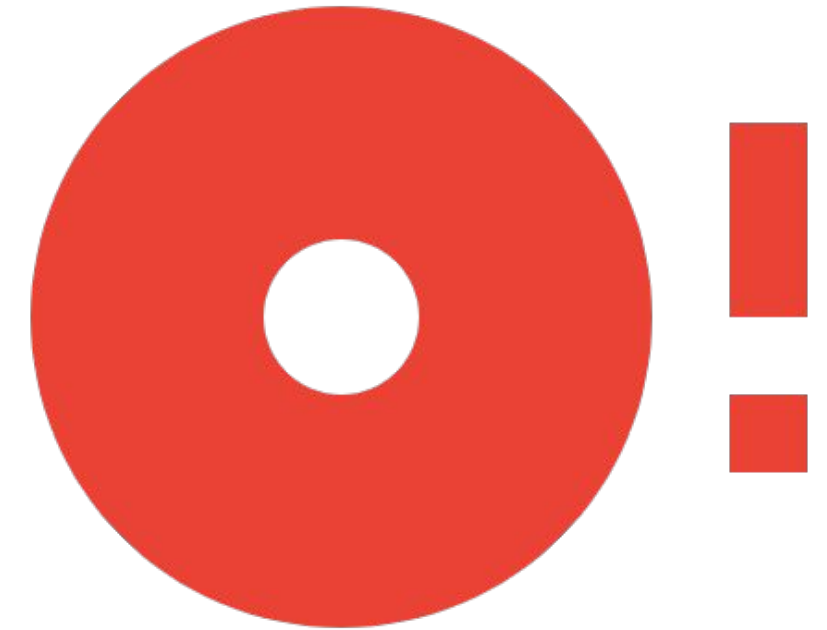


Logs-based metrics



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"	<div><div>Edit metric</div><div>Delete metric</div><div>View logs for metric</div><div>View in Metrics Explorer</div></div>

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"	<div><div>Edit metric</div><div>Delete metric</div><div>View logs for metric</div><div>View in Metrics Explorer</div></div>

Logs-based metrics

Google Cloud Platform patrick-haggerty

Stackdriver Logging

Logs-based metrics

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"	<ul style="list-style-type: none">Edit metricDelete metricView logs for metricView in Metrics Explorer

Logs-based metrics

Google Cloud Platform patrick-haggerty

Stackdriver Logging

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.

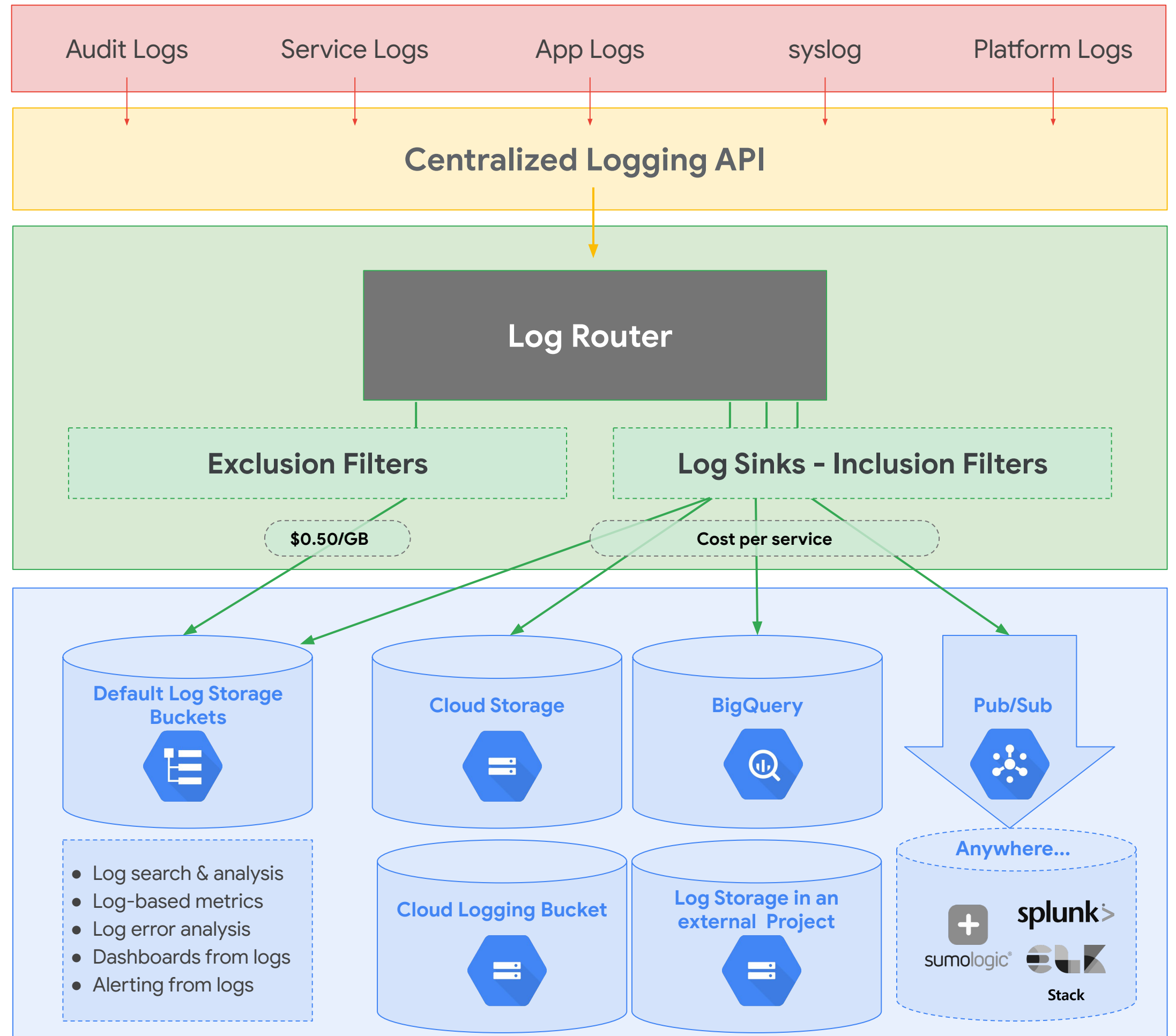
Filter Metrics

<input type="checkbox"/> Name ^	Type	Description	Previous Month Usage	Usage (MTD)	Filter	
<input type="checkbox"/> user/score-fun	Distribution		0 B	7.89 KiB	resource.type="global"	⋮ Edit metric Delete metric View logs for metric View in Metrics Explorer ↗

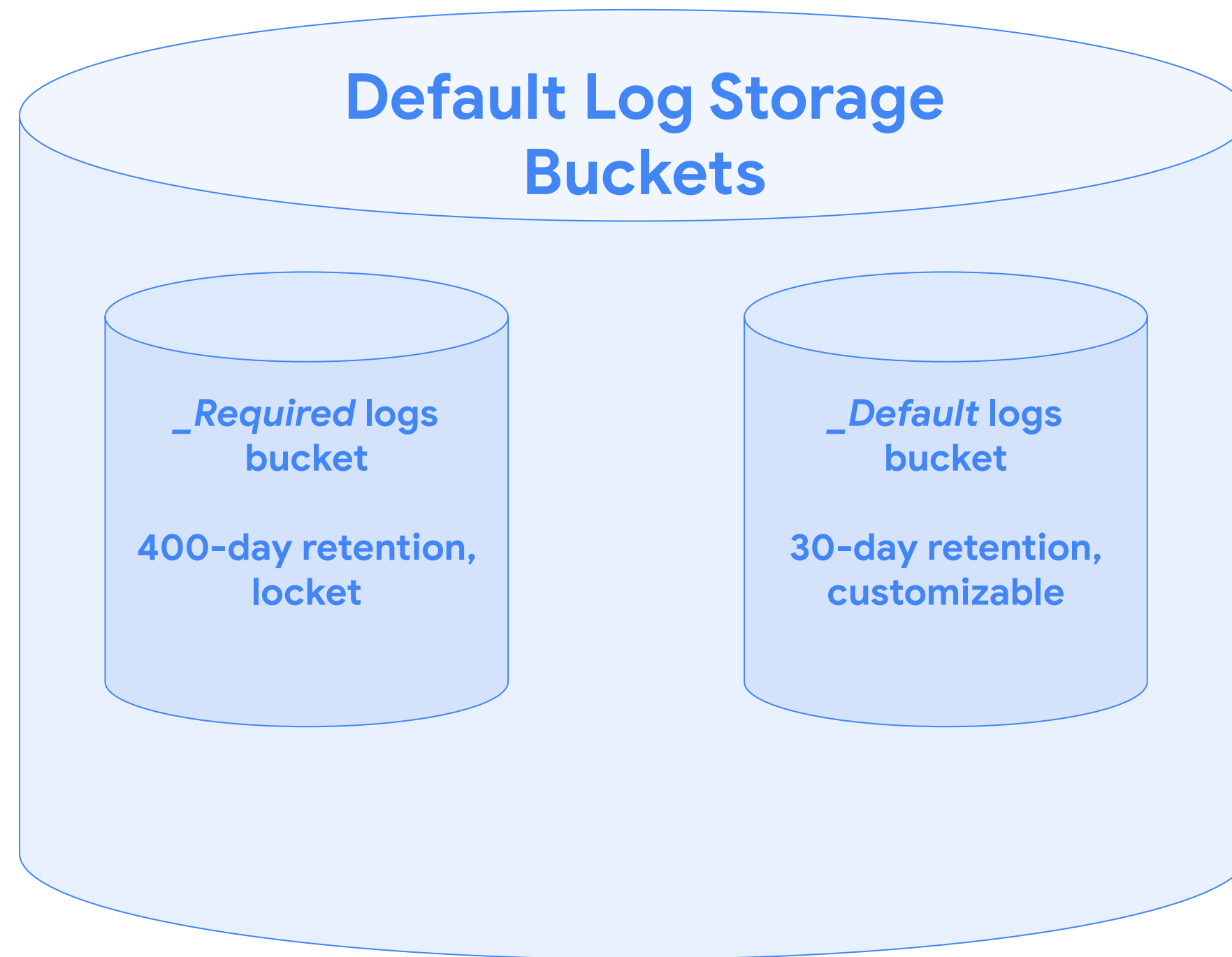
Logs-based metric creation flow

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



Default logs buckets



Create specialized buckets in current or remote projects:

Operations Logging

Logs Viewer

Logs Dashboard

Logs-based Metrics

Logs Router

Resource Usage

Logs Storage

Logs Storage

CREATE LOGS BUCKET


DELETE

Logs buckets








Filter

	Name ↑	Description	Retention period	Region	Status	
<input type="checkbox"/>	_Default	Default bucket	30 days	global	Unlocked	⋮
<input type="checkbox"/>	_Required	Audit bucket	400 days	global	Locked	⋮
<input type="checkbox"/>	application_x_logs	All logs for Application X	30 days	global	Unlocked	⋮

Resource usage



Resource Usage [+ CREATE USAGE ALERT](#)



Last month's ingested log volume
0 B
Total for the month of August. [See bill](#)

This month's ingested log volume
280.34 KiB
since the first of the month.

Excluded log volume
0 B
since the first of the month.


Projected ingestion log volume ?
304.43 KiB
by end of month

Ingestions Exclusions







Logs Ingestion

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 Usage [+ CREATE USAGE ALERT](#)



Last month's ingested log volume
0 B
Total for the month of August. [See bill](#)

This month's ingested log volume
280.34 KiB
since the first of the month.

Excluded log volume
0 B
since the first of the month.

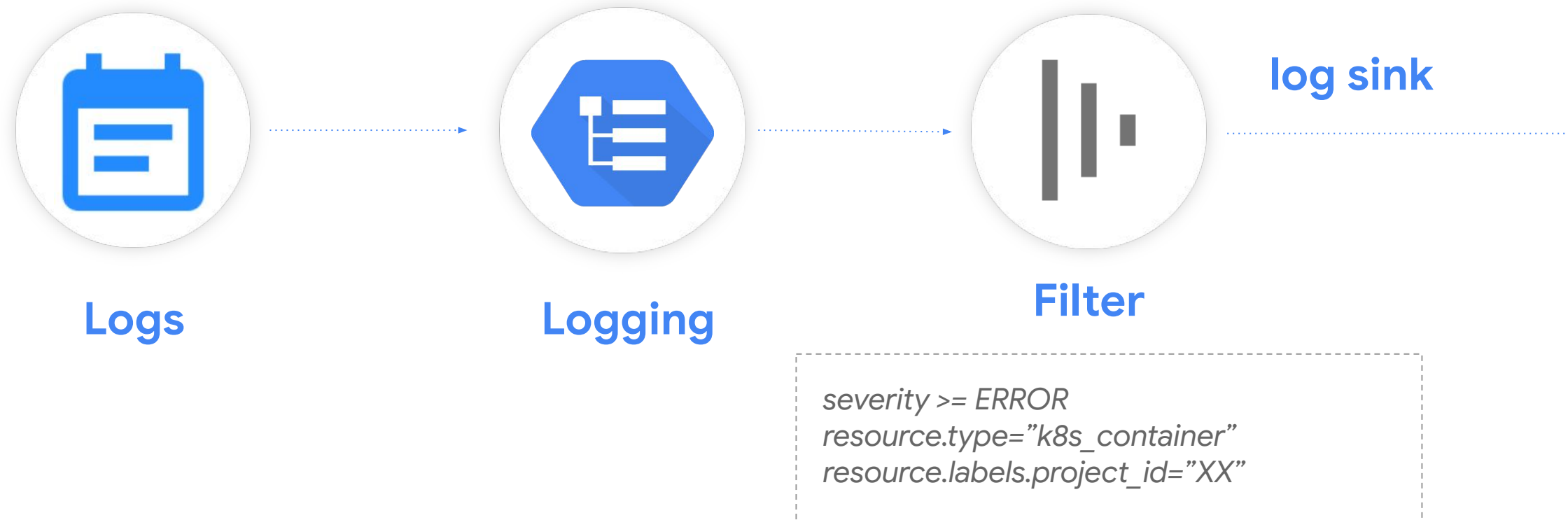
Projected ingestion log volume [?](#)
304.43 KiB
by end of month

[Ingestions](#) [Exclusions](#)

Logs Ingestion

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

Select sink service

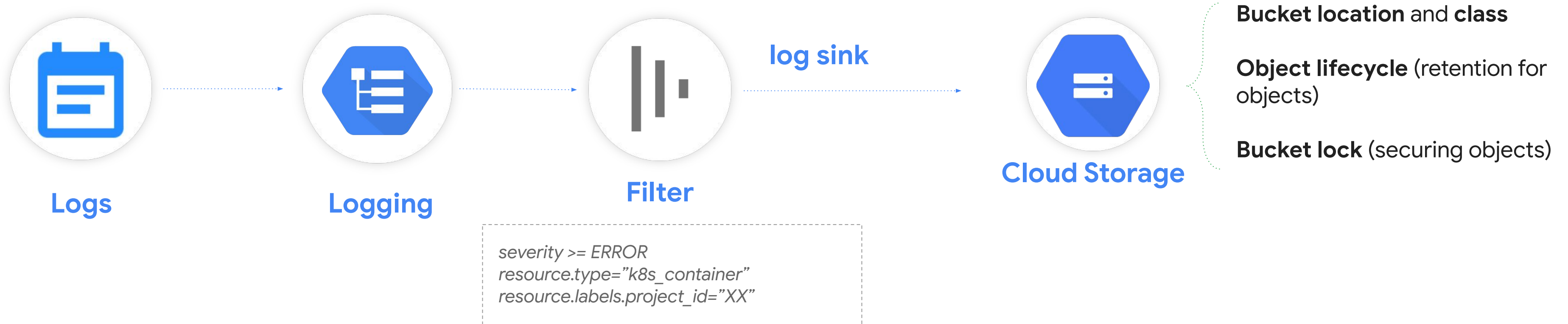
Choose the destination service for a new sink

- ☐ Cloud Logging bucket
- ☐ BigQuery dataset
- ☐ Cloud Storage bucket
- ☐ Cloud Pub/Sub topic
- ☐ Splunk
- ☐ Other project

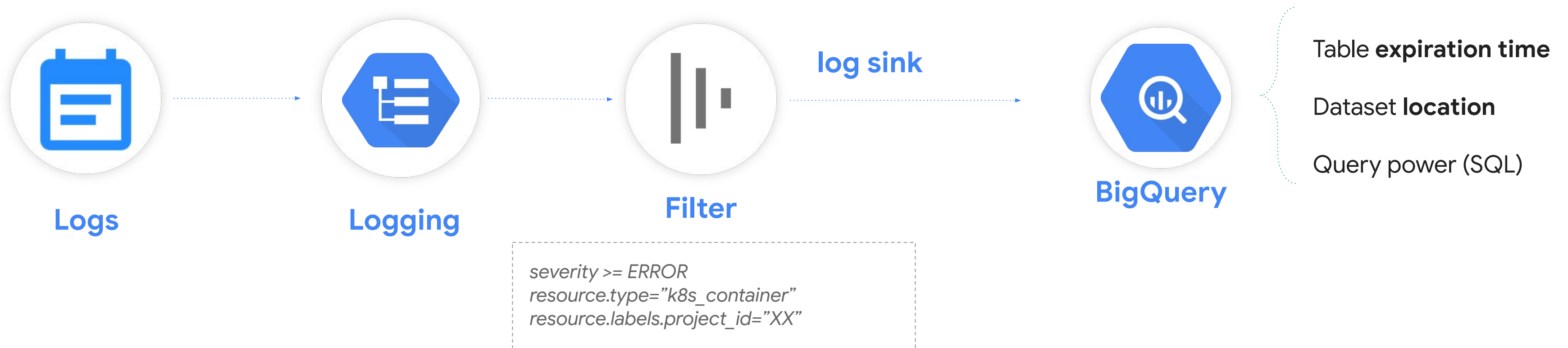
CANCEL

NEXT

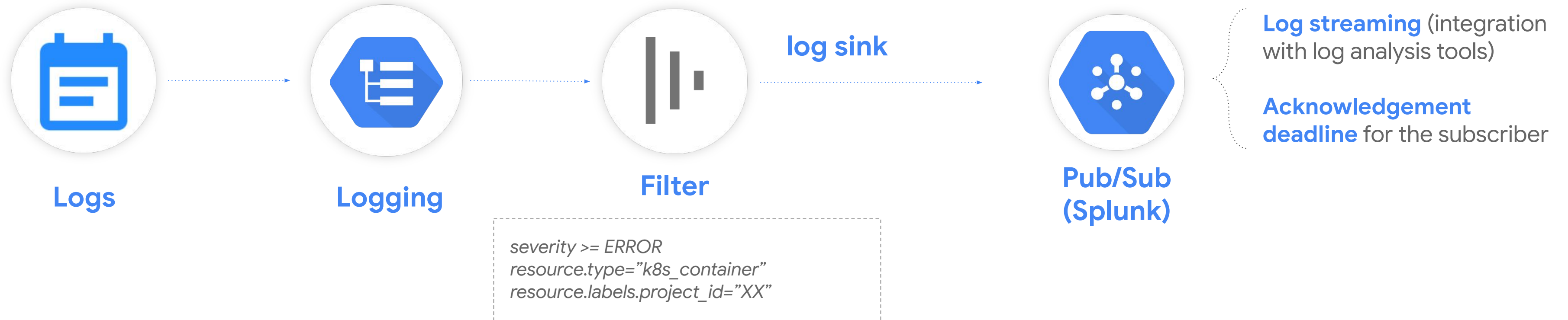
Cloud Storage works well for general storage:



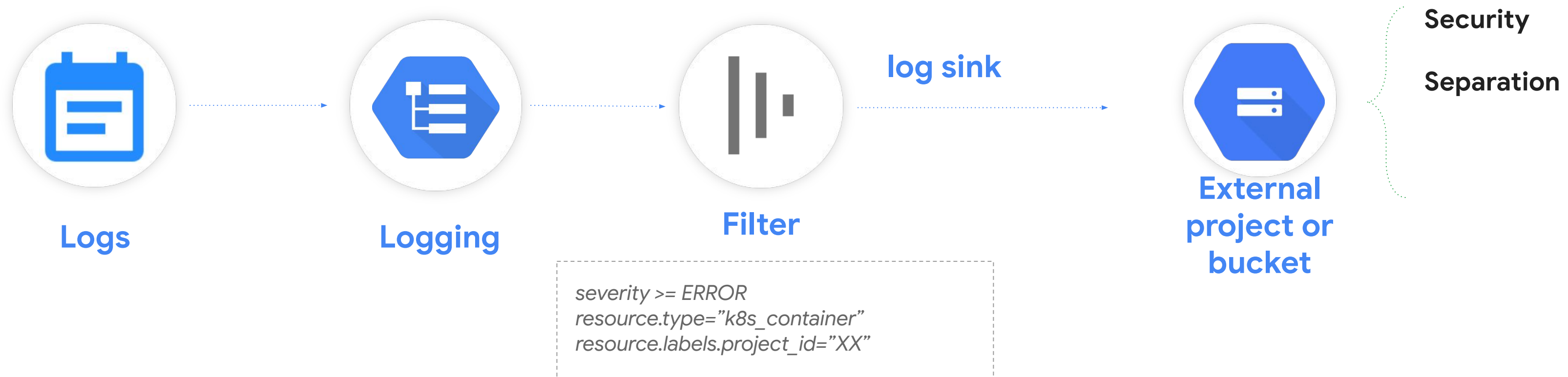
BigQuery for easy warehousing and analysis



Pub/Sub to connect with external systems and applications



Log exports



Create a log sink

The screenshot shows the Google Cloud Platform Logging console. The left sidebar contains navigation links: Stackdriver Logging, Logs Viewer, Logs-based Metrics, Logs Router, and Resource usage. The main area has a top bar with 'CREATE METRIC', 'CREATE SINK' (highlighted), 'SAVE SEARCH', and 'SHOW LIBRARY'. Below this is a filter bar with 'Filter by label or text search', 'Cloud Run Revision, hello-logging', 'All logs', 'Any log level', 'Last hour', and 'Jump to now'. The logs list shows several entries from 2020-02-06. On the right, the 'Edit Sink' dialog is open, showing fields for 'Sink Name', 'Sink Service' (set to Bigquery), 'Sink Destination' (set to Cloud Storage), and 'Sink Destination' (set to Pub/Sub). A 'Create Sink' button is visible.

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

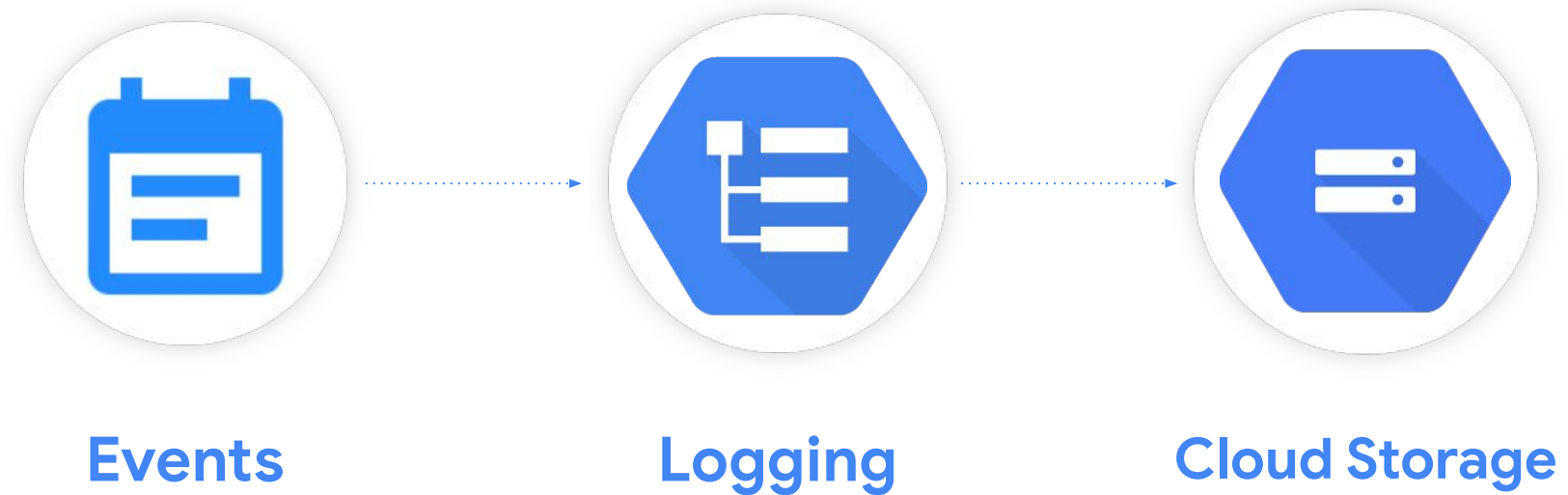
Log archiving and analysis

Example pipeline



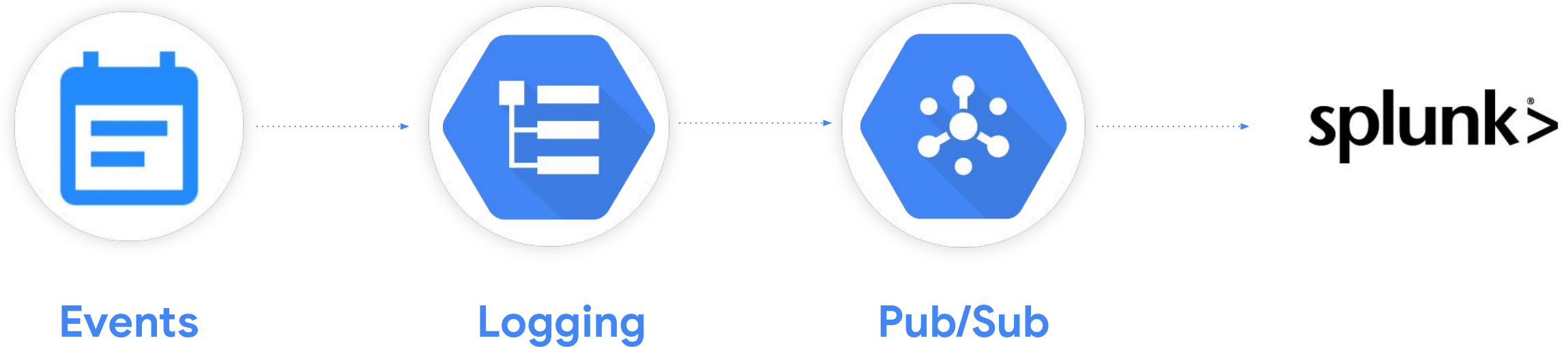
Archive logs for long-term storage

Example pipeline

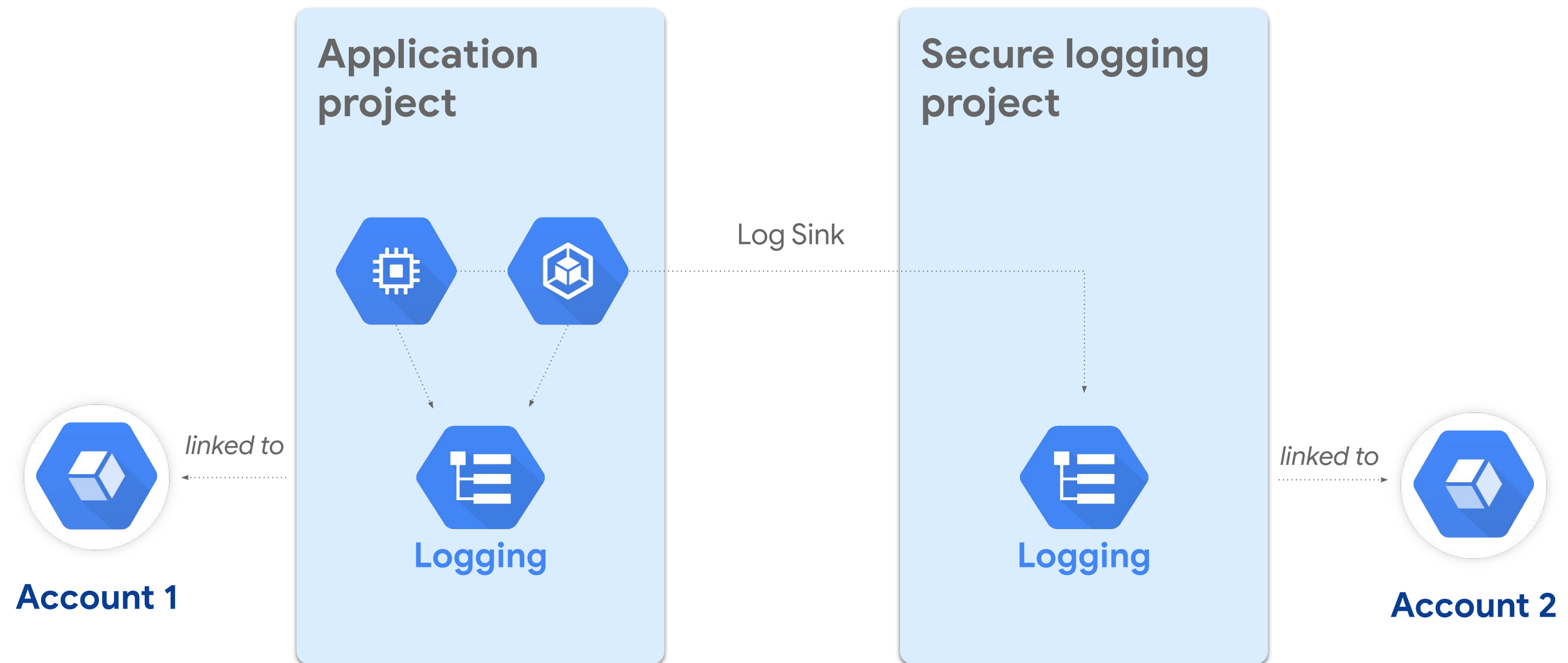


Exporting back to Splunk

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



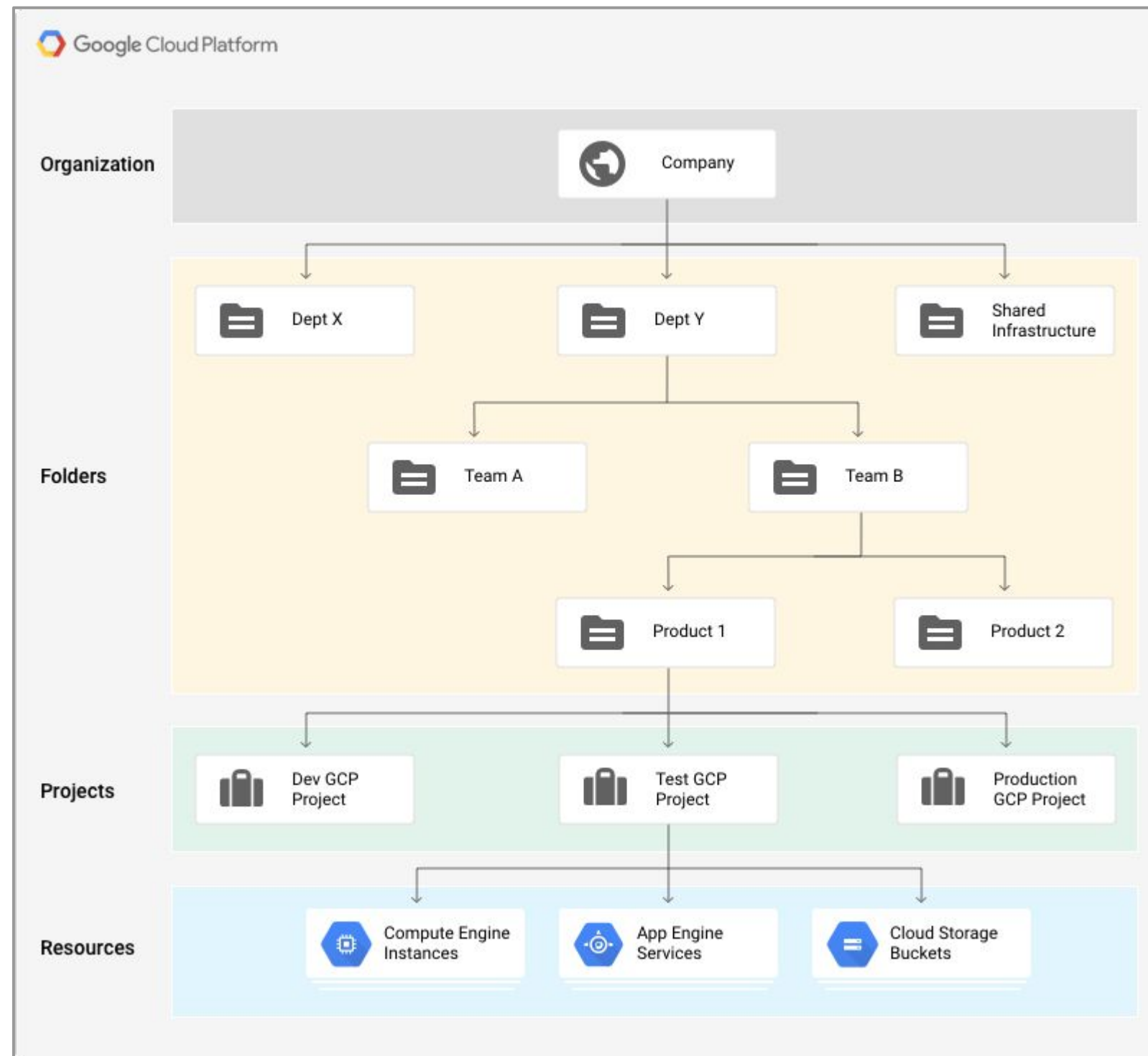
In near real time



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


 IAM & admin


 IAM


 Identity & Organization


 Policy Troubleshooter


 Organization policies


 Quotas


 Service accounts


 Labels


 Settings


 Privacy & Security


 Cryptographic keys

 Identity-Aware Proxy

 Roles

 Audit Logs

 Manage resources



Audit Logs

DEFAULT AUDIT CONFIG

Filter table

?

III

<input type="checkbox"/>	Title ↑	Admin Read	Data Read	Data Write	Exemptions
<input type="checkbox"/>	Access Approval	—	—	—	0
<input type="checkbox"/>	Apigee	—	—	—	0
<input type="checkbox"/>	Cloud Asset API	—	—	—	0
<input type="checkbox"/>	Cloud Billing API	—	—	—	0
<input checked="" type="checkbox"/>	Cloud Build API	—	—	—	0
<input type="checkbox"/>	Cloud Composer API	—	—	—	0
<input type="checkbox"/>	Cloud Data Loss Prevention (DLP) API	—	—	—	0
<input type="checkbox"/>	Cloud Dataproc API	—	—	—	0
<input type="checkbox"/>	Cloud Datastore API	—	—	—	0
<input type="checkbox"/>	Cloud Functions API	—	—	—	0
<input type="checkbox"/>	Cloud Healthcare	—	—	—	0
<input type="checkbox"/>	Cloud Identity-Aware Proxy API	—	—	—	0
<input type="checkbox"/>	Cloud IoT API	—	—	—	0
<input type="checkbox"/>	Cloud Key Management Service (KMS) API	—	—	—	0
<input type="checkbox"/>	Cloud Life Sciences API	—	—	—	0
<input type="checkbox"/>	Cloud Machine Learning Engine	—	—	—	0

Cloud Build API

LOG TYPE

EXEMPTED USERS

Turn on/off audit logging for selected services.

☐ Admin Read

☐ Data Read

☐ Data Write

SAVE

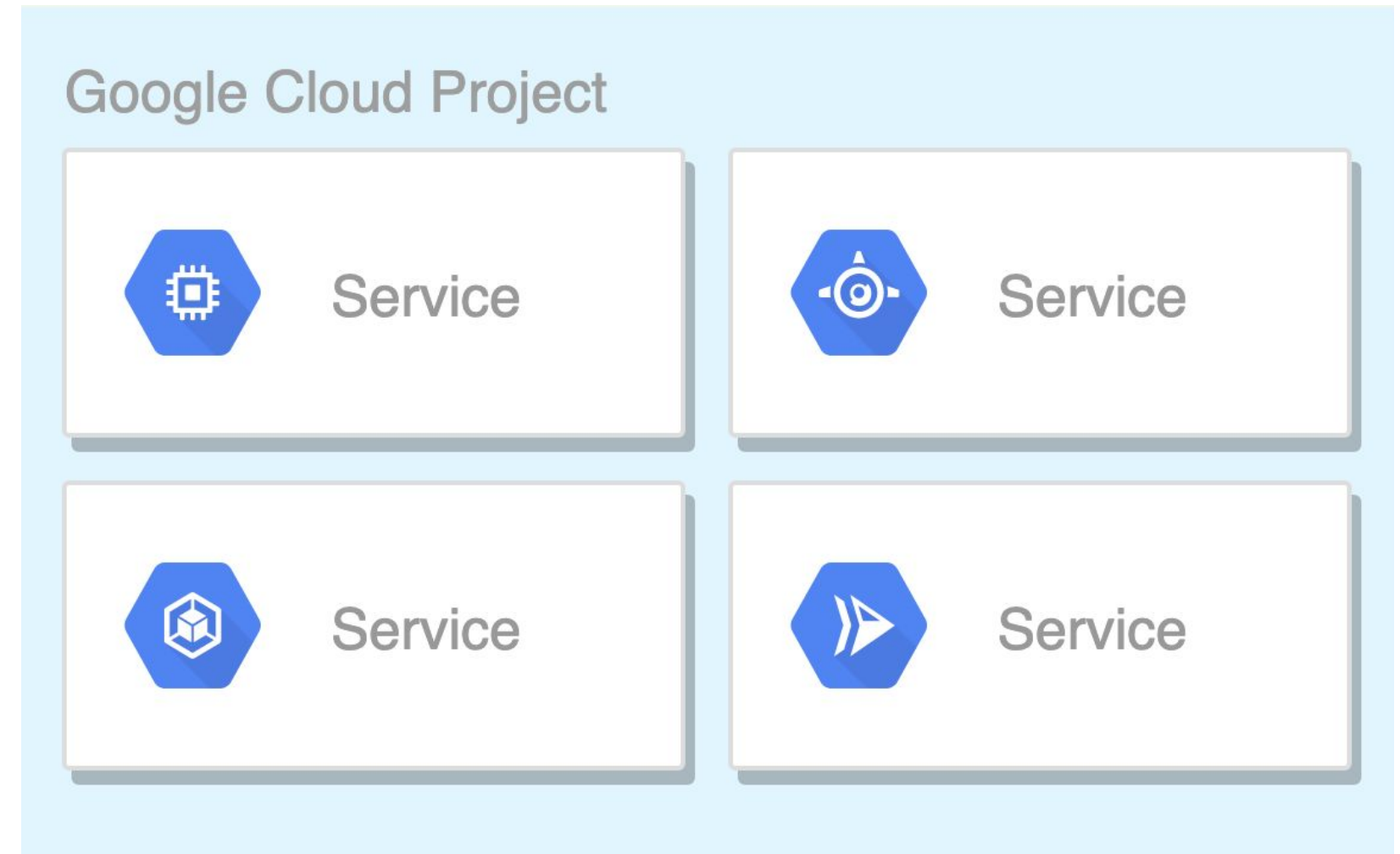


Working with Audit Logs



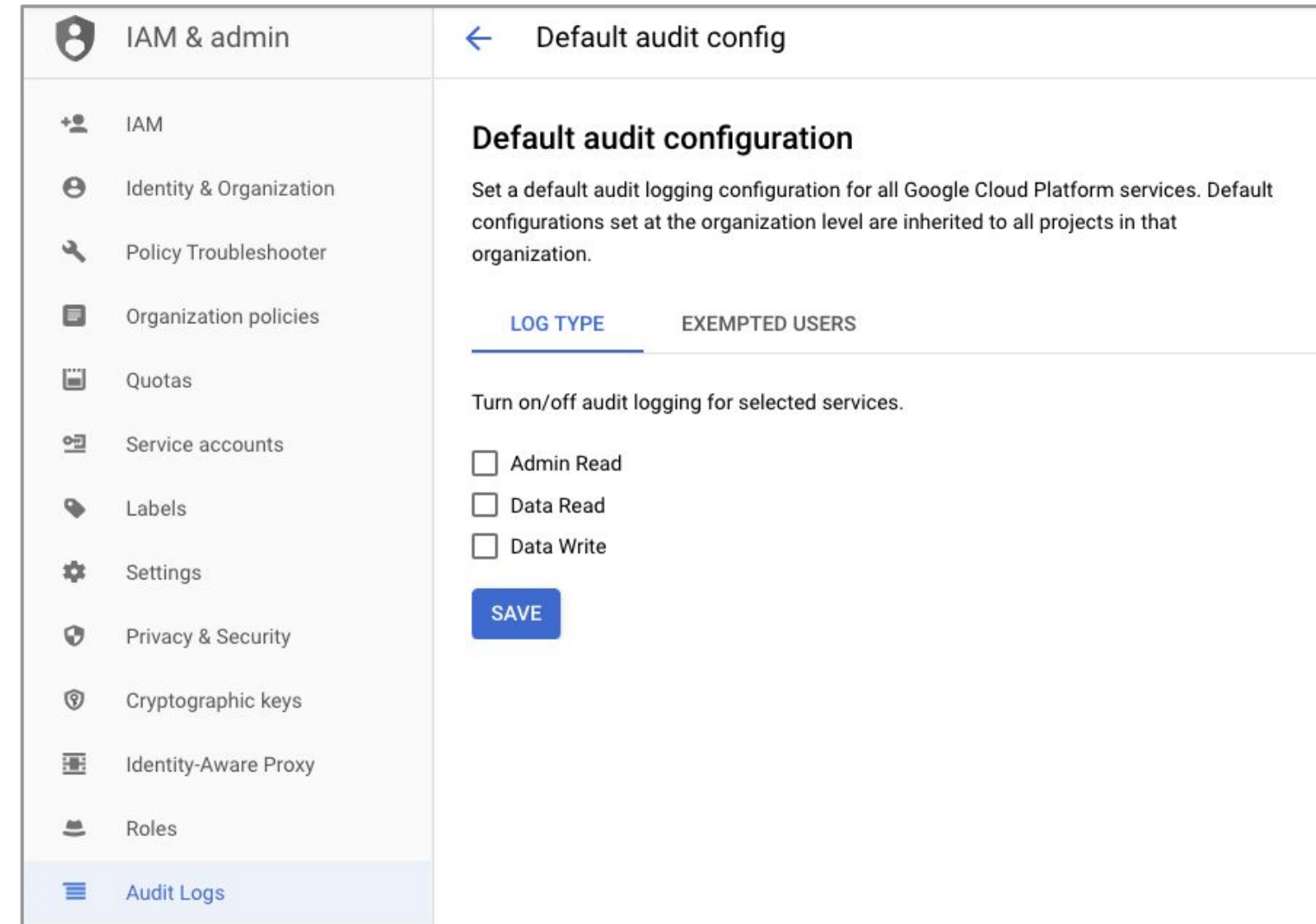
Plan and create test project

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



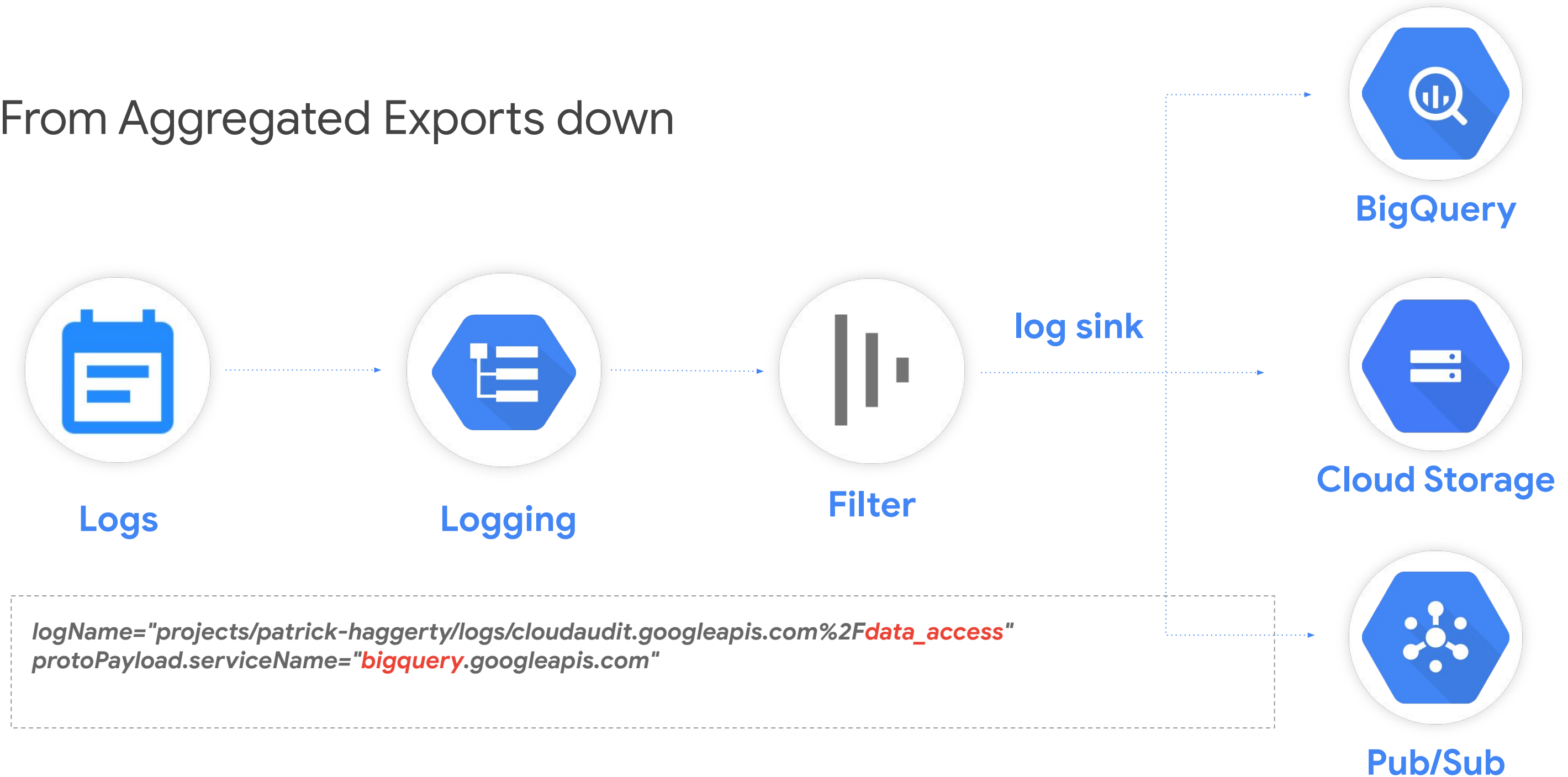
Decide and set org level data access

- 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

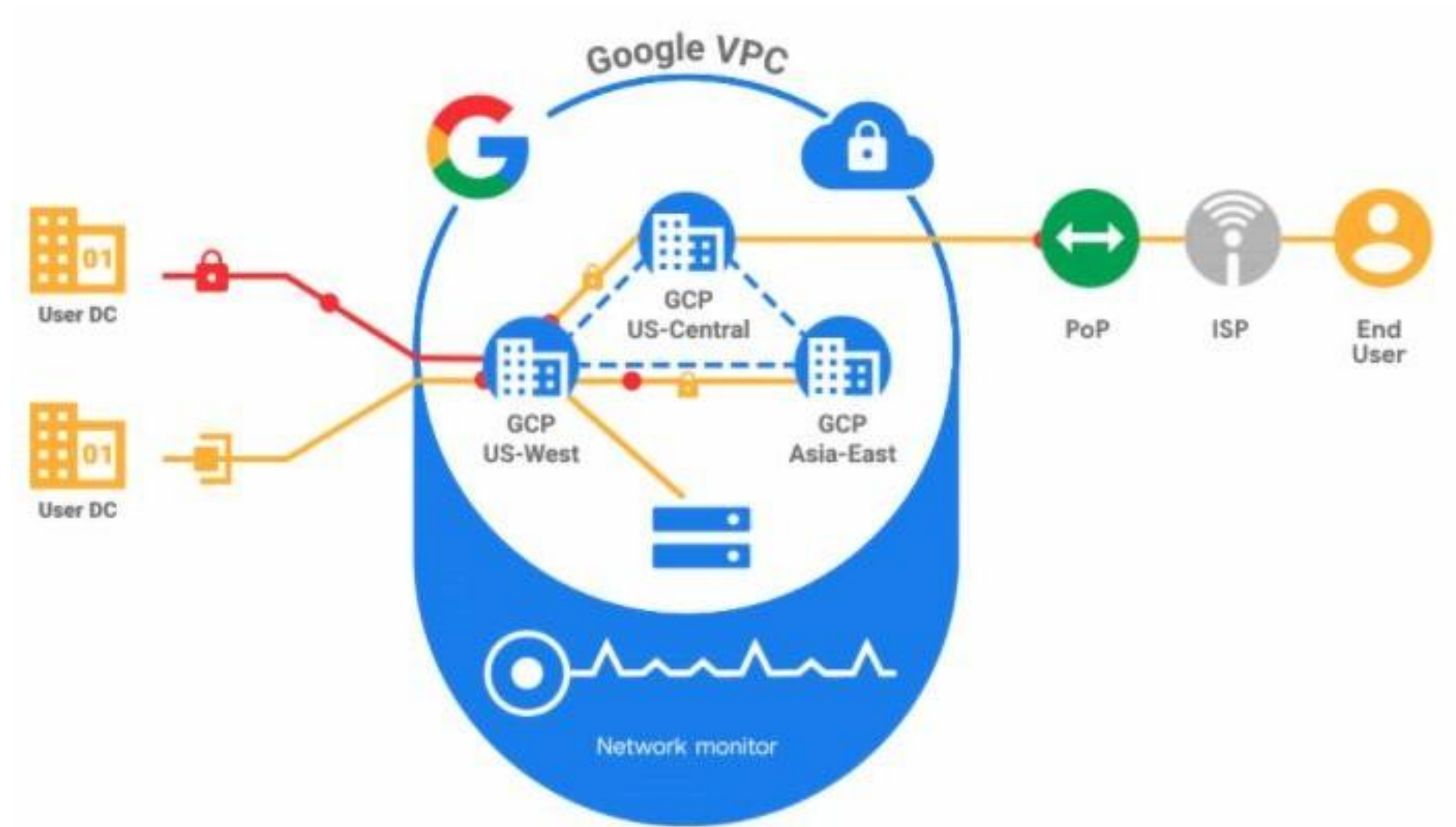
Load Balancer Logs

Cloud NAT Logs

Packet Mirroring

Network Intelligence
Center

VPC Flow Logs record a sample of network flows





Logging

Enable VPC Flow Logs per VPC subnet

VPC network

VPC networks

External IP addresses

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

Subnet details

EDITDELETE

default

VPC Network
default

Region
us-east1

IP address range

Subnetwork IP ranges must be unique and non-overlapping within a VPC network and peered VPC network. The following ranges are currently being used in other regions: 10.128.0.0/20, 22 MORE

10.142.0.0/20

Secondary IP ranges ?
+ ADD IP RANGE

Gateway
10.142.0.1

Private Google access
☐ On
☒ Off

Private Google Access is in effect (even though it has not been enabled manually) for packets sent from this subnet's primary and secondary IP ranges because Cloud NAT is configured for those ranges.
[Learn more](#)

Flow logs
Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. [Learn more](#)
☒ On
☐ Off

Google Cloud



Logging

Use Logging to review your VPC Flow Logs

Log name +

Severity v

Select log names

Reset

×

≡

Search log names

▼

COMPUTE ENGINE

☐

activity_log

compute.googleapis.com%2Factivity_log

☐

nat_flows

compute.googleapis.com%2Fnat_flows

☐

shielded_vm_integrity

compute.googleapis.com%2Fshielded_vm_inte...

☒

vpc_flows

compute.googleapis.com%2Fvpc_flows

▼

CLOUD RUN

☐

requests

run.googleapis.com%2Frequests

☐

stderr

run.googleapis.com%2Fstderr

String Preview

logName="projects/velo...

Cancel

Add

Analyze logs in BigQuery and visualize in Data Studio



BigQuery



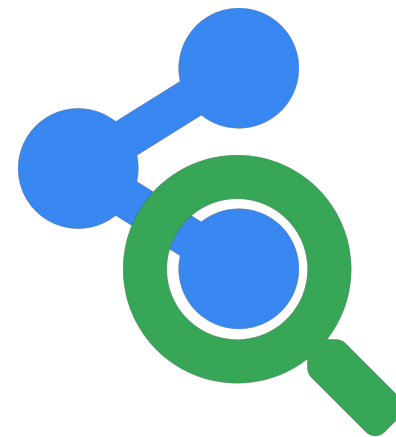
Data Studio

<div><div>RUN QUERY</div><div>Save Query</div><div>Save View</div><div>Format Query</div><div>Show Options</div></div>								
<div><div>Results</div><div>Details</div><div>Download as CSV</div></div>								
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	
<div><div>Table</div><div>JSON</div></div>								

Firewall Rules Logging



Did my firewall rules cause that application outage?



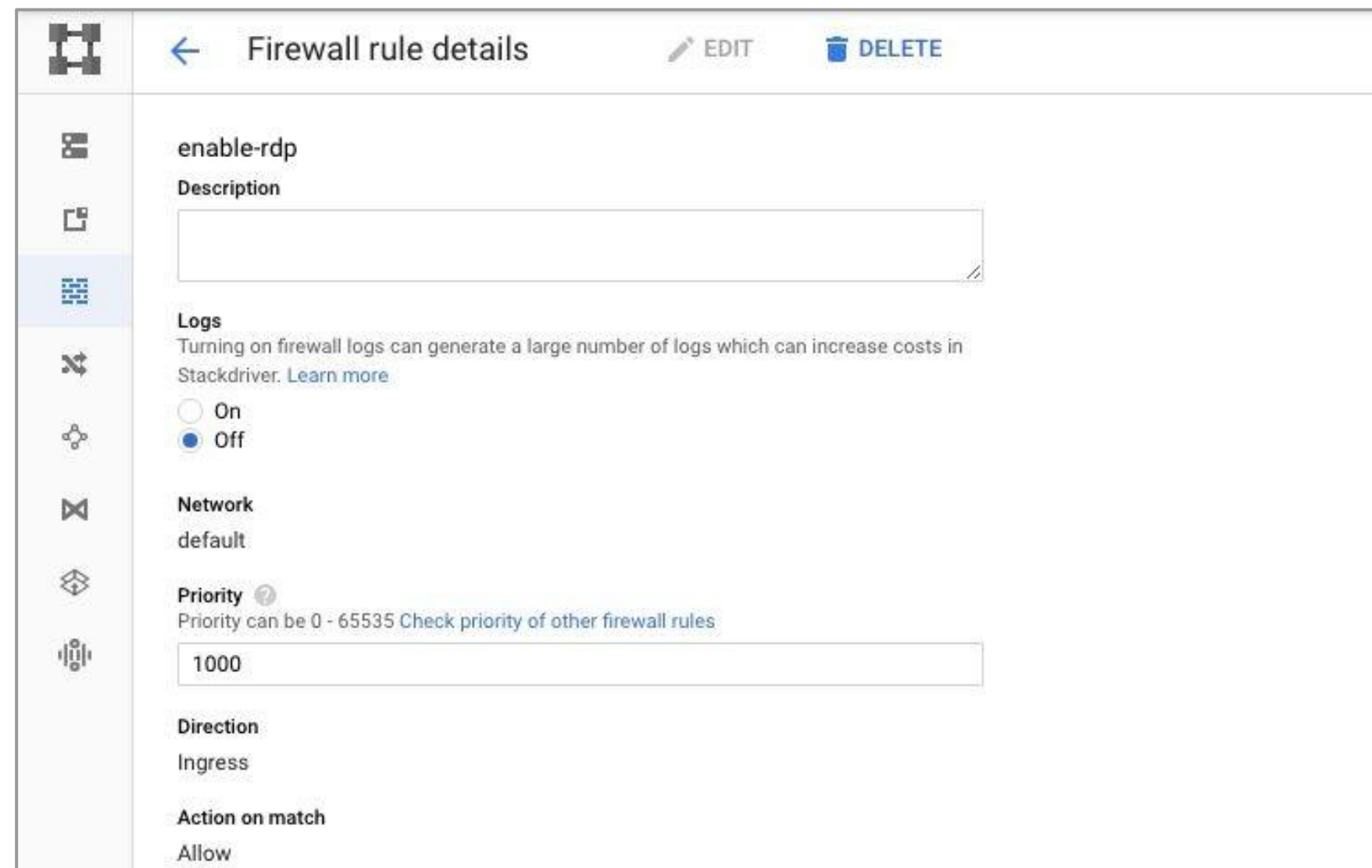
How many connections match the rule I just created?



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 screenshot shows the 'Firewall rule details' page in the Google Cloud console. The rule name is 'enable-rdp'. The 'Logs' section is currently set to 'Off', with a warning that turning on logs can increase costs. The 'Network' is set to 'default', 'Priority' is '1000', 'Direction' is 'Ingress', and 'Action on match' is 'Allow'. The left sidebar contains navigation icons for various Google Cloud services.

enable-rdp

Description

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)

☐ On

☒ Off

Network

default

Priority ?

Priority can be 0 - 65535 [Check priority of other firewall rules](#)

1000

Direction

Ingress

Action on match

Allow

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

Edit backend service

Name
k8s-be-31624--a20d93e6082ea0c3


Description

Backend type
Instance group

Protocol, named port & timeout

Protocol ?	Named port ?	Timeout ?
HTTP	port31624	30 seconds

Backends
Regions: us-central1

k8s-ig--a20d93e6082ea0c3 (Zone: us-central1-c, Port: 3... *Not saved* 

[+ Add backend](#)

Cloud CDN ?
☐ Enable Cloud CDN

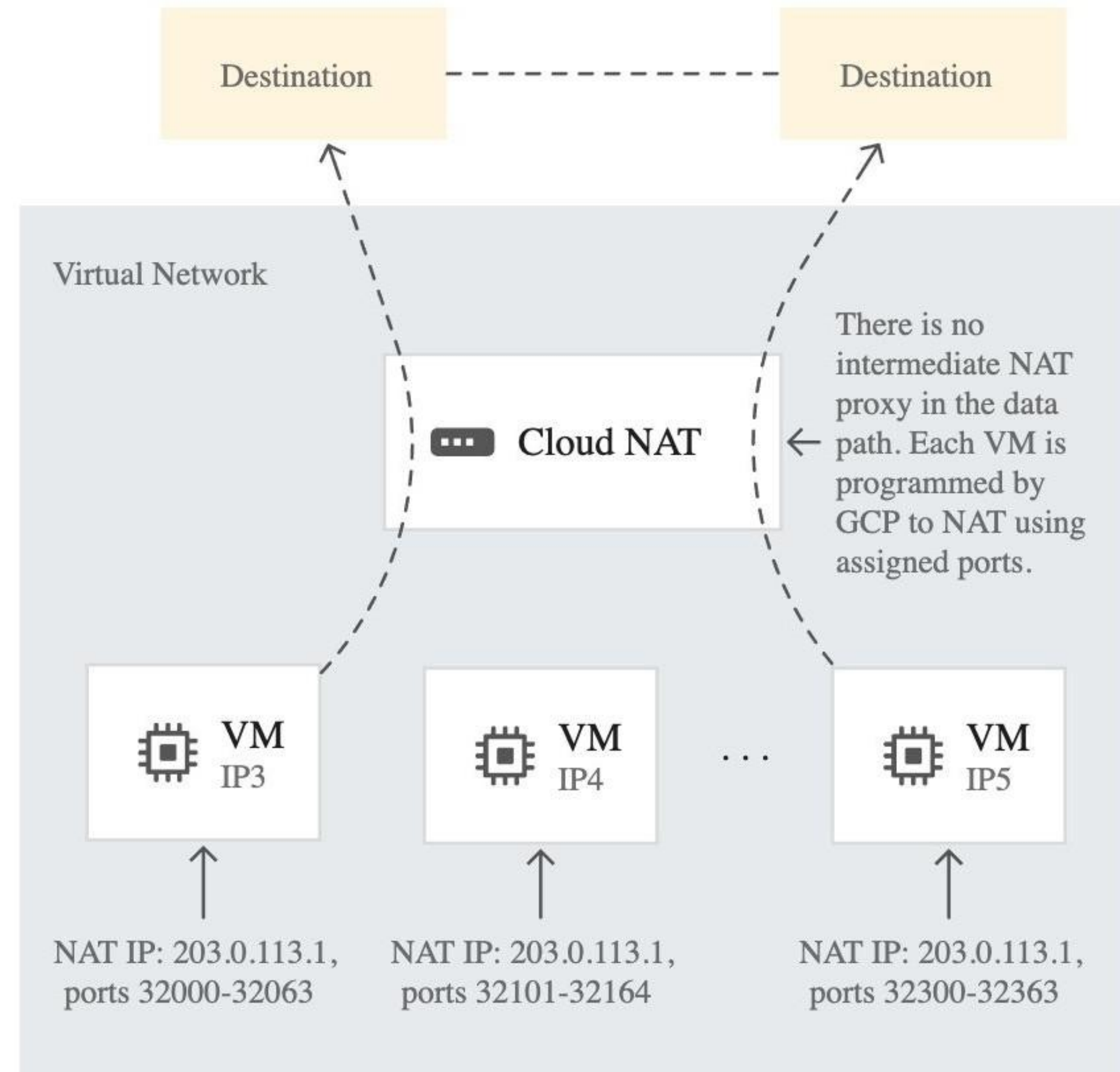
Health check ?
k8s-be-31624--a20d93e6082ea0c3 (HTTP)
port: 31624, timeout: 60s, check interval: 60s, unhealthy threshold: 10 attempts

Logging ?
☒ Enable logging

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

Advanced configurations

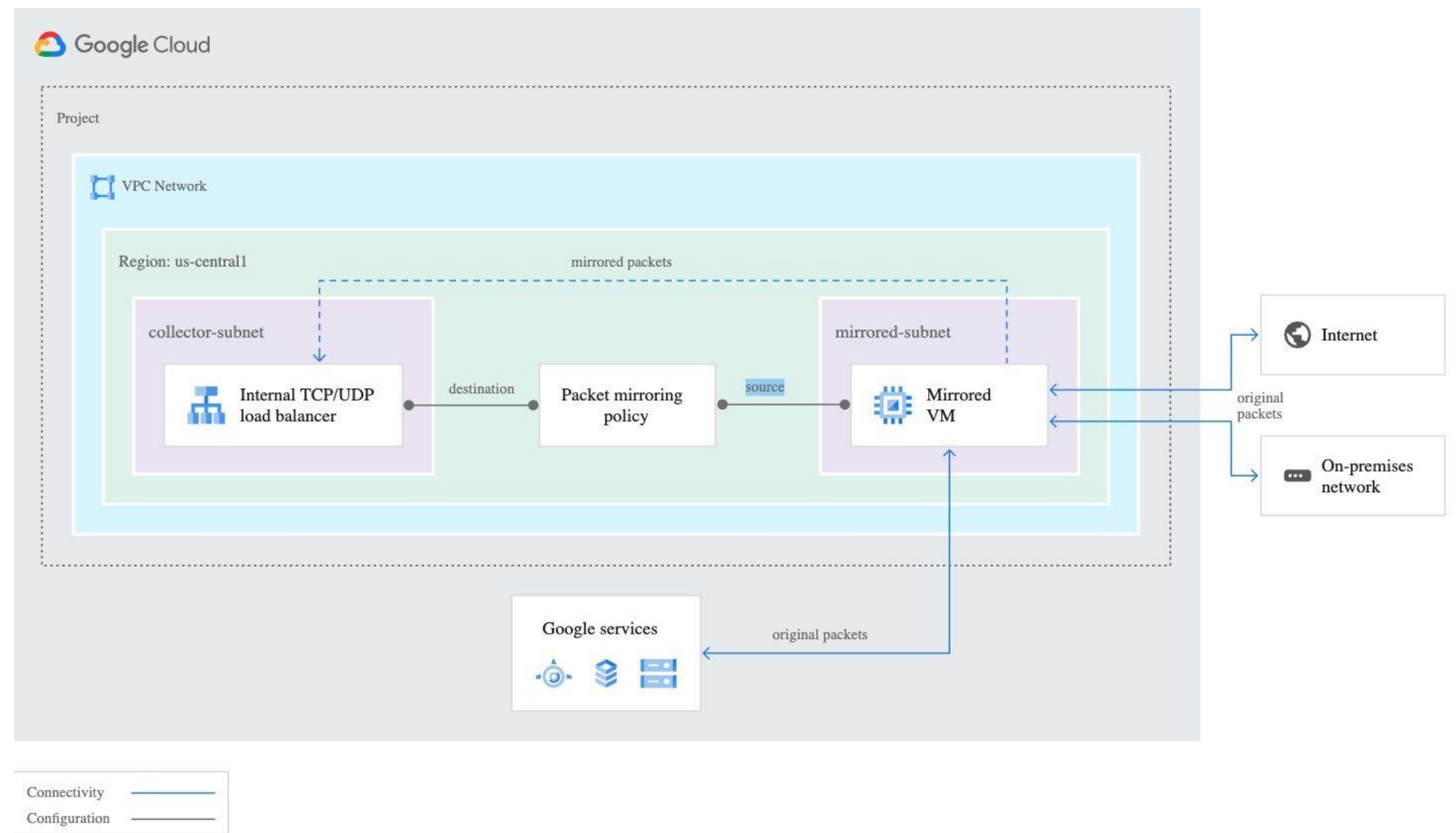
Stackdriver logging ?

Export Cloud NAT logs to Stackdriver

- ☐ No logging
- ☒ Translation and errors
- ☐ Translation only
- ☐ Errors only

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

