The information in this presentation is classified:

Google confidential & proprietary

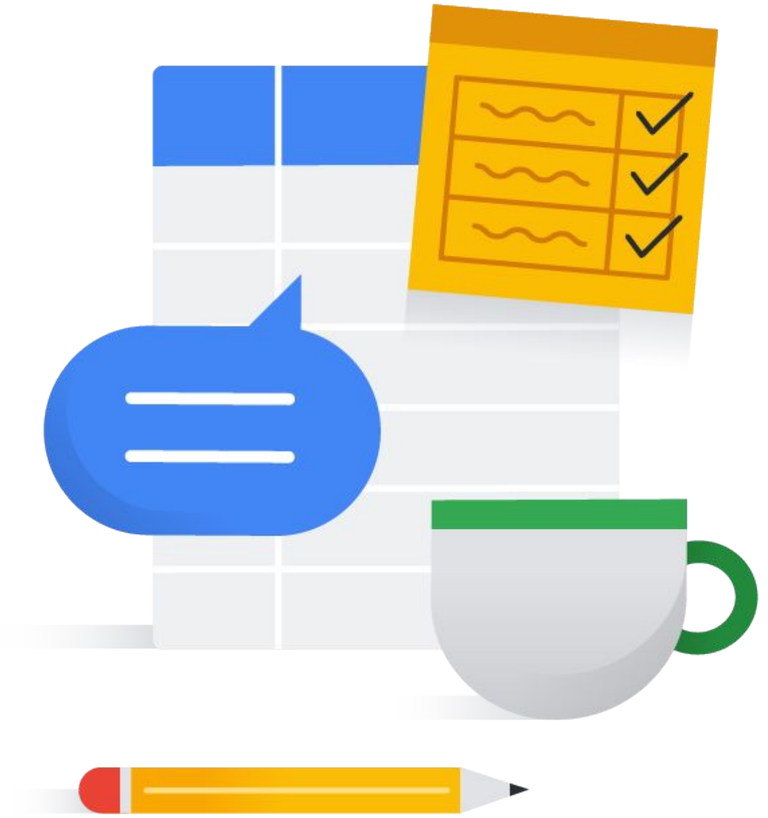
⚠️ This presentation is shared with you under NDA.

- 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!

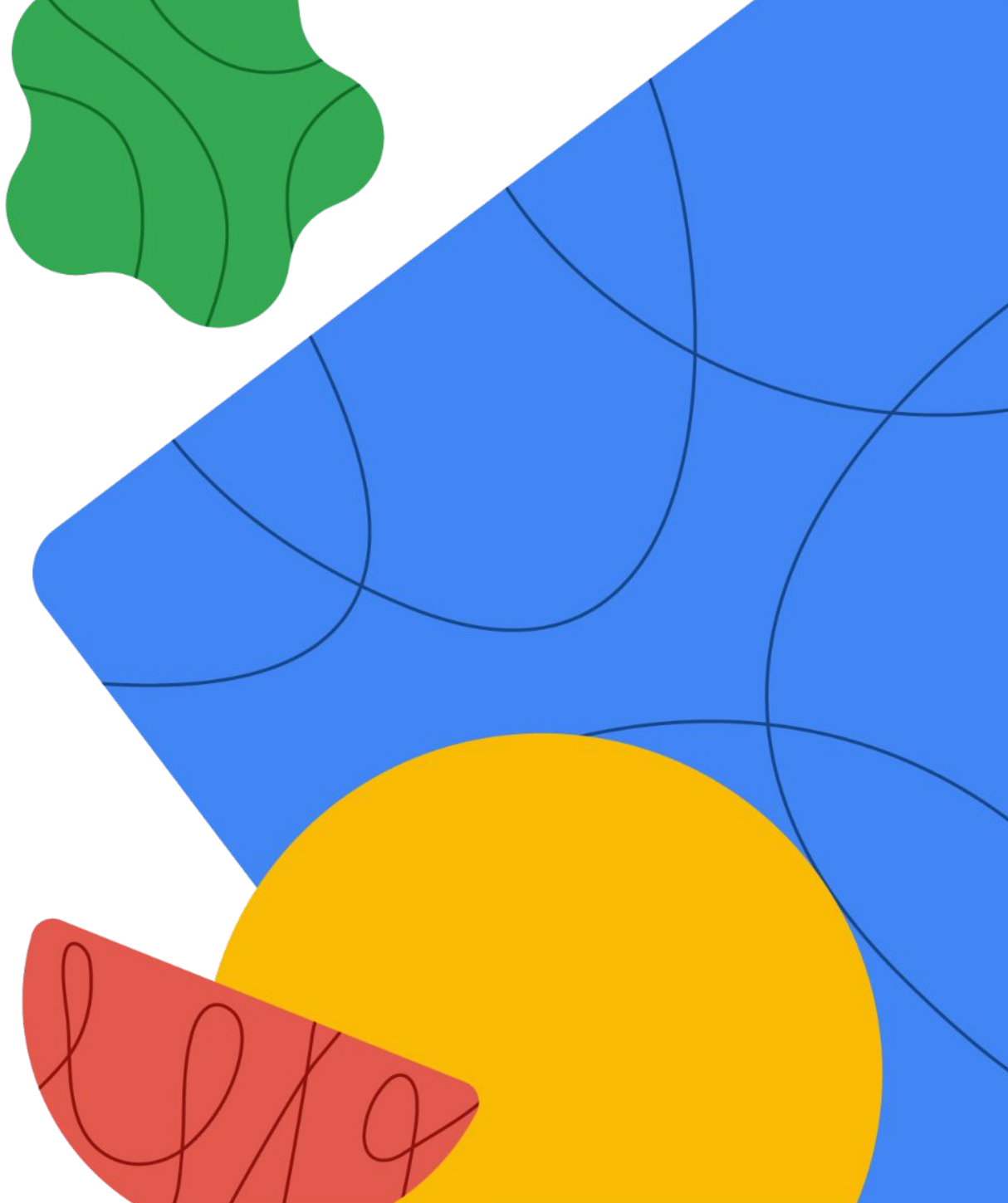
Program issues or concerns?

- Problems with **accessing** Cloud Skills Boost for Partners
  - cloud-partner-training@google.com
- Problems with **a lab** (locked out, etc.)
  - support@qwiklabs.com



Google Cloud

Logging and Monitoring



Our agenda

01 Google Cloud VPC Observability

02 Alerting policies

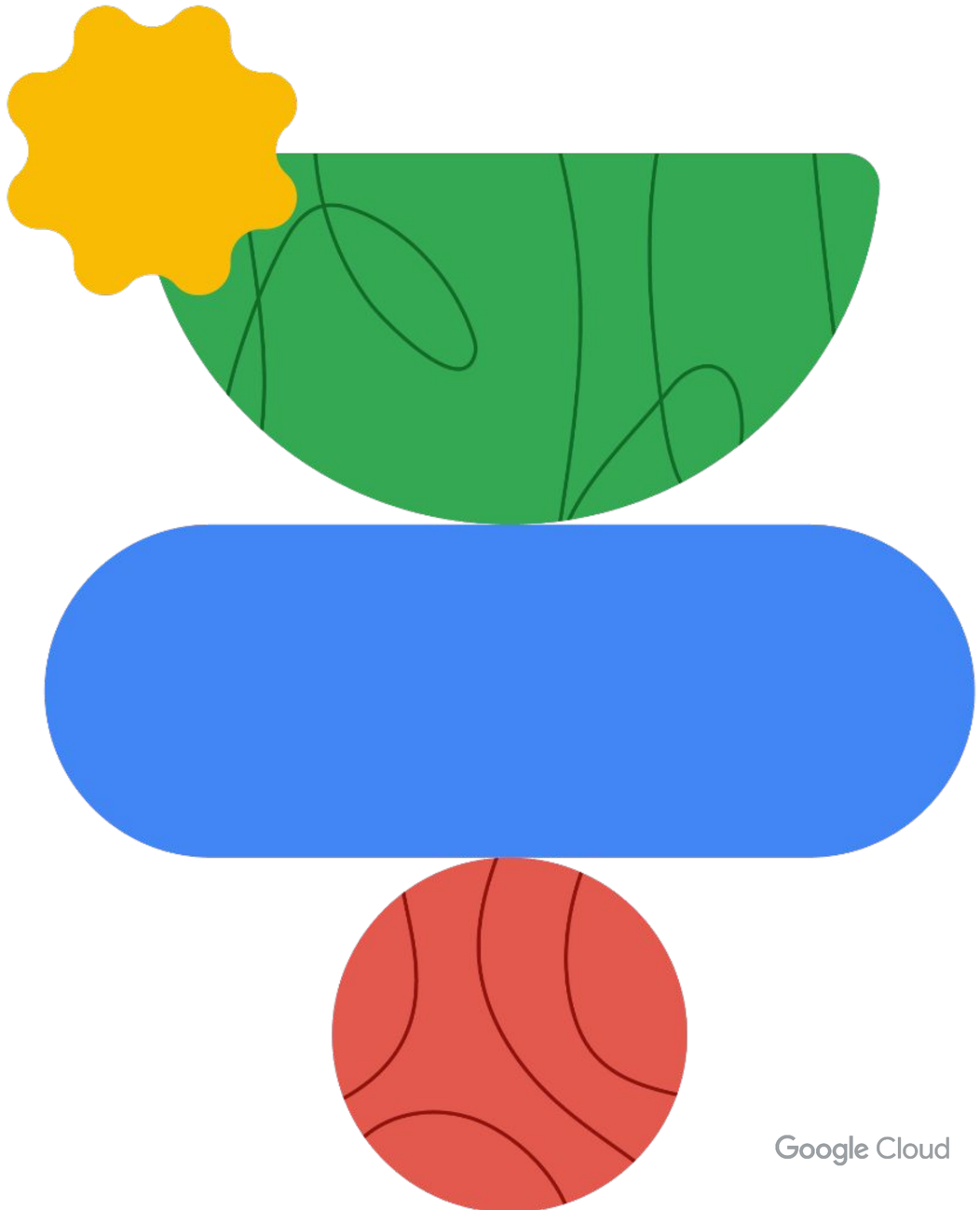
03 Monitoring critical systems

04 Advanced logging and analysis

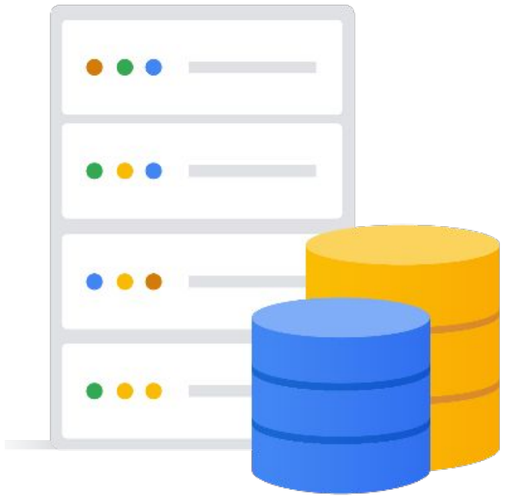
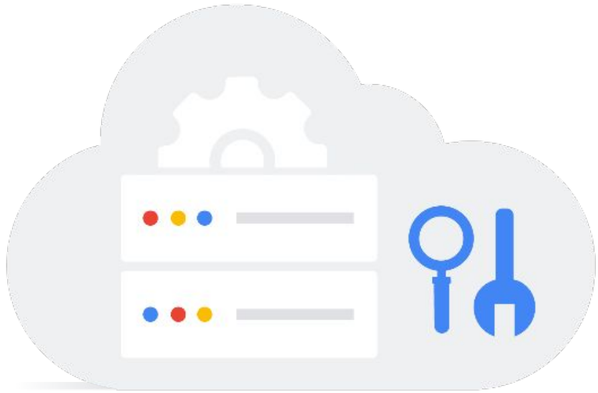
05 Monitoring network security and audit logs

06 Managing incidents

Google Cloud Observability



Need for observability

On-premises	Cloud
	
Physical check	Observability tools

Need for observability

Visibility into system health	Error reporting and alerting	Efficient troubleshooting	Improve performance
Help me understand my application and tell me if it's healthy	Bring my attention directly to problems	Help me fix it if it's broken	Guide me to optimize it

Monitoring gives you real-time system information

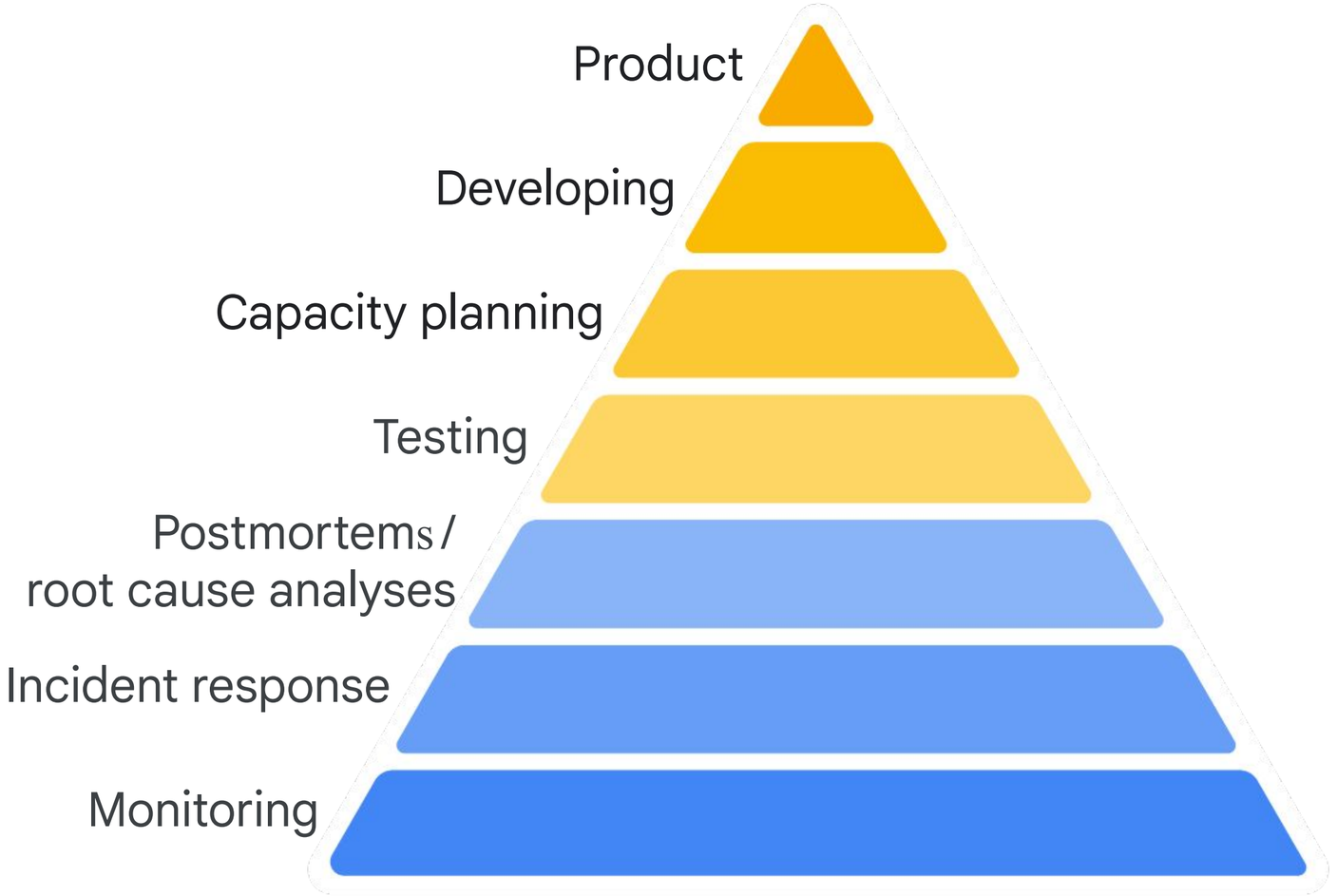
Google's *Site Reliability Engineering* book

landing.google.com/sre/books

Collecting, processing, aggregating, and displaying **real-time quantitative data about a system**, such as:

- Query counts and types
- Error counts and types
- Processing times
- Server lifetimes

Monitoring gives you real-time system information



What’s needed from products

Continual improvement

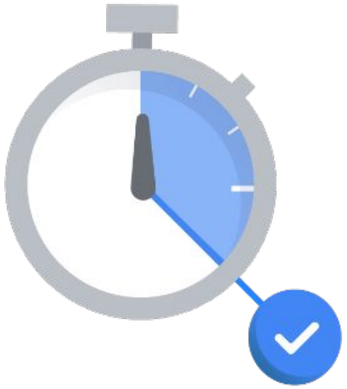
Dashboards

Automated alerts

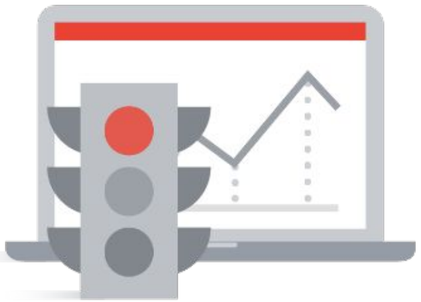
Incident response

Four golden signals

Latency



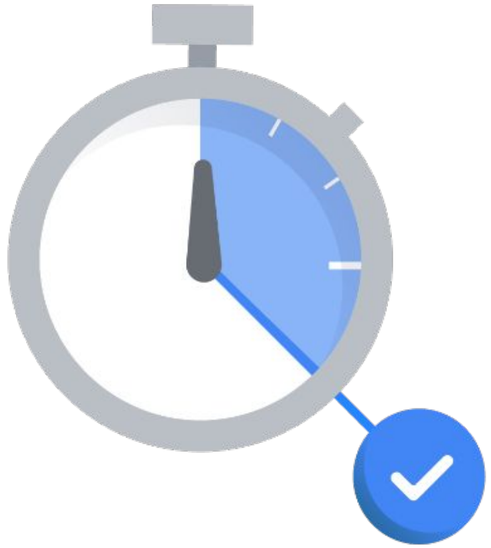
Traffic



Saturation

Errors

The importance of latency



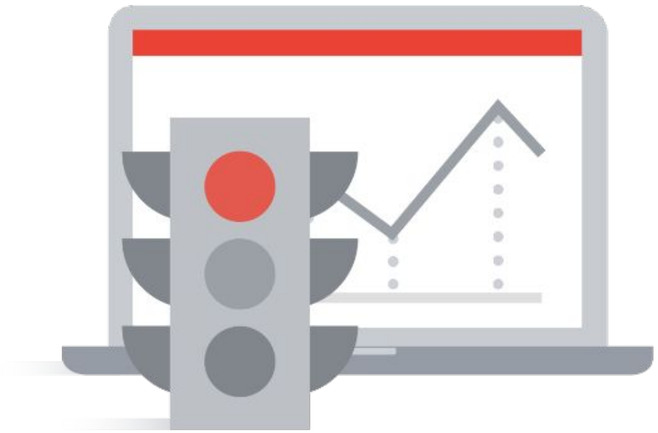
01 Changes in latency could indicate emerging issues.

02 Its values may be tied to capacity demands.

03 It can be used to measure system improvements.

- Page load latency
- Number of requests waiting for a thread

The importance of traffic



01 It’s an indicator of current system demand.

02 Its historical trends are used for capacity planning.

03 It’s a core measure when calculating infrastructure spend.

- # retrievals per second
- # active requests

The importance of saturation

01 It’s an indicator of how full the service is.

02 It focuses on the most constrained resources.

03 It’s frequently tied to degrading performance as capacity is reached.

- % memory utilization
- % thread pool utilization

The importance of errors

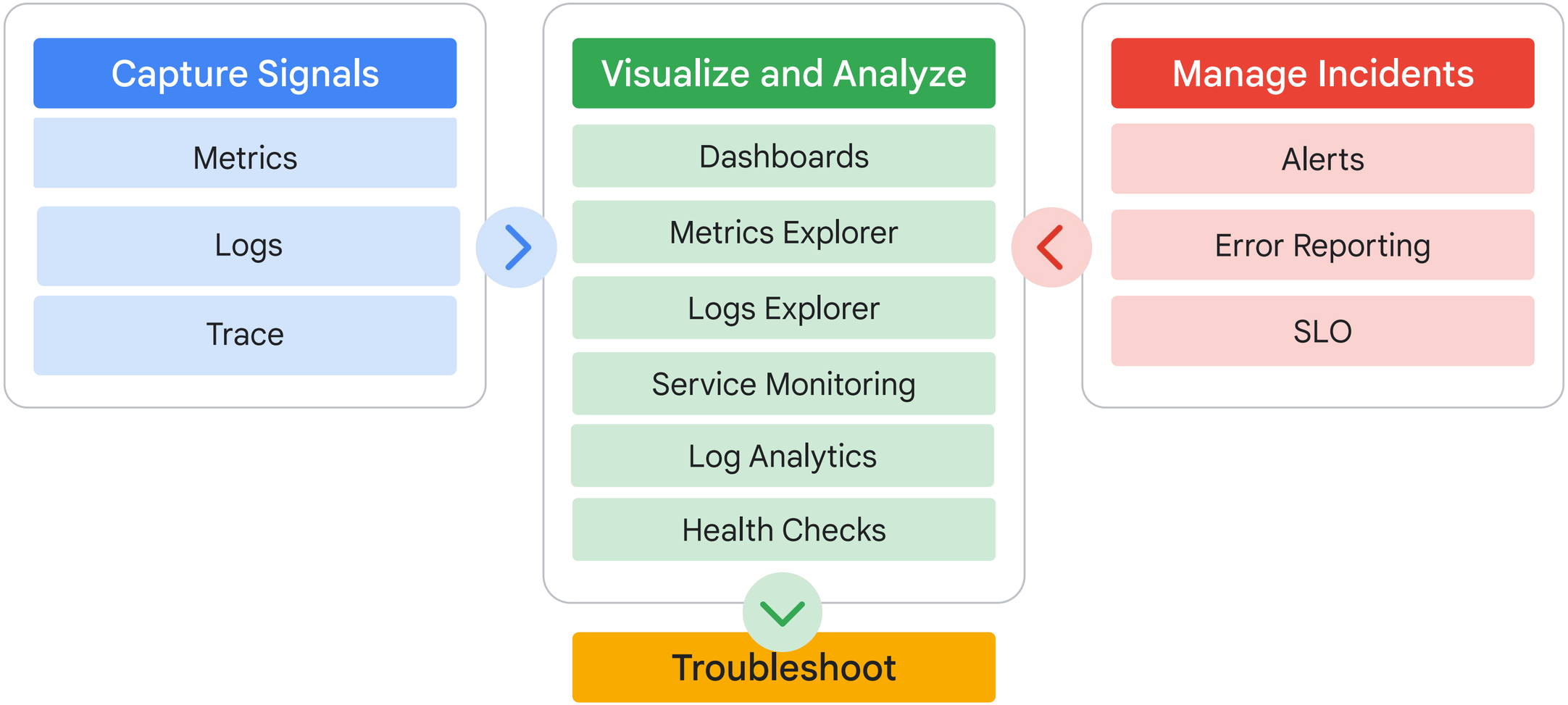
01 They may indicate configuration or capacity issues

02 They can indicate service level objective violations

03 An error might mean it's time to send out an alert

- # failed requests
- # exceptions

Observability concept



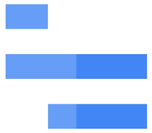
Google Cloud observability

Cloud Monitoring

Cloud Logging

Error Reporting

Cloud Trace



Cloud Profiler

Cloud Monitoring

- Provides visibility into the performance, uptime, and overall health of cloud-powered applications.
- Collects metrics, events, and metadata from projects, logs, services, systems, agents, custom code, and various common application components.
- Ingests that data and generates insights via dashboards, Metrics Explorer charts, and automated alerts.

Cloud Monitoring features

Many free metrics

On 100+ monitored resources services, over 1500+ metrics are immediately available with no cost

Open source standards

Leverage Prometheus and Open Telemetry to collect metrics across compute workloads

Customization for key workloads

Tune with Managed Service for Prometheus on GKE and Cloud Ops Agent on Compute Engine

In-context visualizations & alerts

View relevant telemetry data alongside your workloads across Google Cloud

Cloud Logging

- Allows users to collect, store, search, analyze, monitor, and alert on log entries and events.
- Provides automatic ingestion with simple controls for routing, storing, and displaying your log data.
- Leverage tools like Log Analytics to view trends, or Error Reporting and Log Explorer to quickly examine problems.

Logging has multiple aspects

Collect	• Cloud events, configuration changes, and from customer services • Logs at various level of the resource hierarchy
Analyze	• Log data in real time with the integrated Logs Explorer • Run queries and analyze with Log Analytics • Exported logs from Cloud Storage or BigQuery
Export	• Export to Cloud Storage, or Pub/Sub, or BigQuery • Logs-based metrics for augmented Monitoring
Retain	• Data access and service logs for 30 days and admin logs for 400 days • Longer-term in Cloud Storage or BigQuery

Developers use cases

Developers

- Troubleshooting
- Debugging

Get started quickly – Out-of-the-box collection of system metrics and logs

Use logging SDKs and library – Integration into popular SDKs to support rich log formatting

Analyze log in real-time – Analyze log data in real-time, debug code, troubleshoot your apps

Find errors quickly – Find errors via stack traces automatically with Error Reporting

Operators use cases

Operators

- SLO/alerting
- Log management
- Workload management
- Cost management

Collect the right telemetry – Instrumentation for Compute Engine, on-prem and other cloud providers

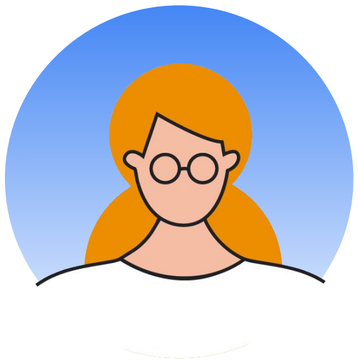
Centralize logs – Centralize logs for specific users, teams and/or organizations

Manage logs – Set retention periods, select supported regions for regional data storage

Set alerts – Understand log volume/cost, set alerts on important application metrics

Export logs – Export to Google Cloud for storage, analysis, integrate with 3rd parties

Security operations use cases



SecOps Analyst

Ensures Google Cloud resources are operated securely, using platform features to comply with organizational security needs.

Collect audit logs – Collect Google Cloud audit logs by default, advanced security logs such as data access logs

Collect network telemetry data – Collect and analyze VPC flow logs, GKE network, firewall, load balancer logs

Analyze logs for security events – View audit logs and other events to investigate possible security events

Error Reporting

Error Reporting **identifies, counts, analyzes, and aggregates** the crashes in your running cloud services.

Error Reporting features

Real time processing

Applications errors are processed and displayed within seconds

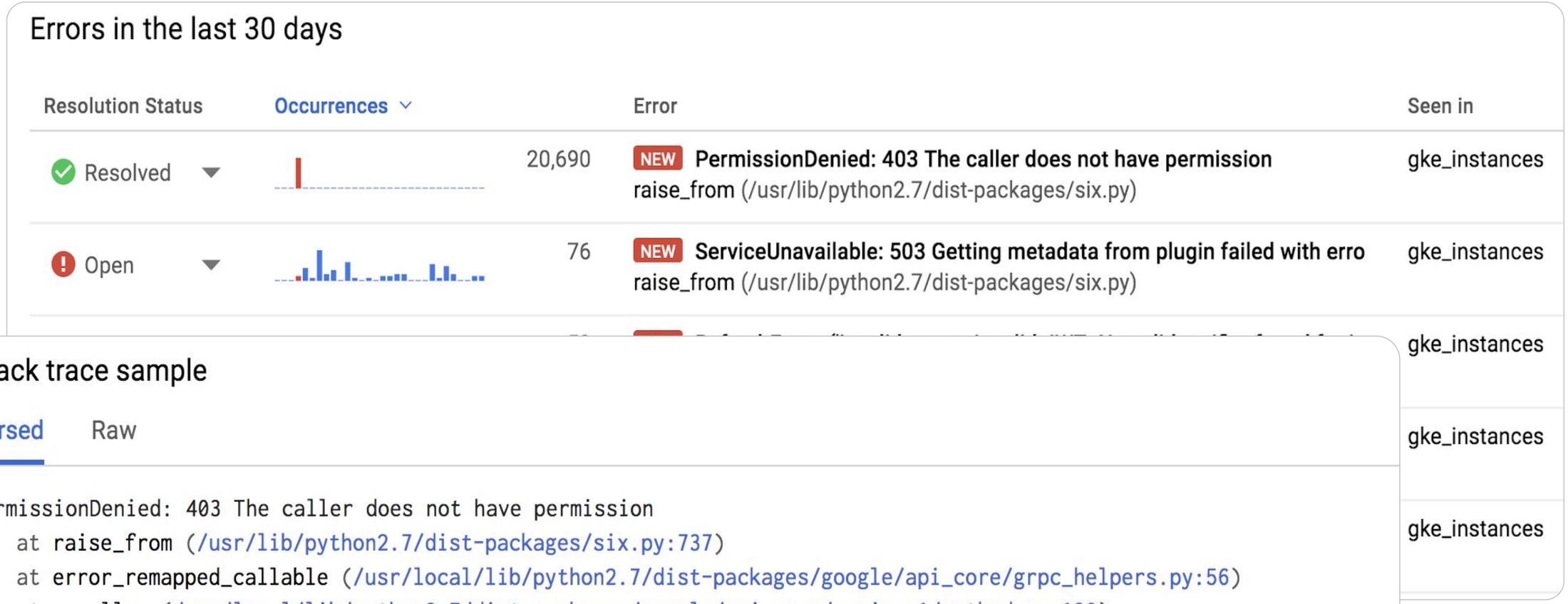
Quickly view and understand errors

A dedicated page displays the details of the error

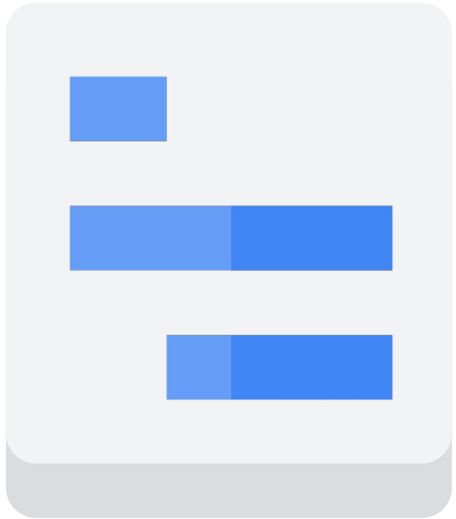
Instant notification

You are notified when events occur

Error Reporting interface



Cloud Trace



- Collects latency data from distributed applications and displays it in the Google Cloud console.
- Captures traces from applications deployed on App Engine flexible and standard environment, Compute Engine VMs, Google Kubernetes Engine containers, Cloud Run and non-Google Cloud environments.

Latency reports

Cloud Profiler

- Uses statistical techniques and extremely low-impact instrumentation to provide a complete picture of an application.
- Allows developers to analyze applications running anywhere.
- Presents the call hierarchy and resource consumption of the relevant function in an interactive flame graph.

Google Cloud Observability

Explores the known and unknown issues

User-focused products

Understand a customer's journey with SLO monitoring, uptime checks, tracing and more.

Open, flexible foundations

Leverage popular open source projects like Prometheus, OpenTelemetry, and Fluentbit.

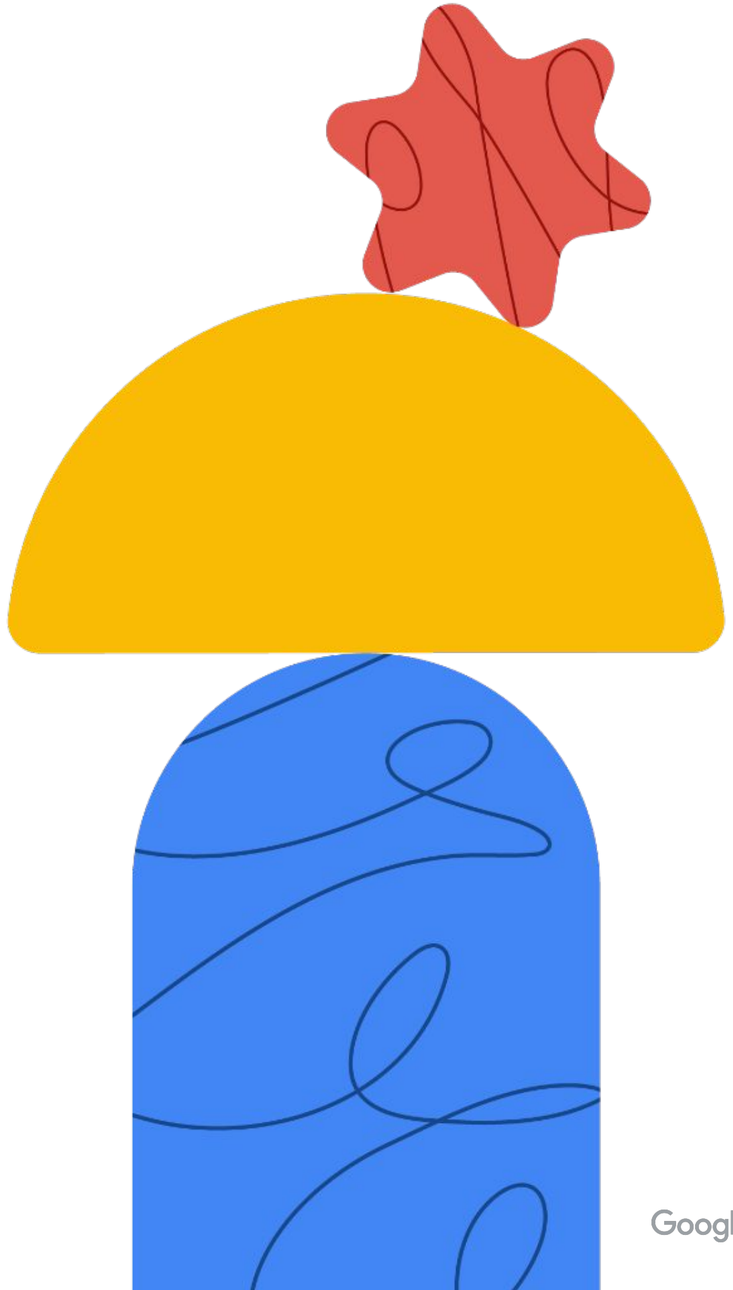
Integrated for ease

Automatically ingest log, connect data sets, collect in-context telemetry across Google Cloud service.

Analysis and alerting

Use powerful analysis tools and leverage alerting for both automated and human-led resolutions.

Alerting policies



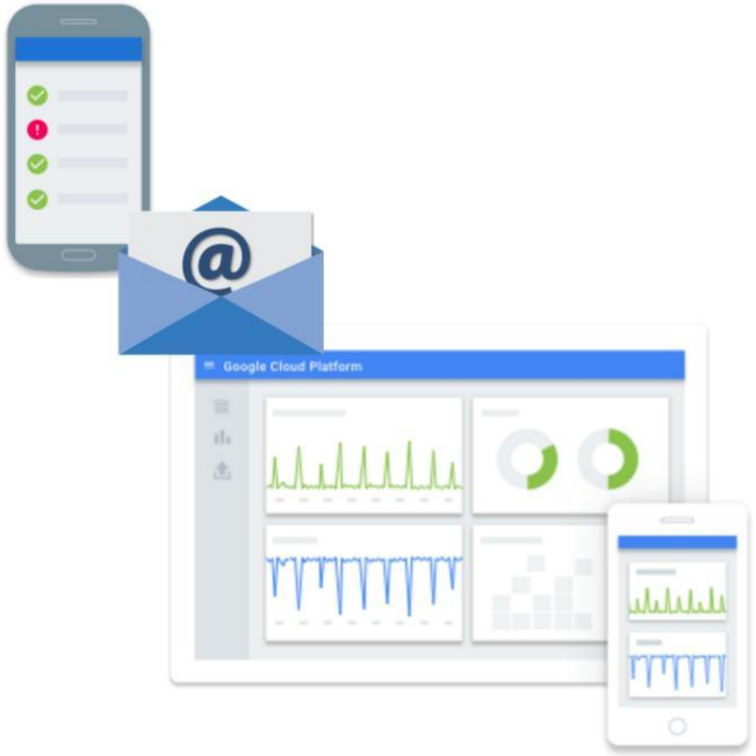
Goal

A person is notified when:

1. A service is down.
2. SLOs or SLAs are not being met.
3. Something needs to change.

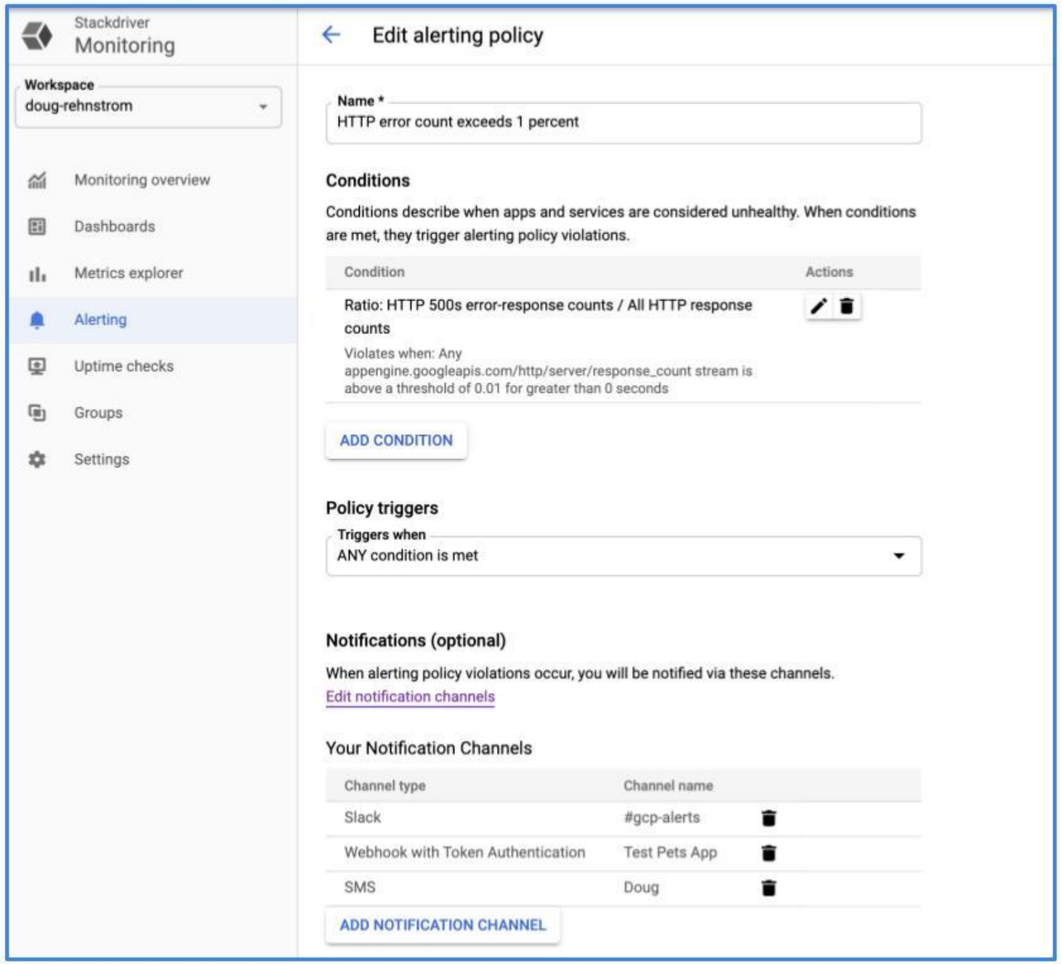
Prioritize alerts based on customer impact and SLA

- Involve humans only for critical alerts.
- Send a message to your team's Slack channel or use SME for high-priority alerts.
  - Pagerduty
- Log low-priority alerts for later analysis.
  - Ticket
  - Email

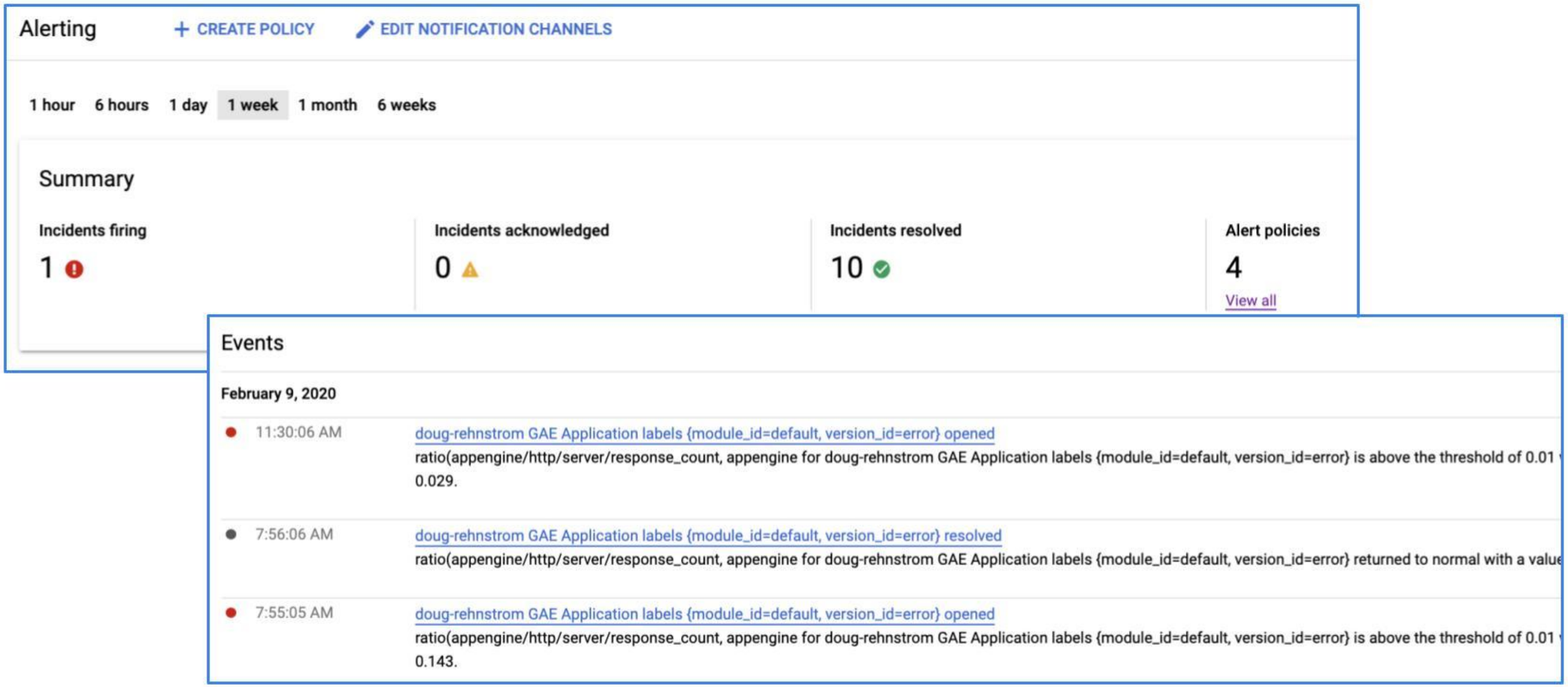


Use alerting policies to define alerts

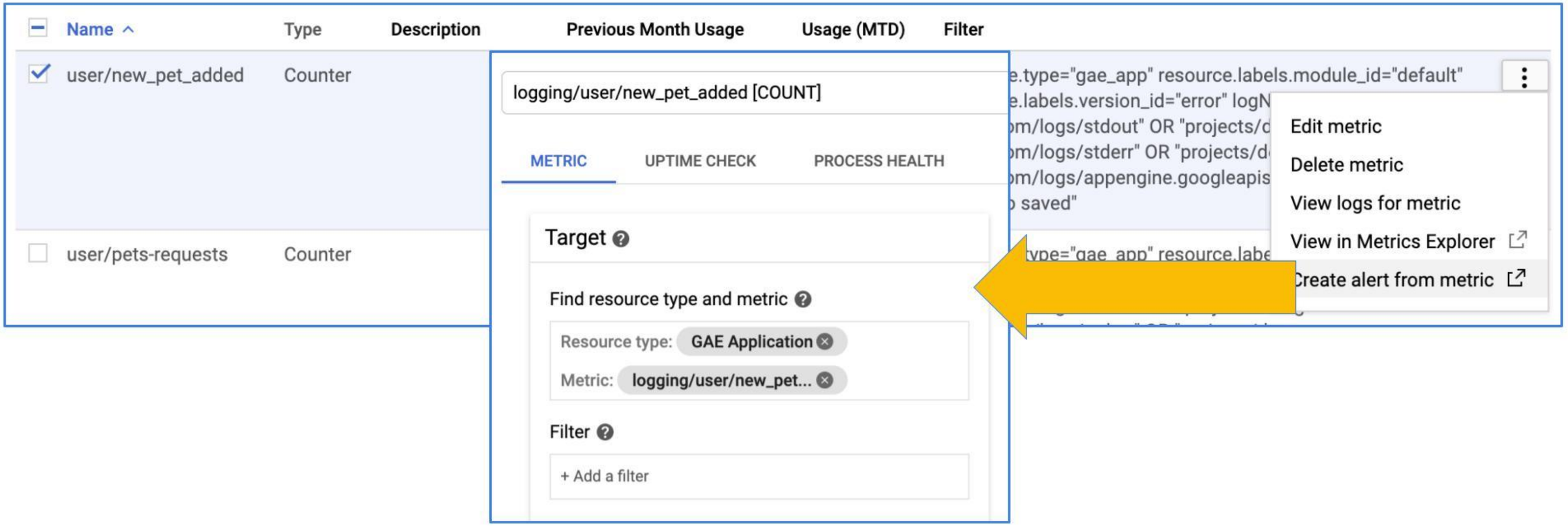
- An alerting policy has:
  - A name
  - One or more conditions
  - Notifications
  - Documentation



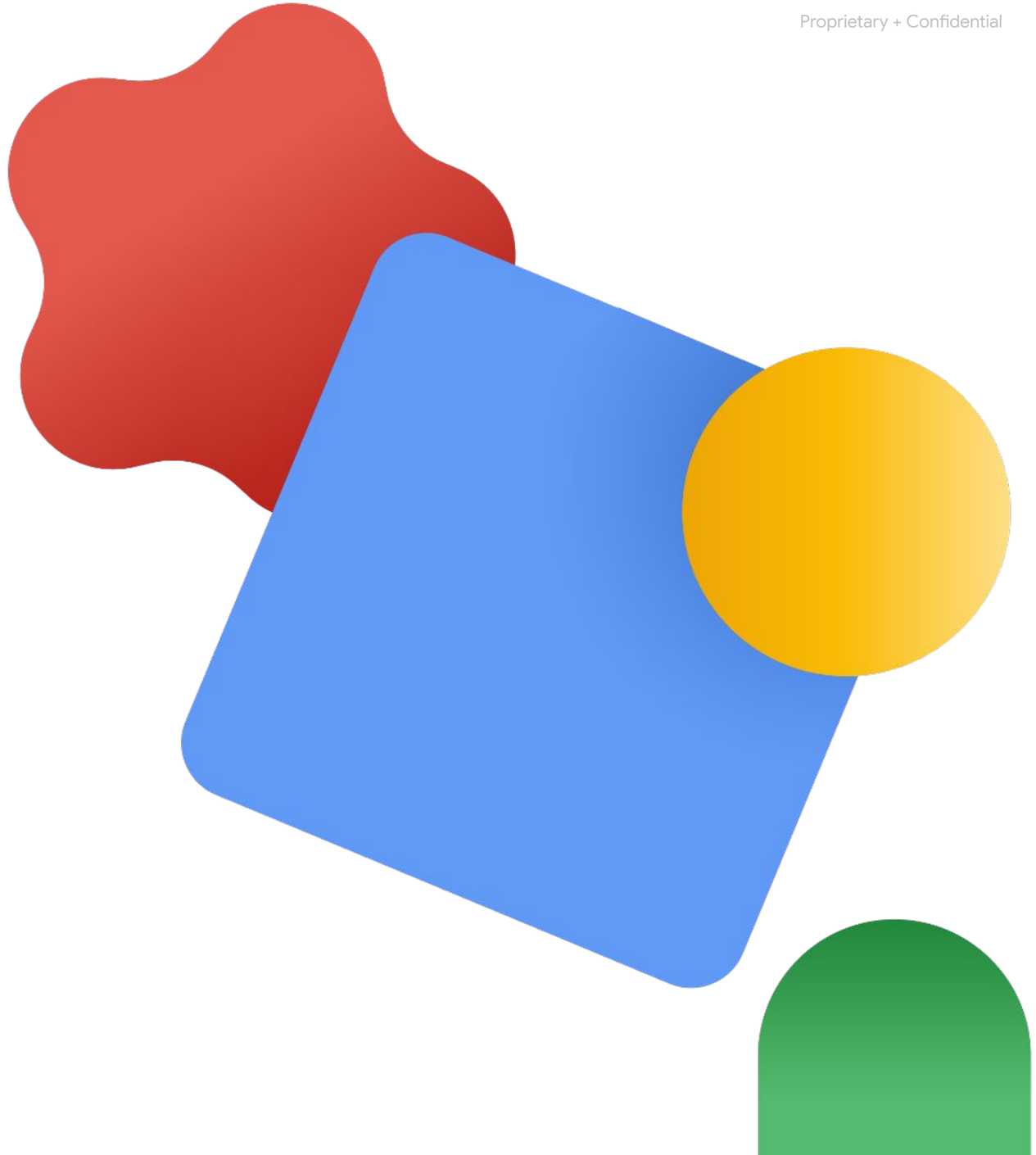
Alerting UI summarizes incidents and events



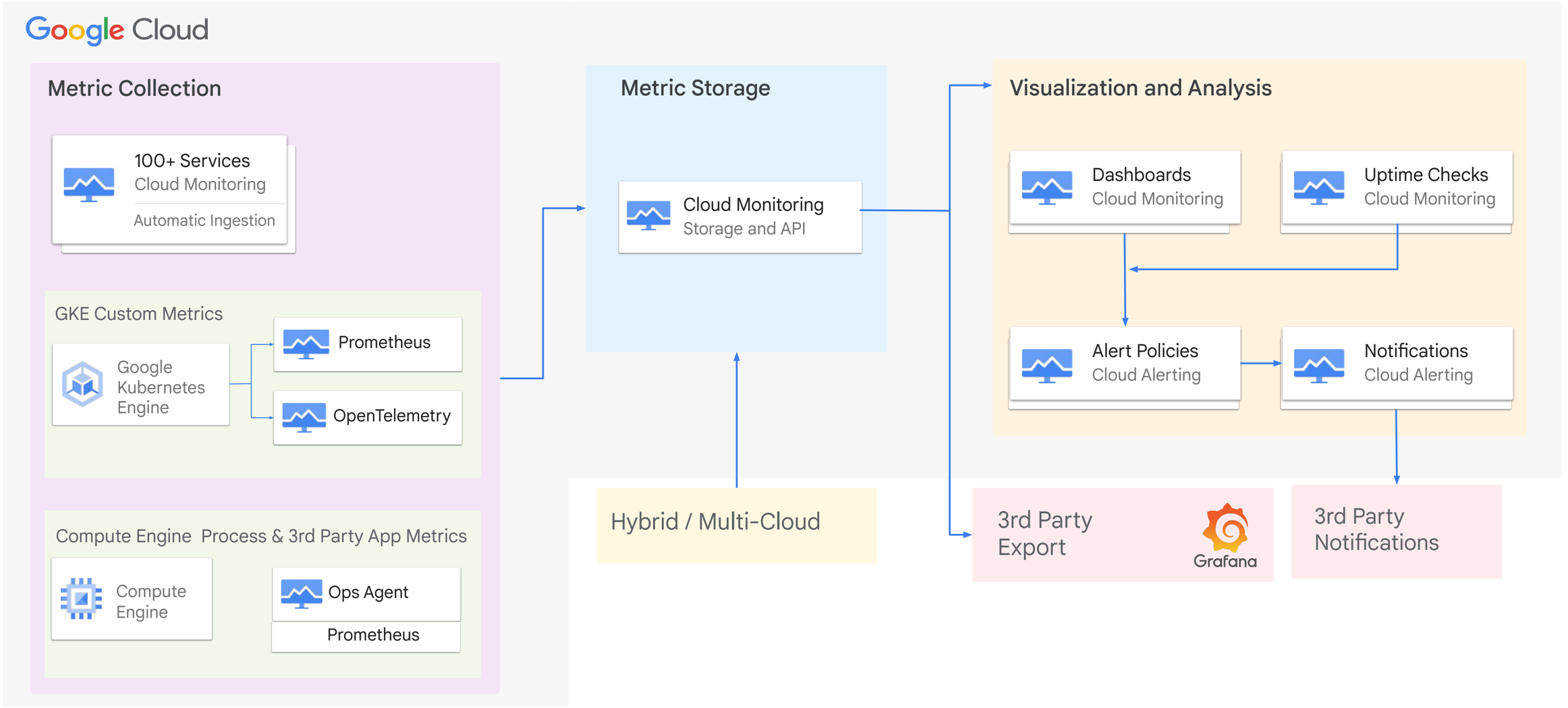
Attach alerts to logs-based metrics



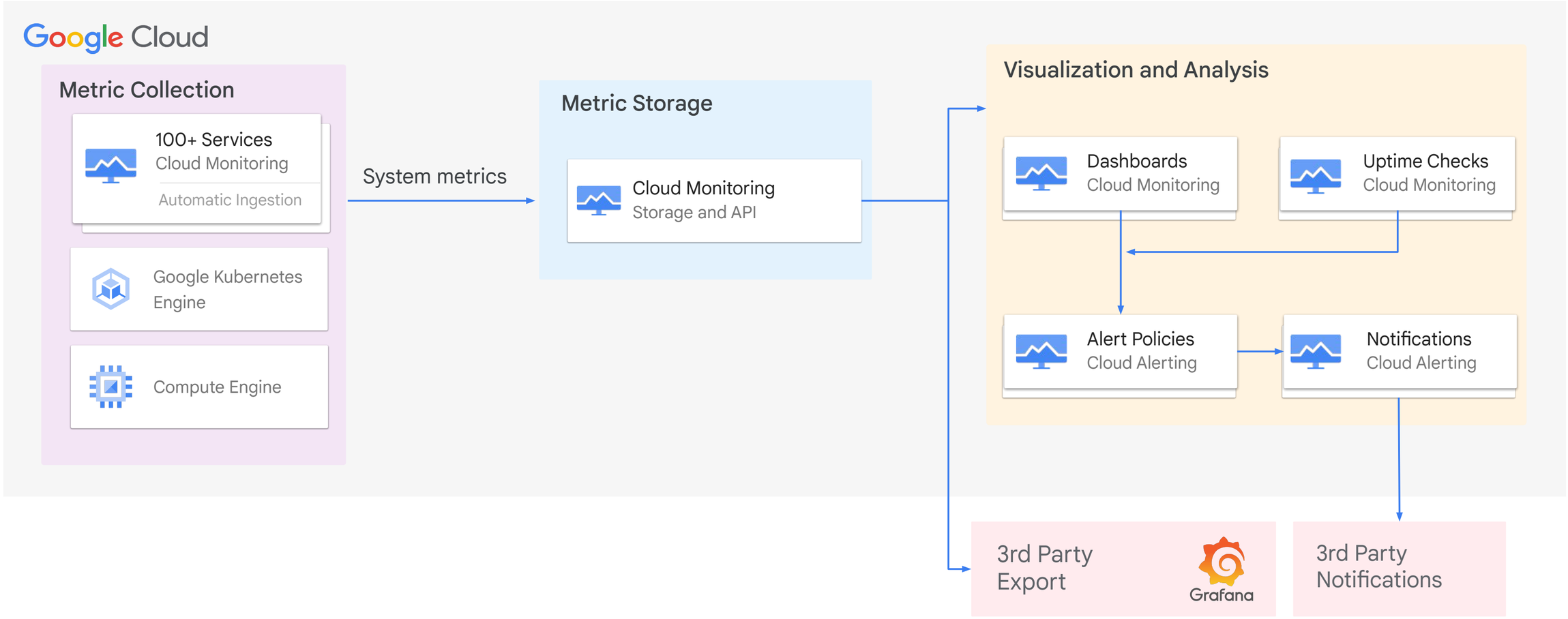
Monitoring critical systems



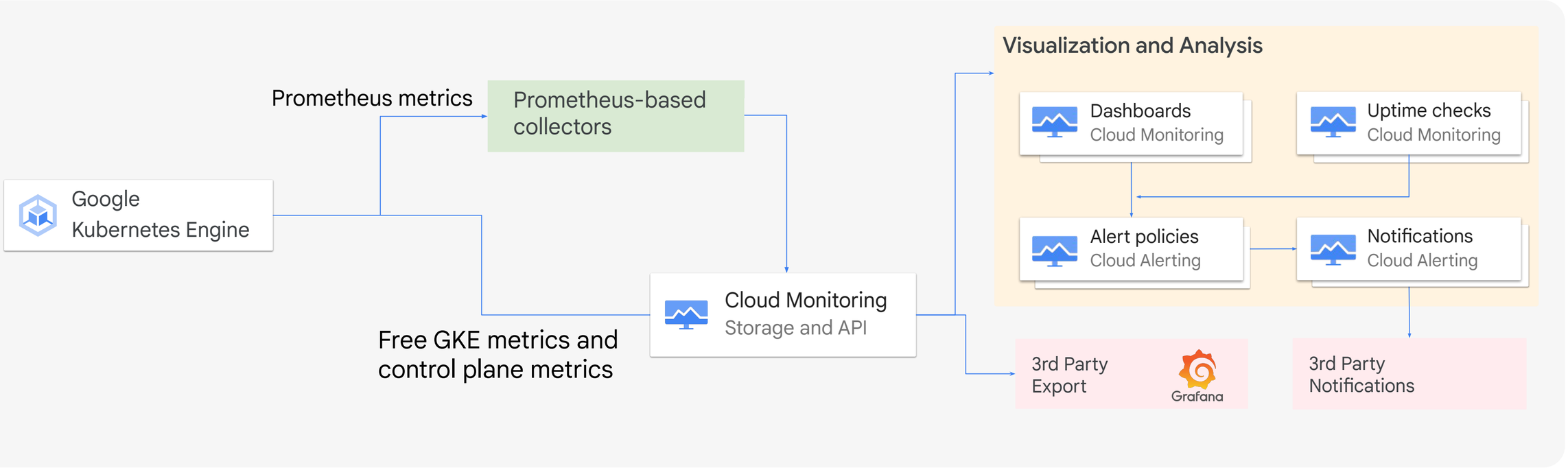
Cloud Monitoring architecture



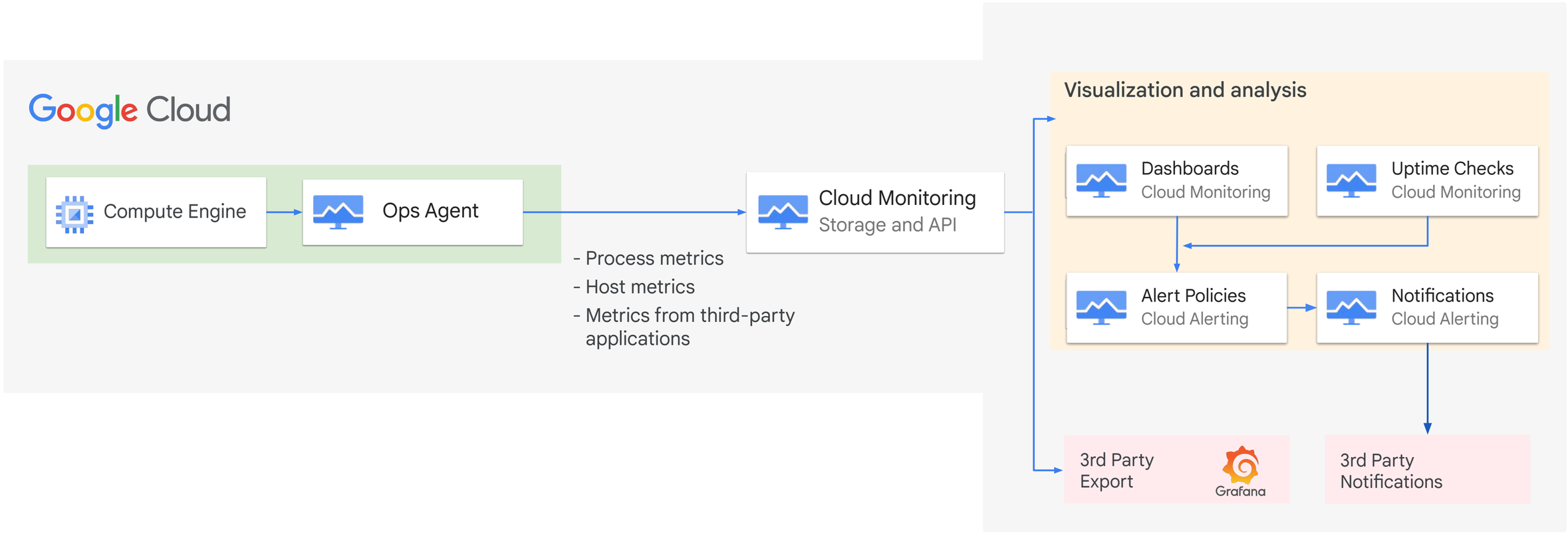
Platform monitoring



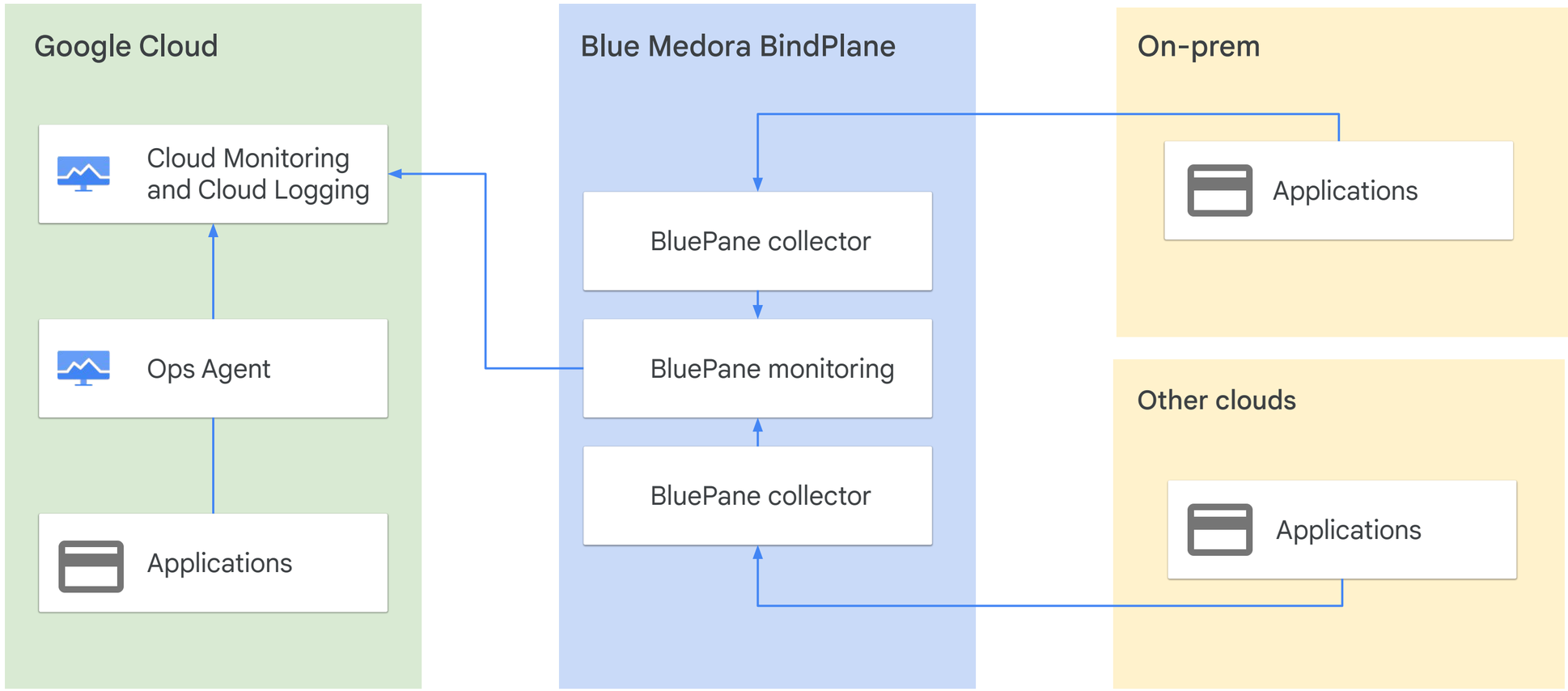
Application monitoring - GKE



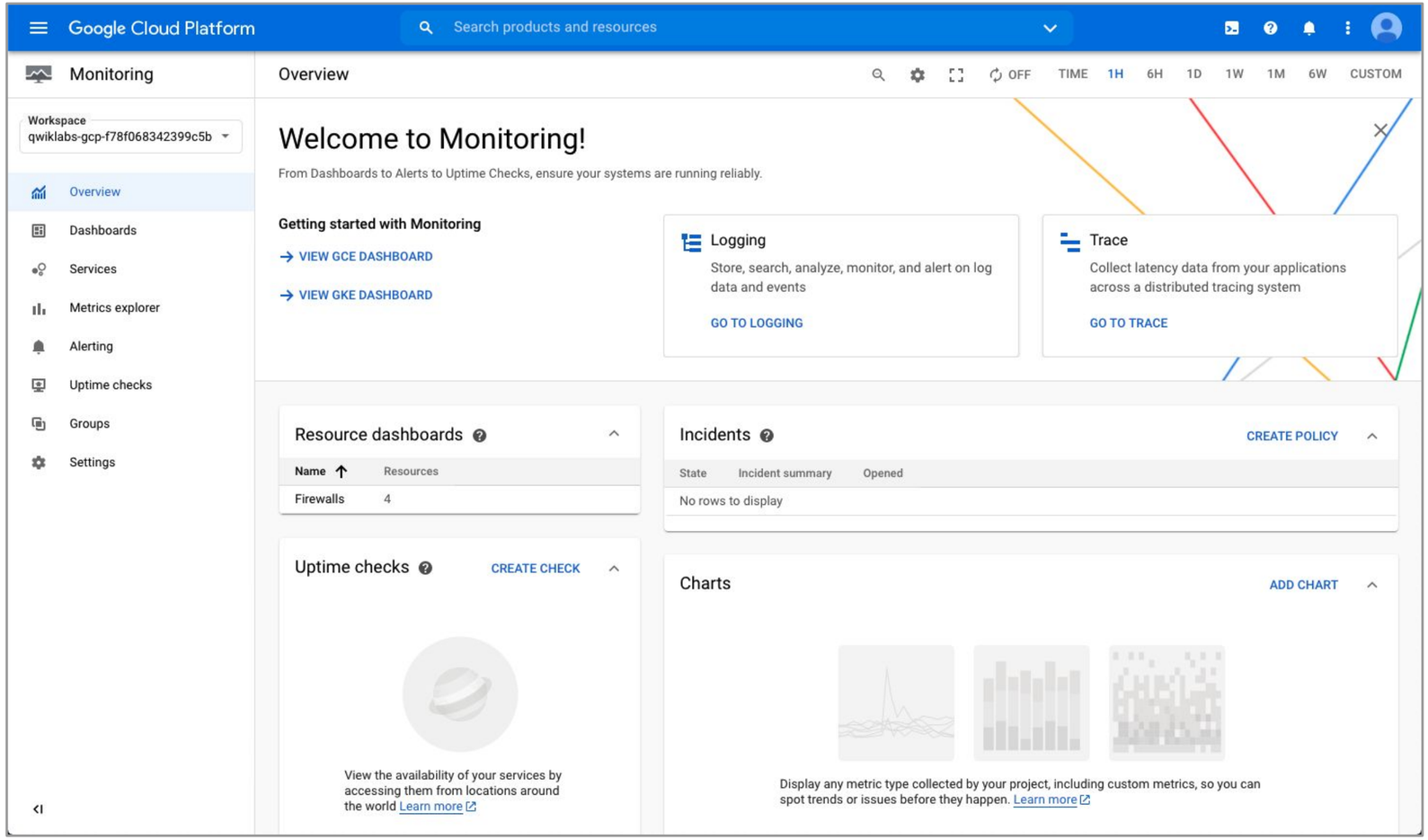
Application monitoring – Compute Engine



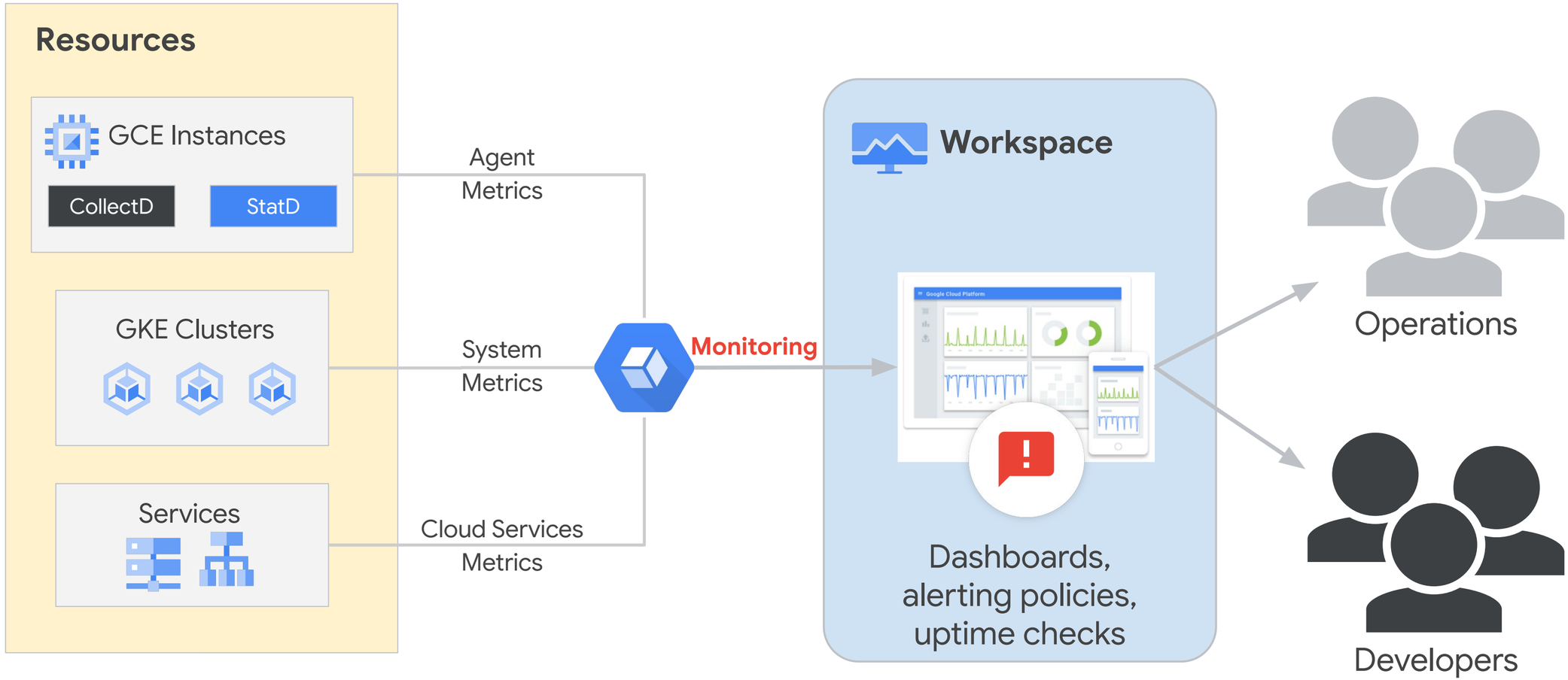
Hybrid monitoring and logging



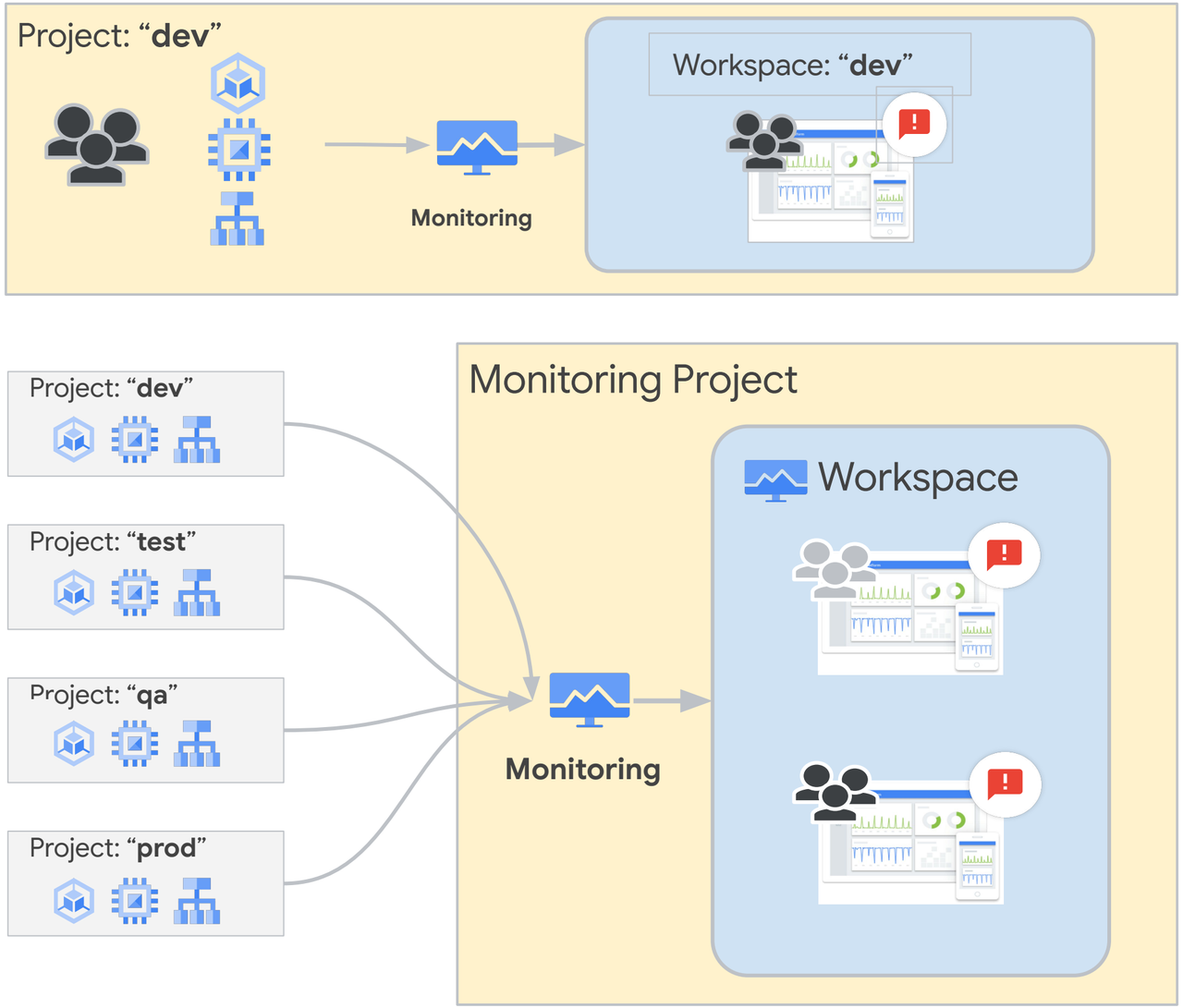
Monitoring is configured via workspaces



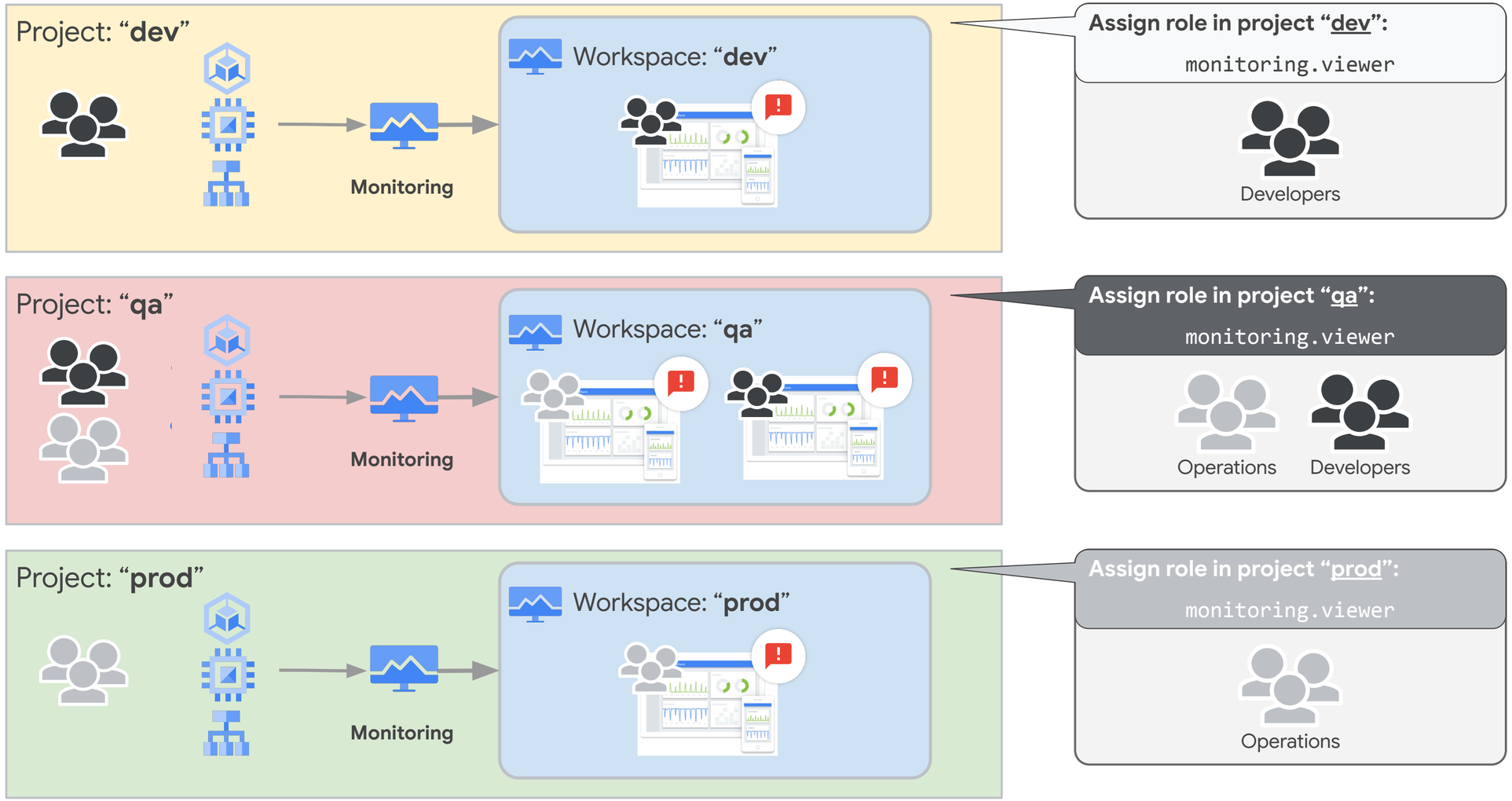
Organize your monitoring efforts with workspaces



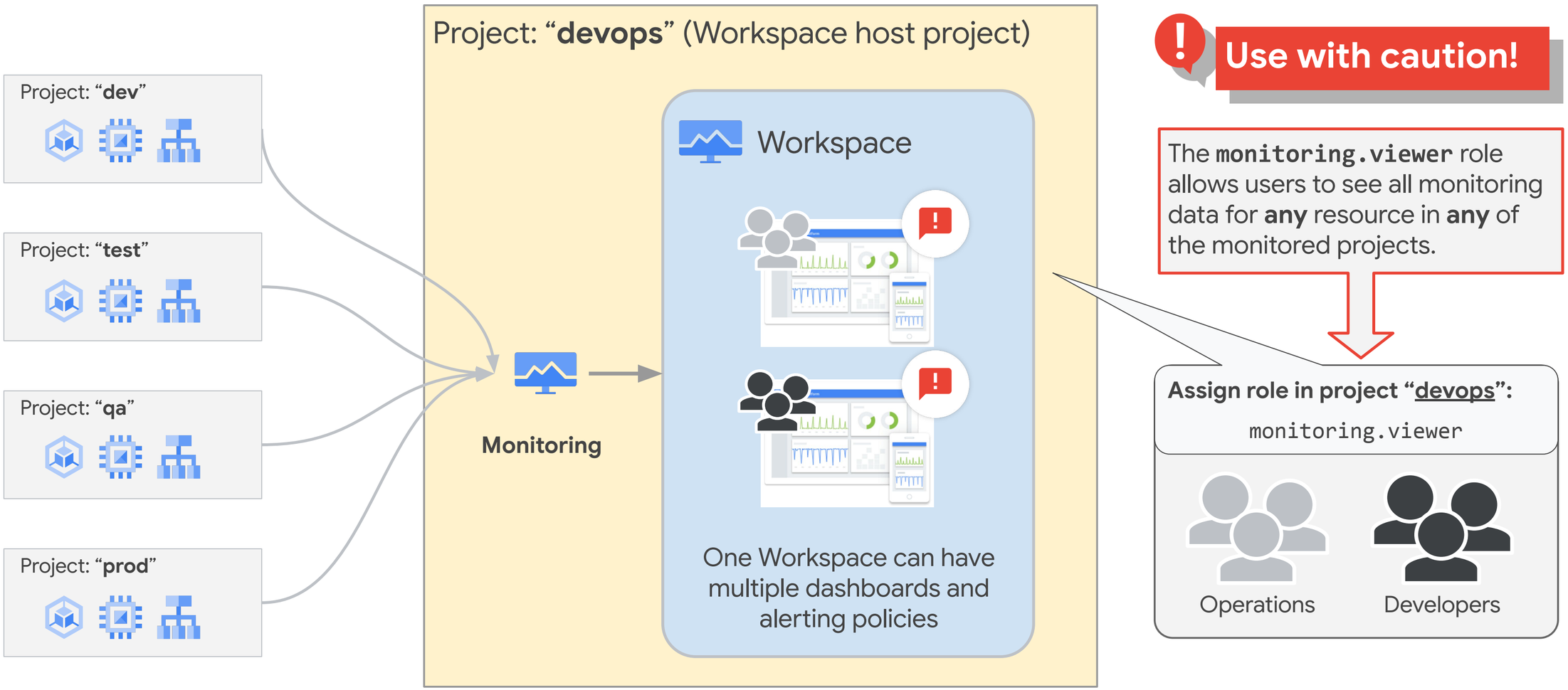
Two options for monitoring Workspace architectures



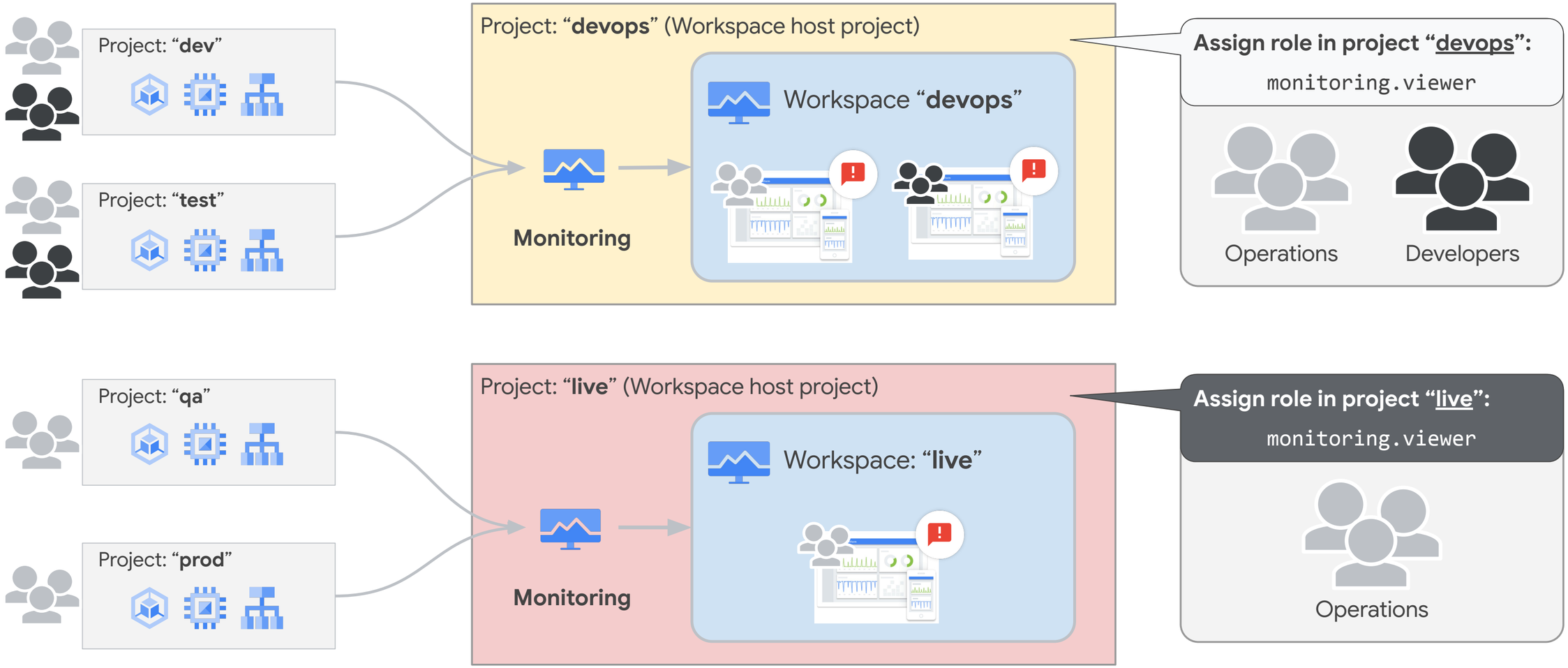
Monitor by project for maximum isolation



One Workspace can monitor multiple projects



Logical groupings can be very effective



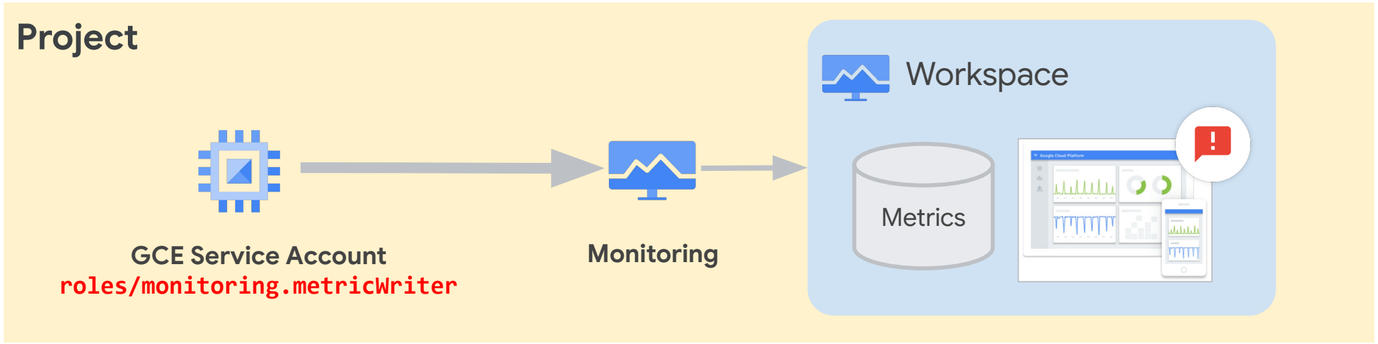
IAM roles control user access to workspaces

To initially create the monitoring workspace, a user will need the Monitoring Editor or Monitoring Admin role in the workspace host project.

Role Name	Description
Monitoring Viewer	Gives you read-only access to the Monitoring console and API
Monitoring Editor	Gives you read-write access to the Monitoring console and API, and lets you write monitoring data to a workspace
Monitoring Admin	Gives you full access to all Monitoring features

Services may need permission to add metric data

For example, the service account of a GCE instance with the monitoring agent installed - grant the service account the Monitoring Metric Writer role in the Workspace host project.



Monitoring Metric Writer

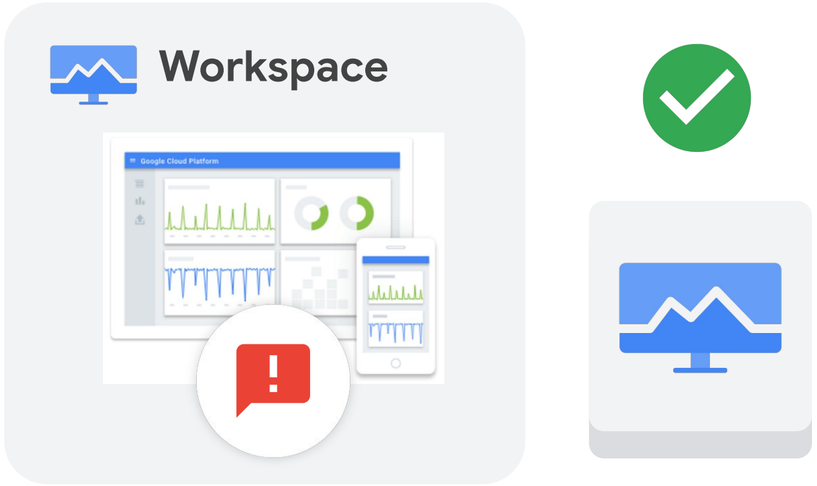
Permits writing monitoring data to a Workspace.

This does not permit read access to the Monitoring console.

Typically this permission is used by service accounts.

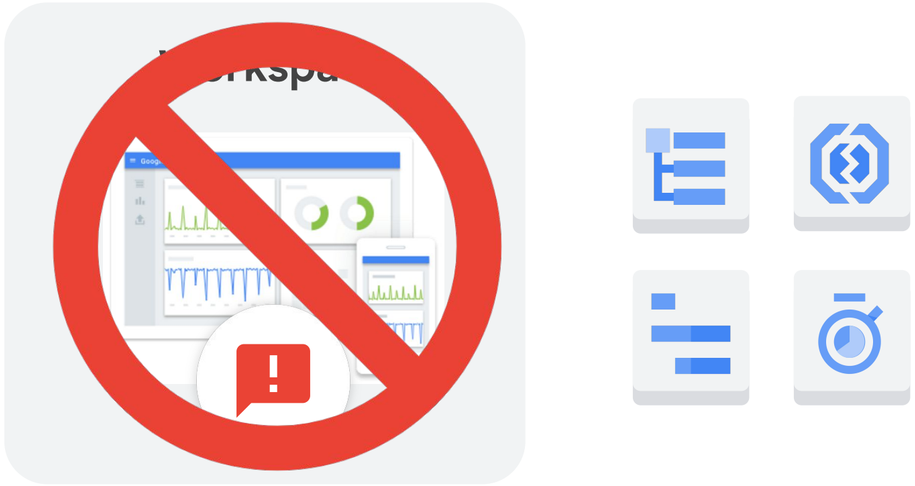
Remember, workspaces only affect monitoring

Only the Monitoring system relies upon workspaces.

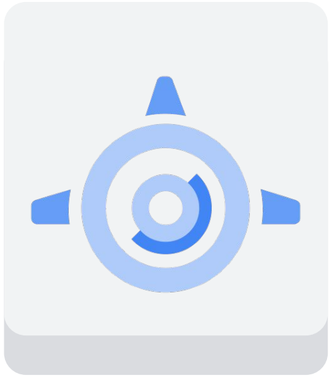


The other tools in this course:

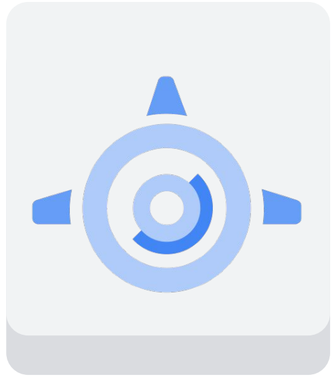
- Are configured on a per-project basis.
- Have their own Cloud IAM roles.



Built-in monitoring



App Engine
Flexible environment



App Engine
Standard
environment

Google Kubernetes
Engine

Istio

Ops Agent

01

Primary agent for collecting telemetry from your Compute Engine instances.

02

Monitor your VM instances without the need for any additional configuration after the install.

03

Gain visibility into CPU, disk, and network performance.

04

Unify gathering of metrics and logs into a single agent.

05

Replaces the legacy Monitoring and Logging agents that Google Cloud offered.

Monitoring third-party applications

Applications

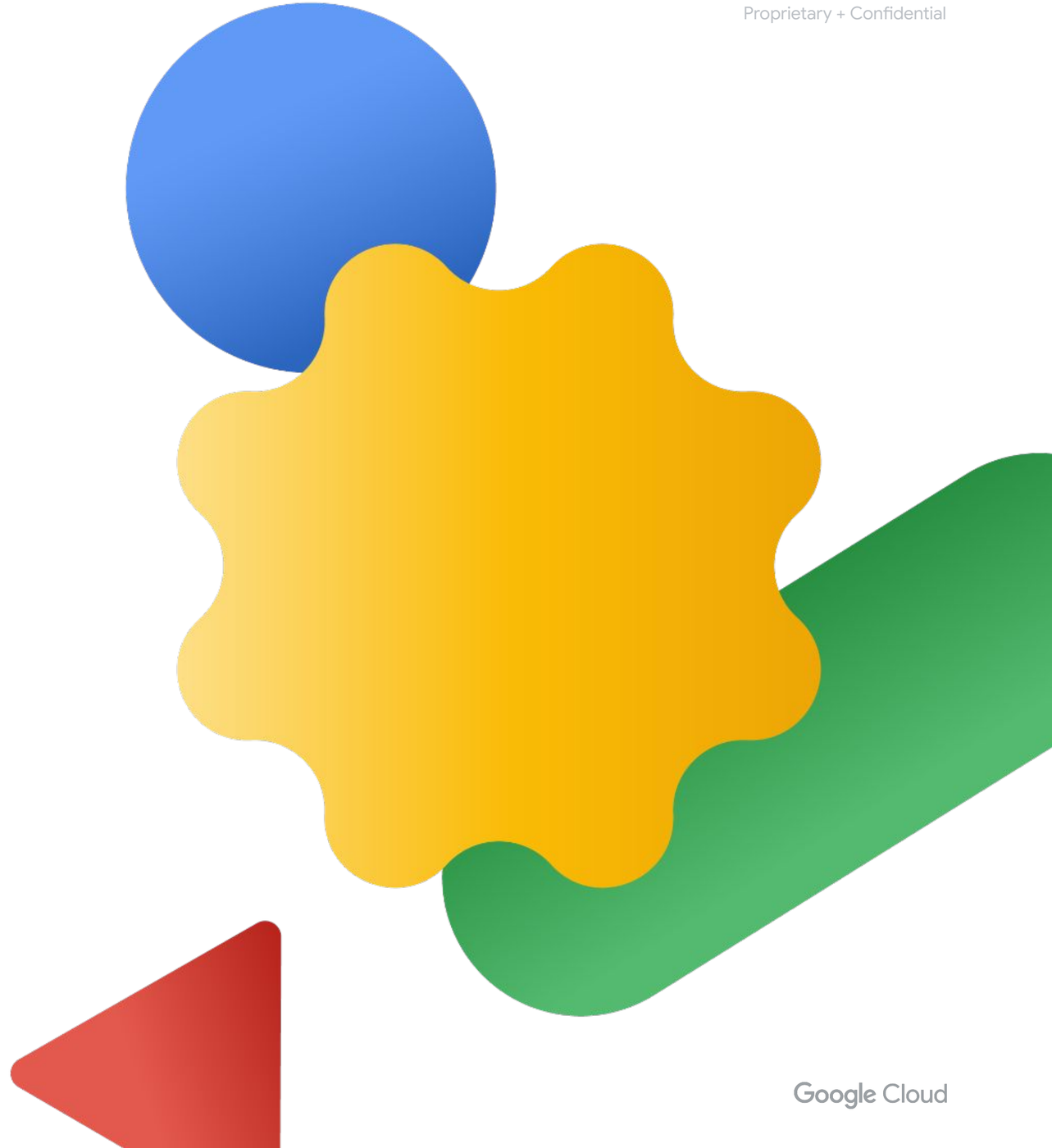
- Apache web saver
- Cassandra
- CouchDB
- Elasticsearch
- HBase
- JVM Monitoring
- Kafka
- Memcached
- MongoDB

Monitoring third-party applications

Applications

- MySQL
- Nginx
- PostgreSQL
- RabbitMQ
- Redis
- Riak StatsD
- Tomcat
- Varnish
- ZooKeeper

Advanced logging and analysis



Cloud Logging help you understand your application

Gather data from various workloads

Gathers the information required to troubleshoot and understand the workload and application needs

Analyze large volumes of data

Tools like Error Reporting, Log Explorer, and Log Analytics let you drive insights from large sets of data

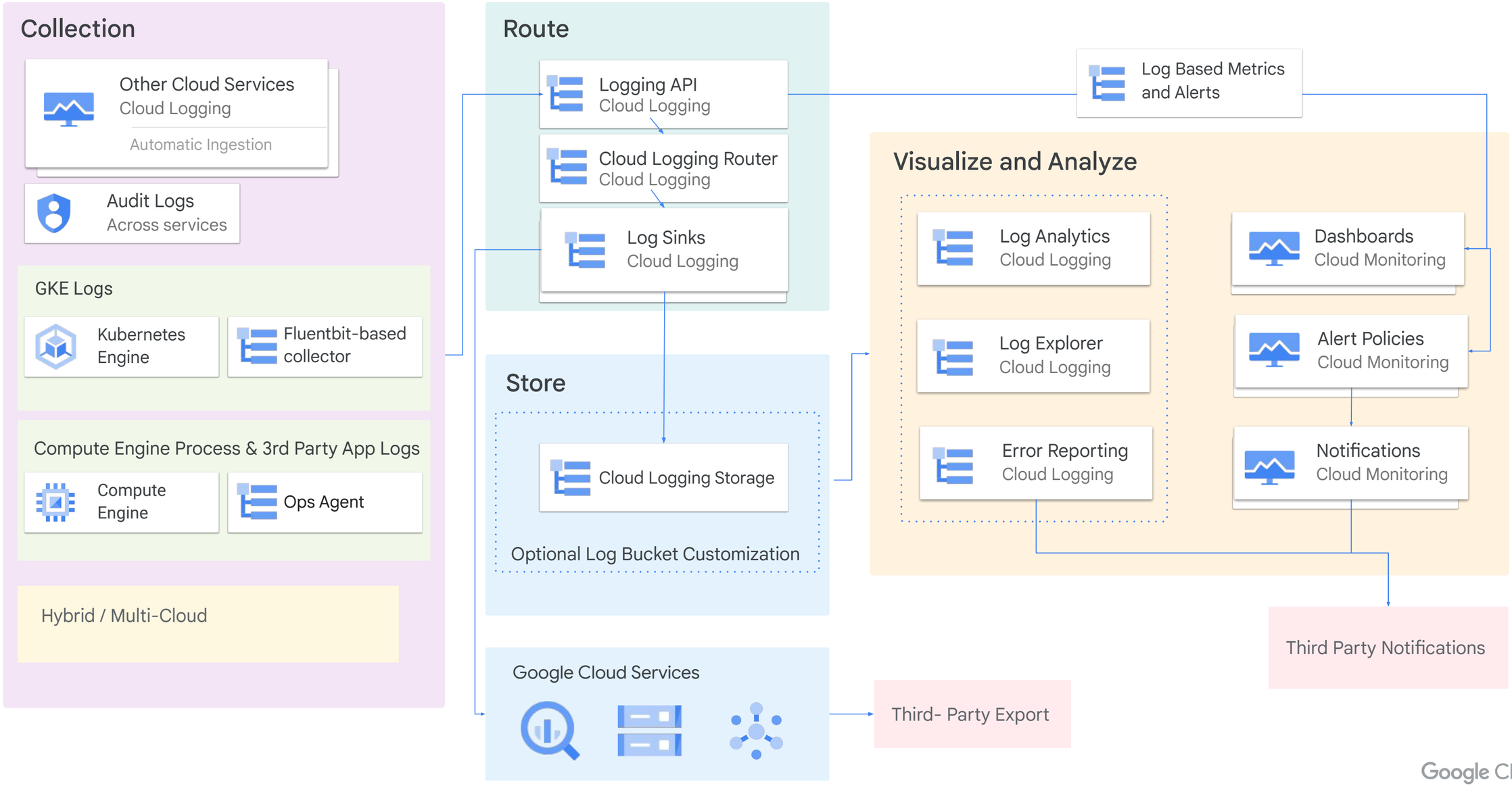
Route and store logs

Route your logs to the region or service of your choice for additional compliance or business benefits

Get compliance insights

Leverage audit and app logs for compliance patterns and issues

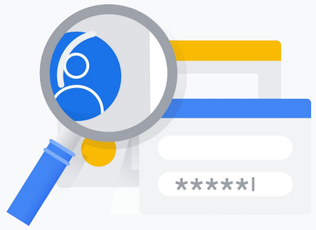
Cloud Logging architecture



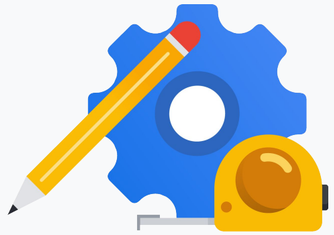
Available logs

Platform logs

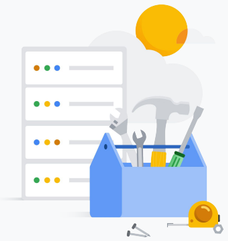
Component logs



Security logs



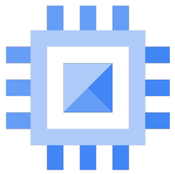
User-written logs



Multi / Hybrid Cloud logs

Logs collection in Google Cloud

Some logs from Google Cloud resources are collected automatically.

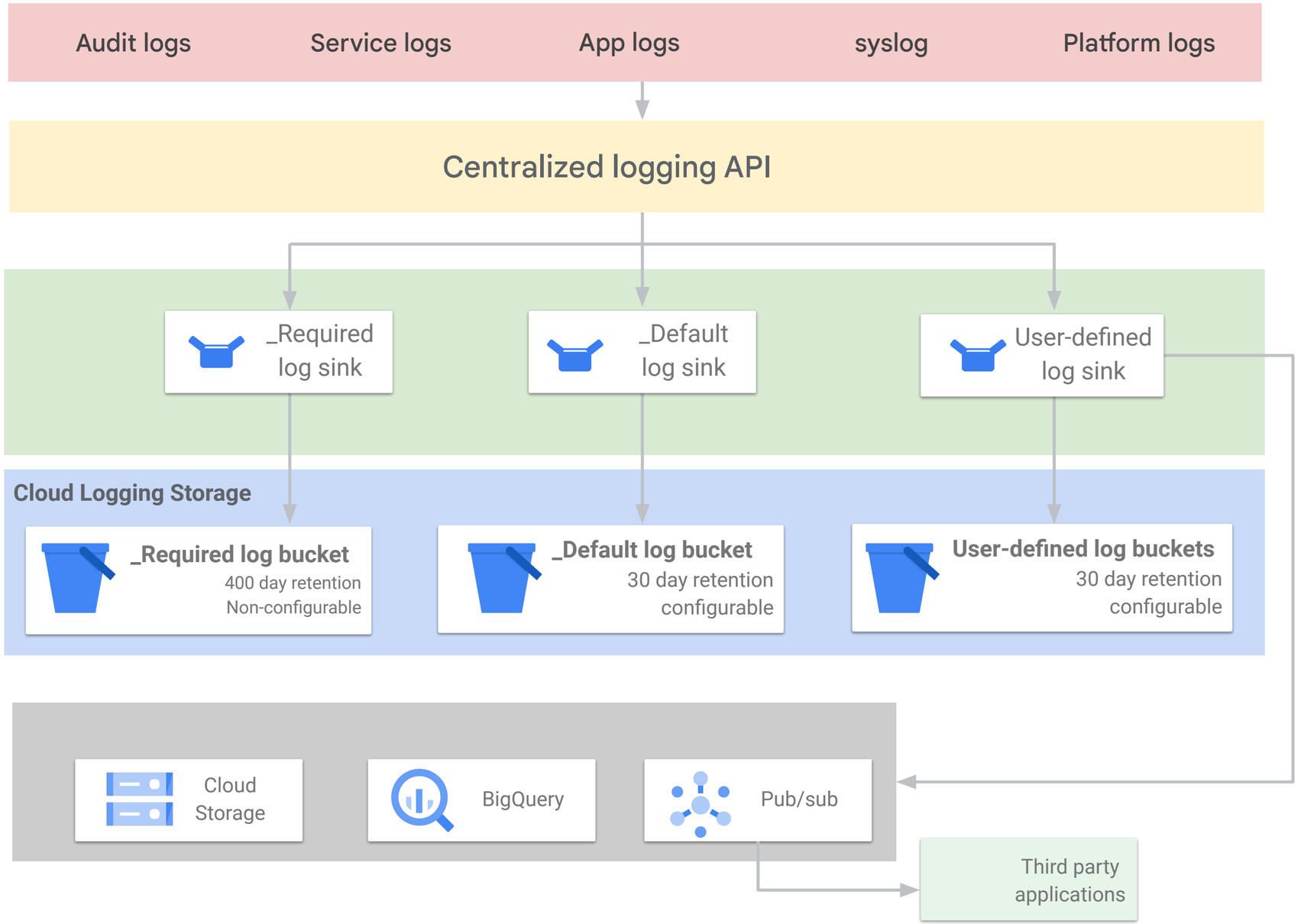
	Google Kubernetes Engine	Compute Engine	Serverless compute services
			
Cloud Logging	Logs written to **stdout and stderr** are collected automatically	Install the **Ops Agent** on your VMs	Logs written to **stdout** and **stderr** are collected automatically

Log routing and storage

Cloud Logging receives log entries through Cloud Logging API.

Sinks contain the inclusion and exclusion filters that determine the log destination.

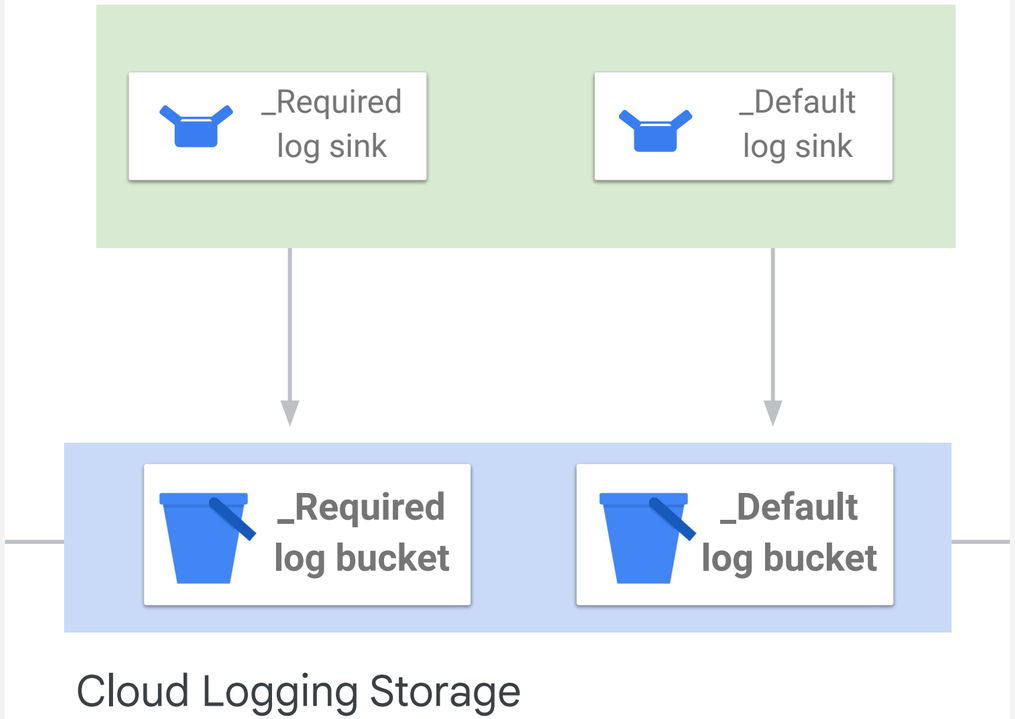
Cloud Storage buckets are different storage entities than Cloud Logging buckets.



Google Cloud Logging: Automatic Log Bucket Creation

`_Required`

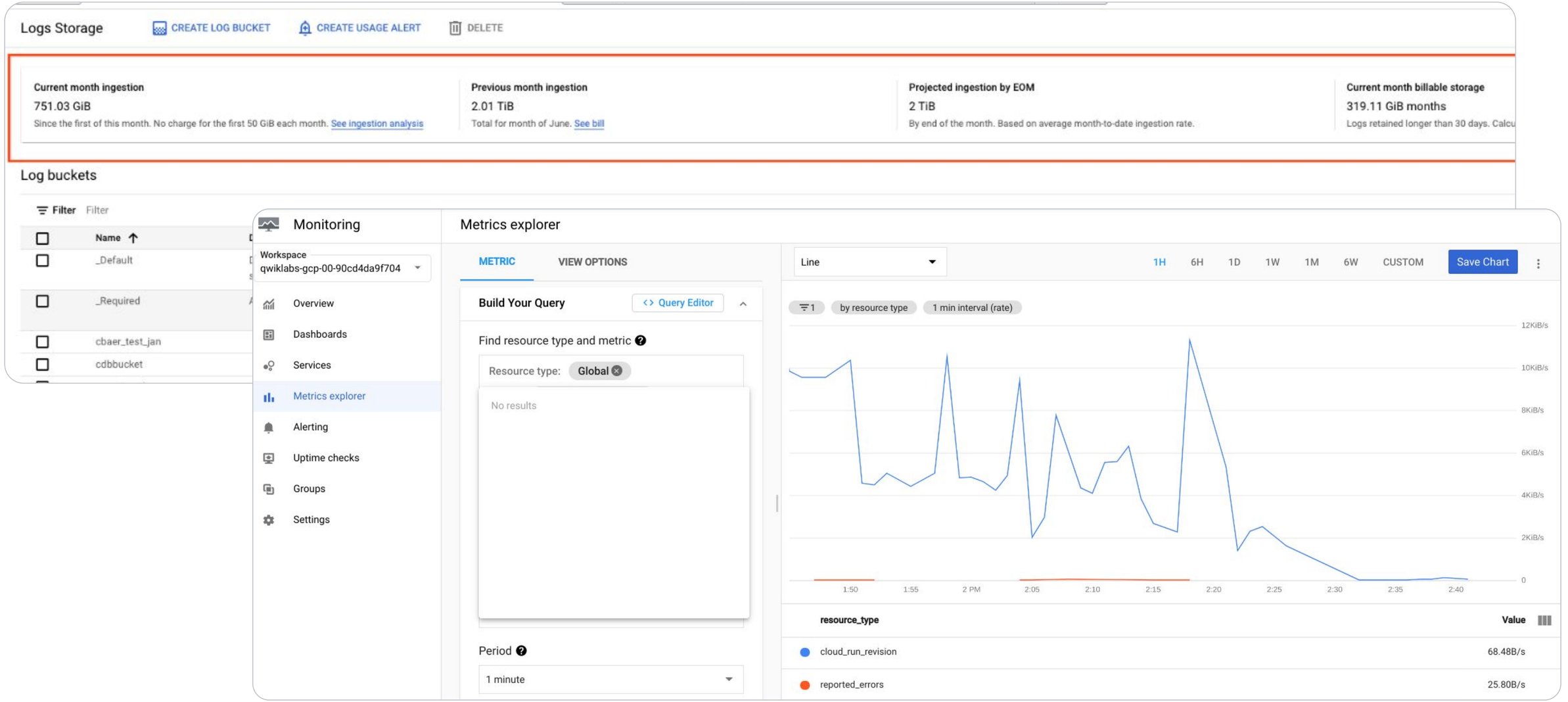
- Routes admin activity, system event and access transparency logs automatically
- No charges
- Retention period: Non-configurable 400 days
- Cannot be deleted or modified



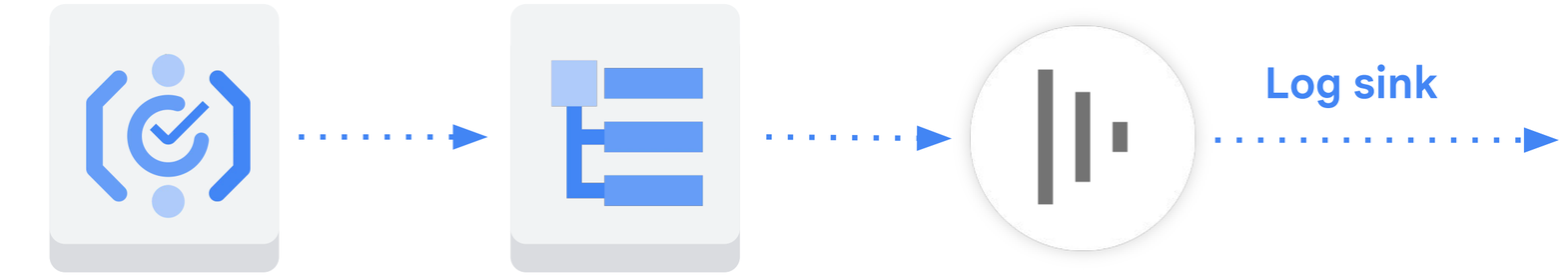
`_Default`

- Logs not ingested by _required bucket are routed by the _Default sink
- No charges
- Configurable retention period
- Cannot be deleted but can be disabled.

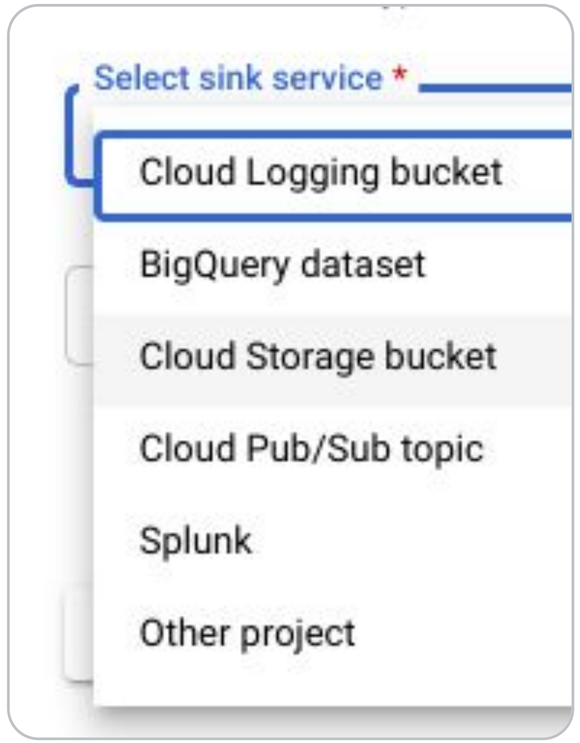
Logs storage and usage



Log router sinks and sink locations

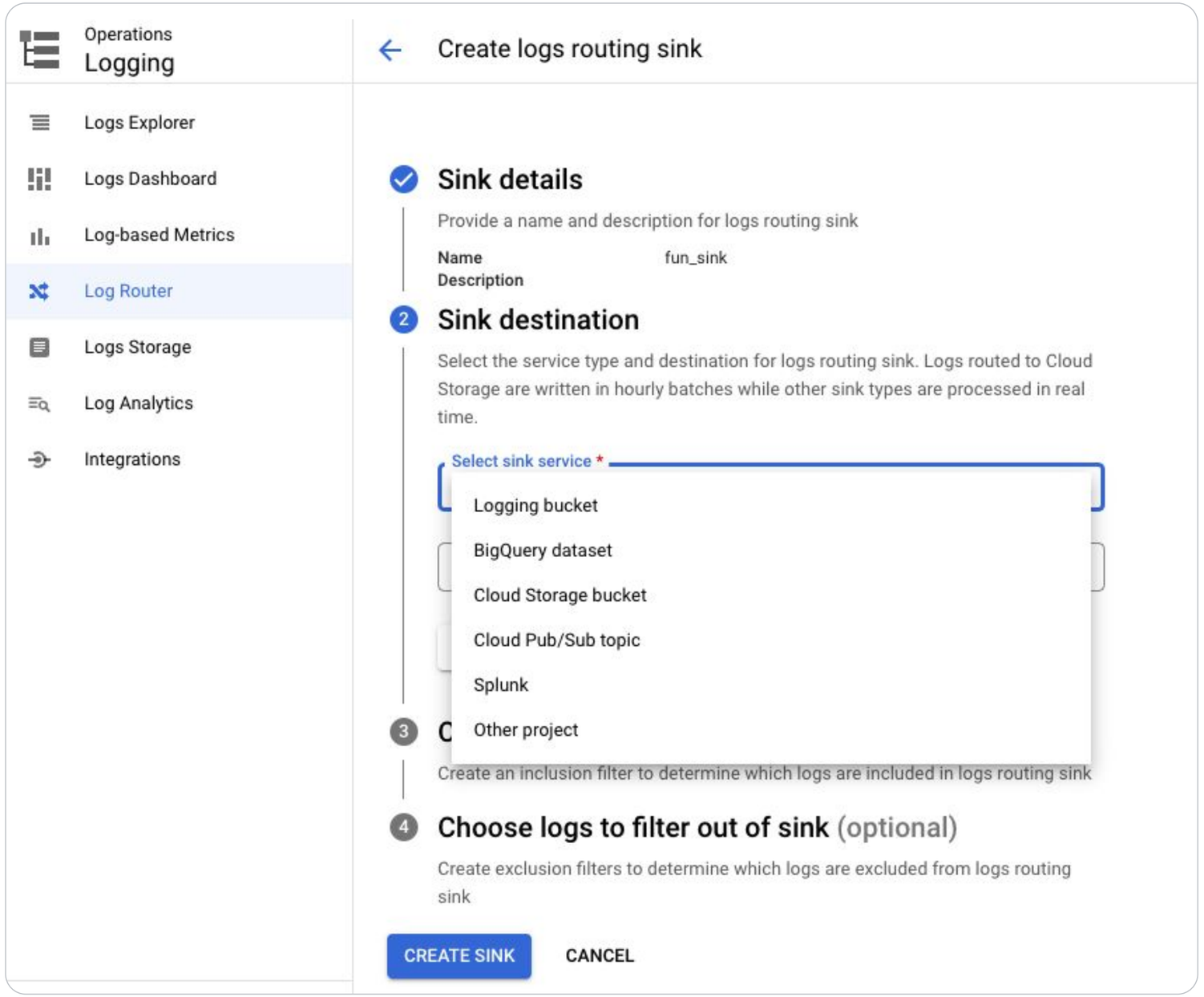



```
severity >= ERROR
resource.type="k8s_container"
resource.labels.project_id="XX"
```



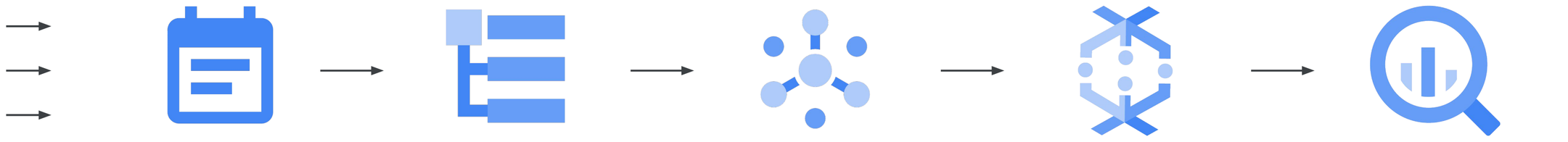
Sink locations

Create a log sink



Log archiving and analysis

Example pipeline



1 Events

2 Logging

3 Pub/Sub

4 Dataflow

5 BigQuery

Archive logs for long-term storage

Example pipeline

1 Events

2 Logging

3 Cloud Storage

Exporting back to Splunk

Example pipeline

1 Events

2 Logging

3 Pub/Sub

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

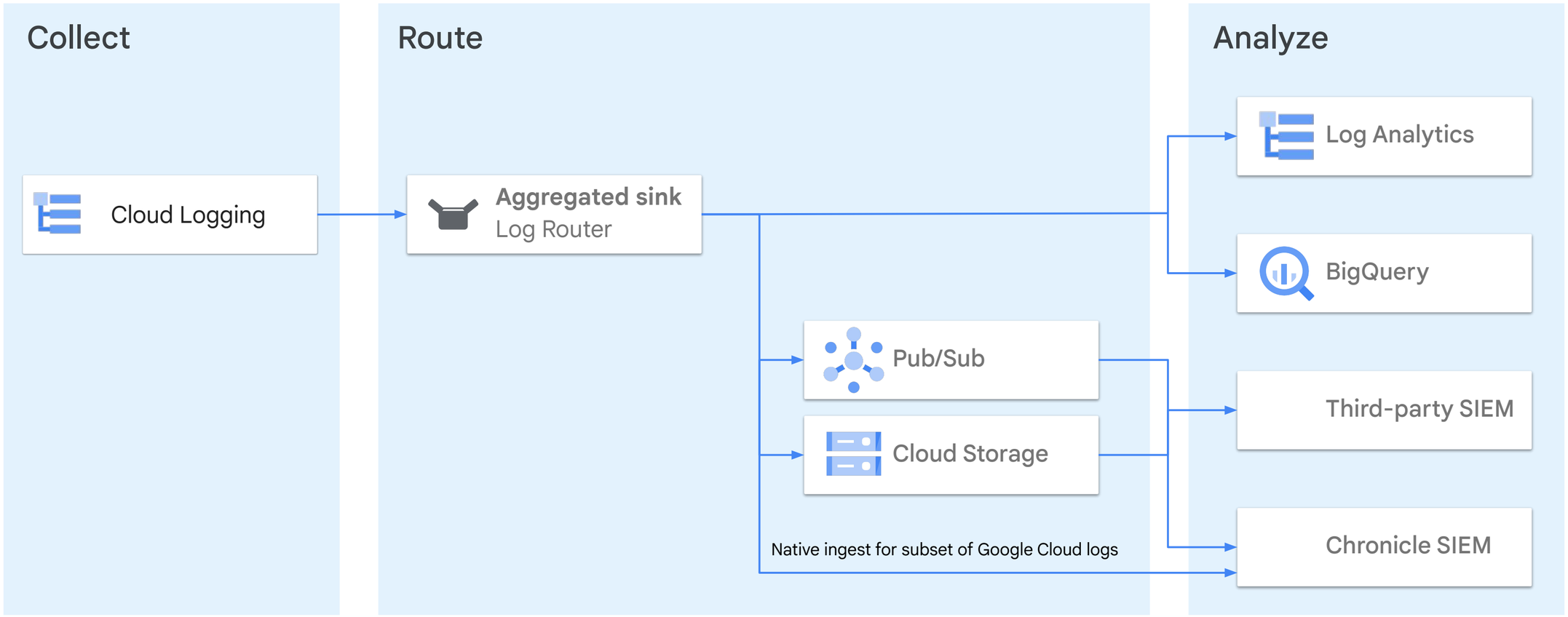
- A **folder-level log sink** aggregates logs on the folder level.
- You can also include logs from children resources (subfolders, projects).

Organization

- An **organization-level log sink** aggregates logs on the organization level.
- You can also include logs from children resources (subfolders, projects).

Security log analytics workflow

Security log analytics workflow recommends aggregated sinks



Heading

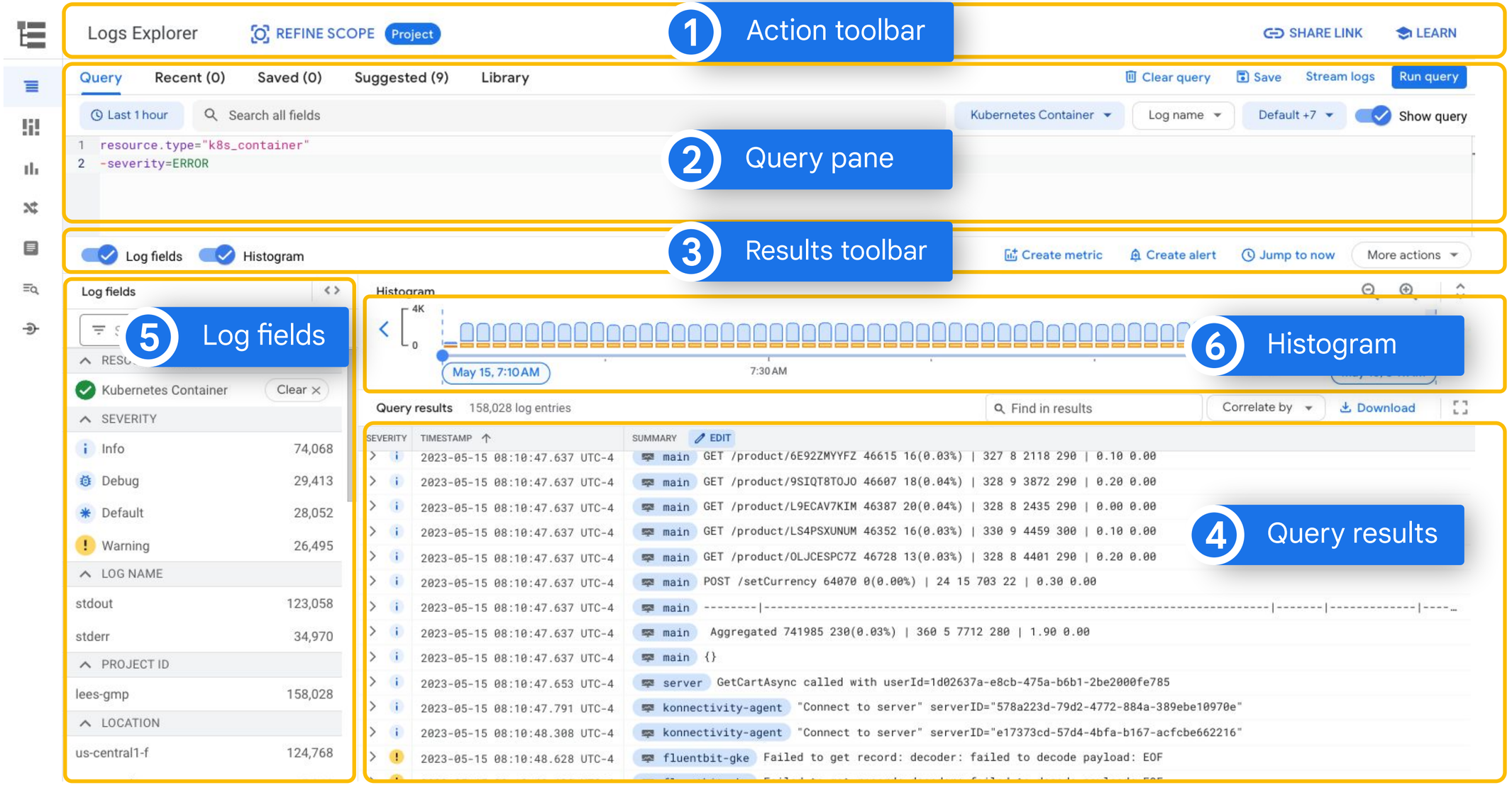
Last three days from syslog and *apache_access* for a particular *gce_instance*

```
SELECT
  timestamp AS Time, logName as Log, textPayload AS Message
FROM
  (TABLE_DATE_RANGE(my_bq_dataset.syslog_,
    DATE_ADD(CURRENT_TIMESTAMP(), -2, 'DAY'), CURRENT_TIMESTAMP())),
  (TABLE_DATE_RANGE(my_bq_dataset.apache_access_,
    DATE_ADD(CURRENT_TIMESTAMP(), -2, 'DAY'), CURRENT_TIMESTAMP()))
WHERE
  resource.type == 'gce_instance'
  AND resource.labels.instance_id == '1554300700000000000'
ORDER BY time;
```

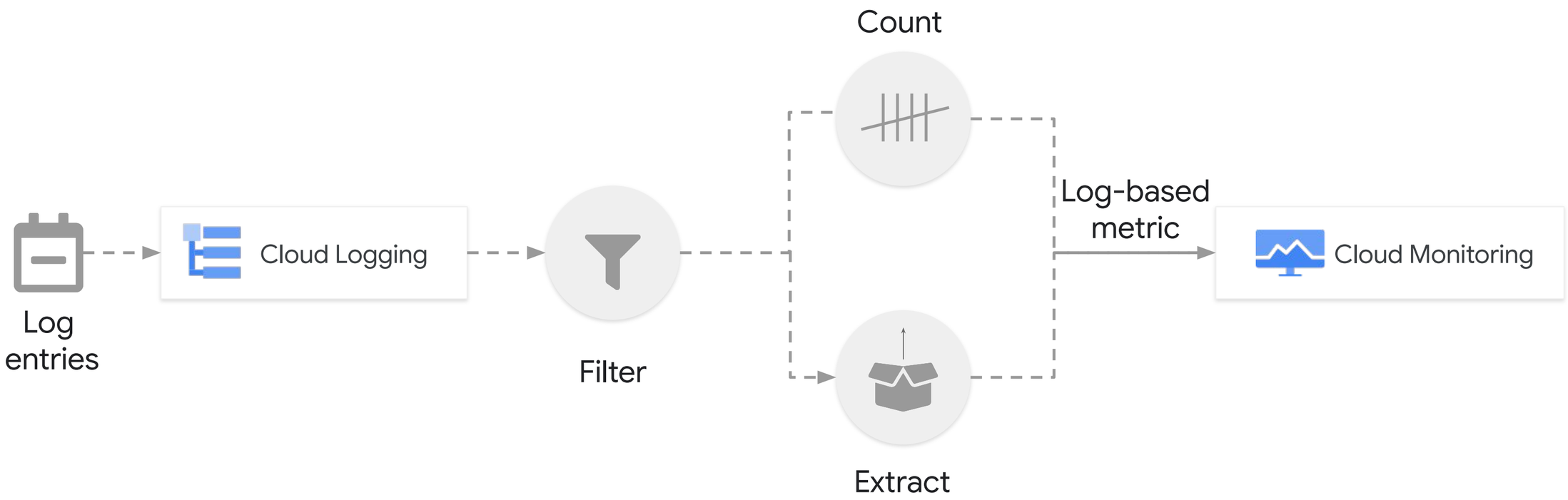
Failed App Engine requests for the last month

```
SELECT
  timestamp AS Time,
  protoPayload.host AS Host,
  protoPayload.status AS Status,
  protoPayload.resource AS Path
FROM
  (TABLE_DATE_RANGE(my_bq_dataset.appengine_googleapis_com_request_log_,
    DATE_ADD(CURRENT_TIMESTAMP(), -1, 'MONTH'), CURRENT_TIMESTAMP()))
WHERE
  protoPayload.status != 200
ORDER BY time
```

Logs Explorer



Logs-based metrics



Logs-based metrics derive metric data from the content of log entries.

Logs-based metrics are suitable in different cases

Count the occurrences

Count the occurrences of a message, like a warning or error, in your logs and receive a notification when the number of occurrences crosses a threshold.

Observe trends in your data

Observe trends in your data, like latency values in your logs, and receive a notification if the values change in an unacceptable way.

Visualize extracted data

Create charts to display the numeric data extracted from your logs.

Key access control roles

Logs Configuration Writer

It can list, create, get, update, and delete log-based metrics.

Logs Viewer

It allows users to view the existing logs.

Monitoring Viewer

A monitoring viewer reads the time series in log-based metrics.

Logging Admin, Editor, Owner

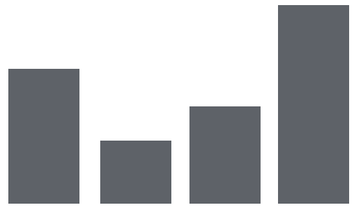
These are broad-level roles that can create log-based metrics.

Log-based metric types

+1

Counter metrics

Count the number of matched log entries



Distribution metrics

Record the statistical distribution of the extracted log values

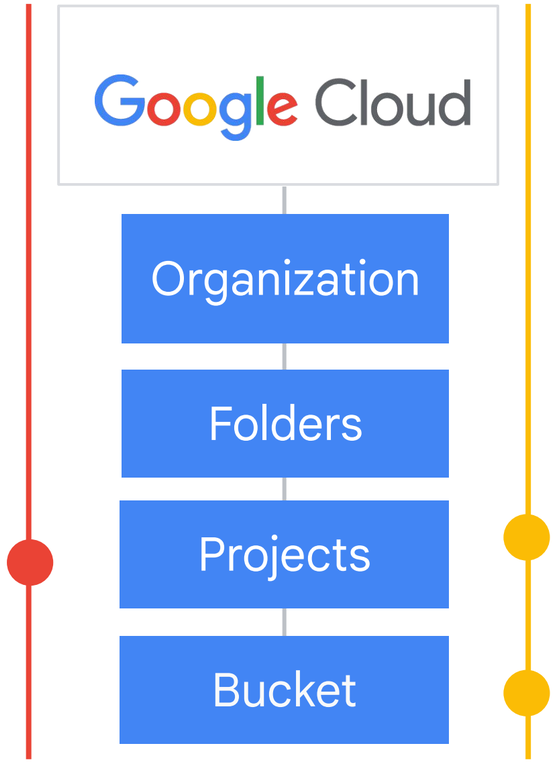
01

Boolean metrics

Record where a log entry matches a specified filter

Scope of log-based metrics

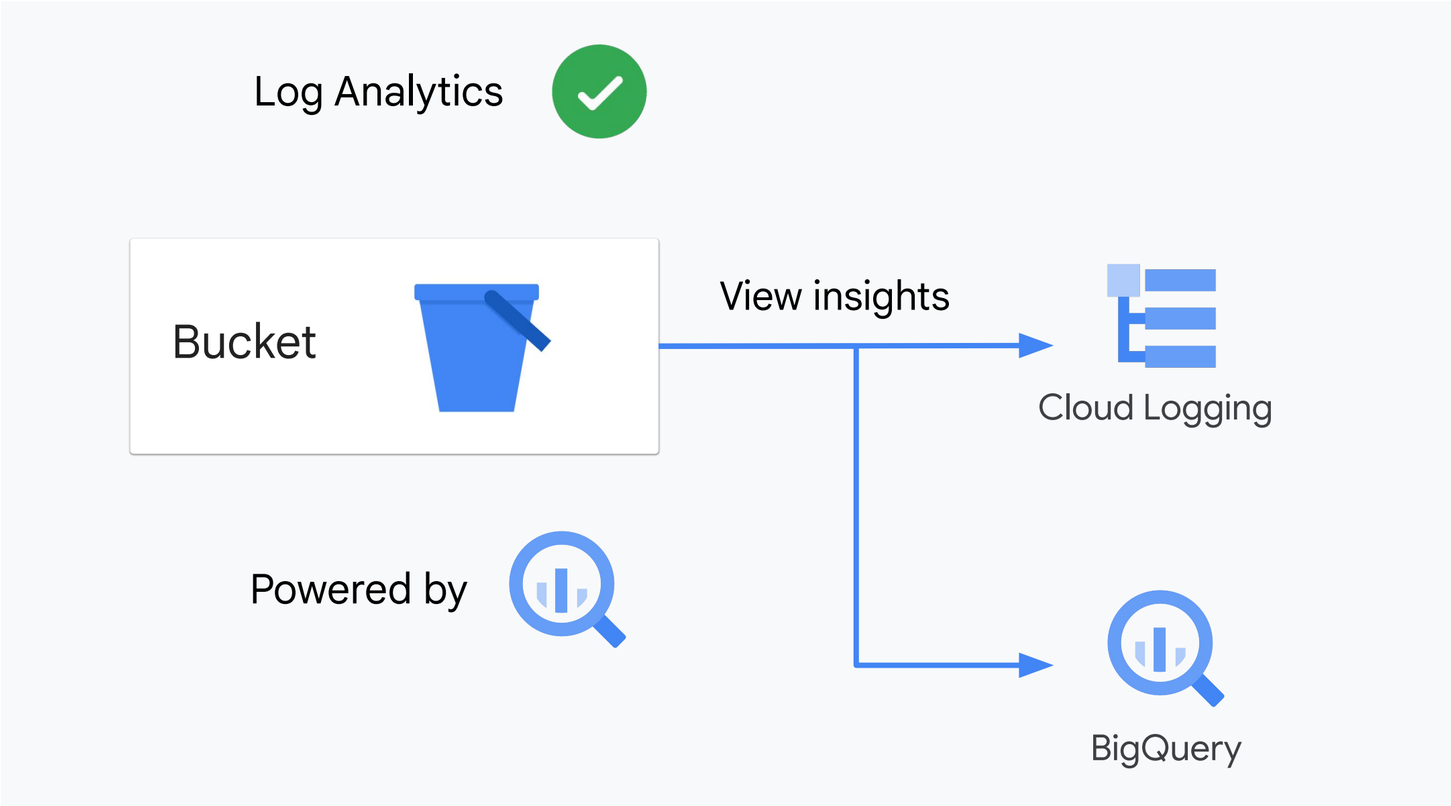
System-defined log-based metrics apply at the project level



User-defined log-based metrics can apply either at project or bucket level

Perform analytics on log data

Using Log Analytics



Cloud Logging and Log Analytics use cases

Troubleshooting

Logs Explorer

Get to the root cause with search, filtering, histogram and suggested searches.

Log Analysis

Log Analytics

Analyze application performance, data access and network access patterns.

Reporting

BigQuery link and Looker products

Use the same logs data in Log Analytics directly from BigQuery to report on aggregated application and business data found in logs.

Data logging in BigQuery

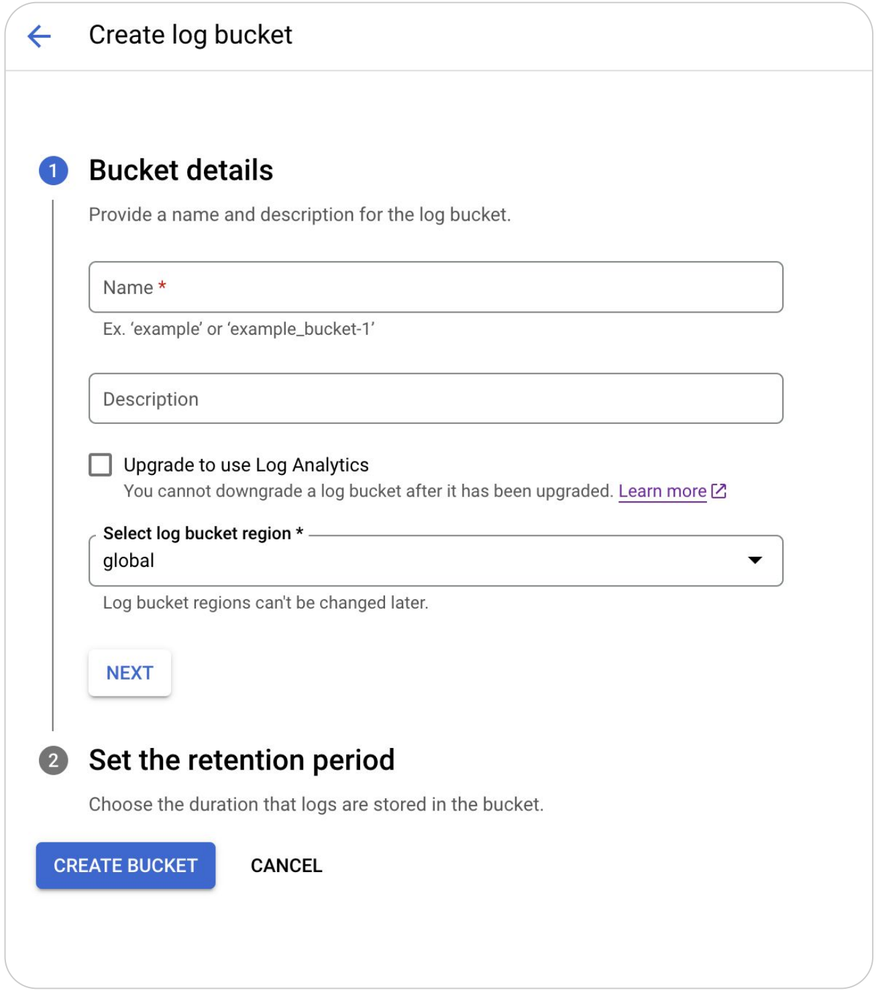
How different is analytics-enabled bucket log data from logs routed to BigQuery?

- **Log data in BigQuery is managed by Cloud Logging.**
- **BigQuery ingestion and storage costs are included in your Logging costs.**
- **Data residency and lifecycle are managed by Cloud Logging.**

Creating a log-analytics enabled bucket

- Create a log bucket with Log Analytics enabled.
- Create a sink to route logs to the newly created bucket.
- Check **Upgrade to use Log Analytics.**

You can't downgrade the log bucket to remove the use of Log Analytics.



Log Analytics use cases

DevOps

Reduce MTTR by using advanced analytical capabilities to diagnose issues.

“Help me quickly troubleshoot an issue by looking at the top count of requests grouped by response type and severity”.

Security

Better investigate security-related attacks with queries over large volumes of security logs.

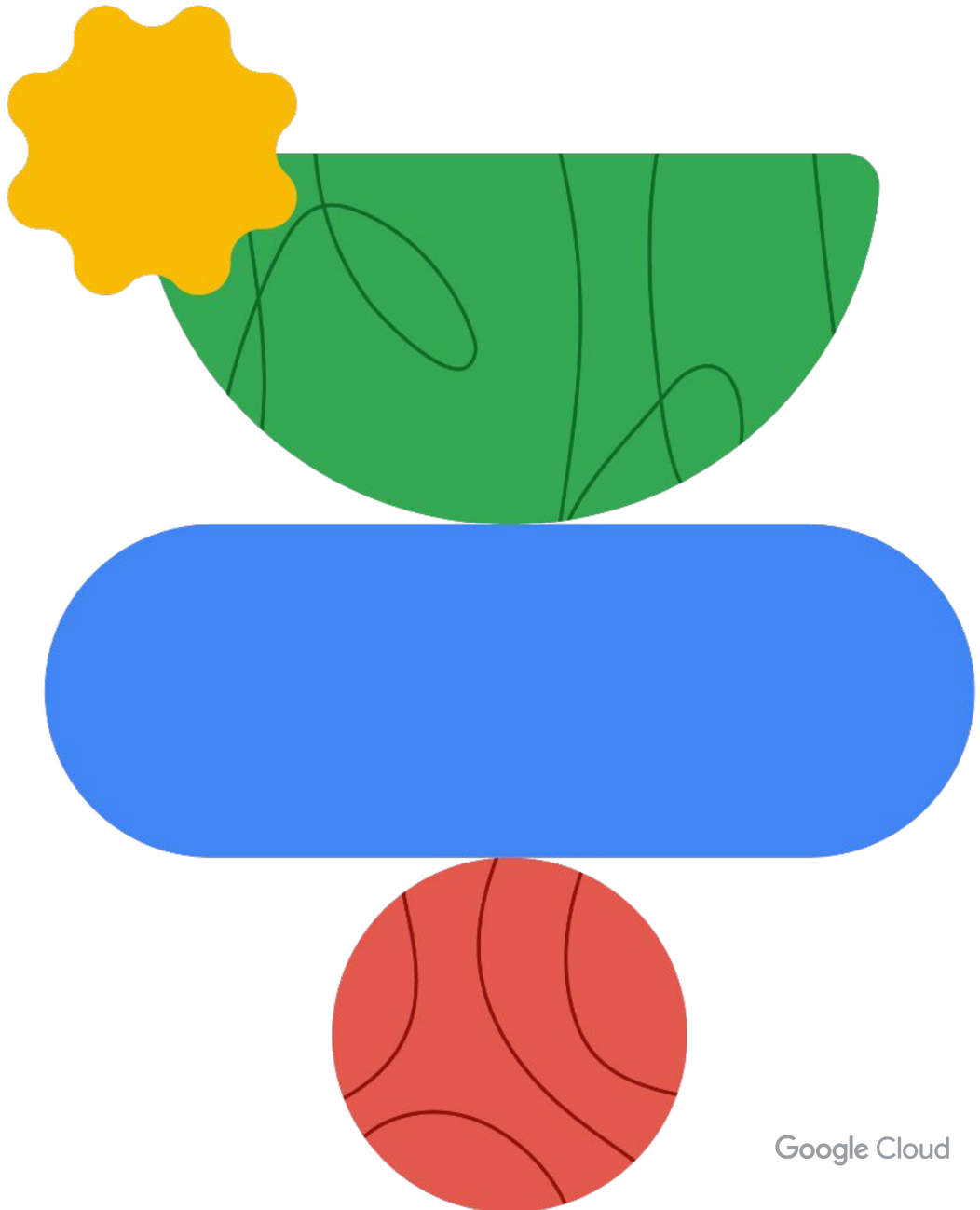
“Help me find the all the audit logs associated with a specific user over the past month”.

IT or Network Operations

Provide Better network insight and management through advanced log aggregation capabilities

“Help me identify network issues for GKE instances using VPC and firewall rules”.

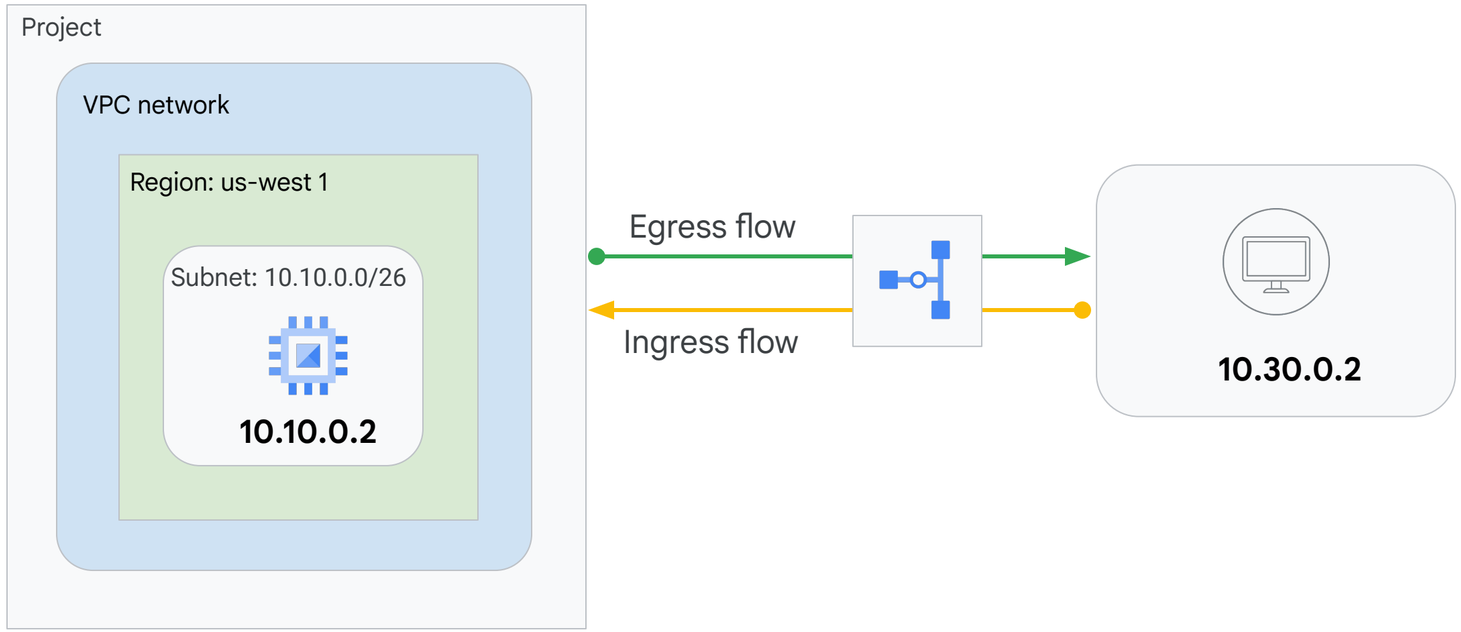
Monitoring network security and audit logs



VPC Flow Logs is used to monitor network by recording a portion of network flows sent and received by VM instances (including GKE nodes).

VPC Flow Logs example

VM to external traffic flow



Flow logs reported from the VM:

Egress flow: 10.10.0.2 to 10.30.0.2

Ingress flow: 10.30.0.2 to 10.10.0.2

The VM and and on-premises endpoint are connected through a Cloud VPN or Cloud Interconnect instance.

VPC Flow Logs properties

Samples are from the VM's perspective.

- An egress deny firewall is logged.
- An ingress deny firewall rule is not logged.

Samples are logged for each VMs. This includes inbound and outbound traffic:

- VM to VM, VM to a host on the internet, VM to on-premises host, etc.

Enable VPC Flow Logs per VPC subnet

VPC Flow Logs is activated or deactivated at a subnet level.

All VMs within that subnet have VPC Flow Logs automatically enabled.

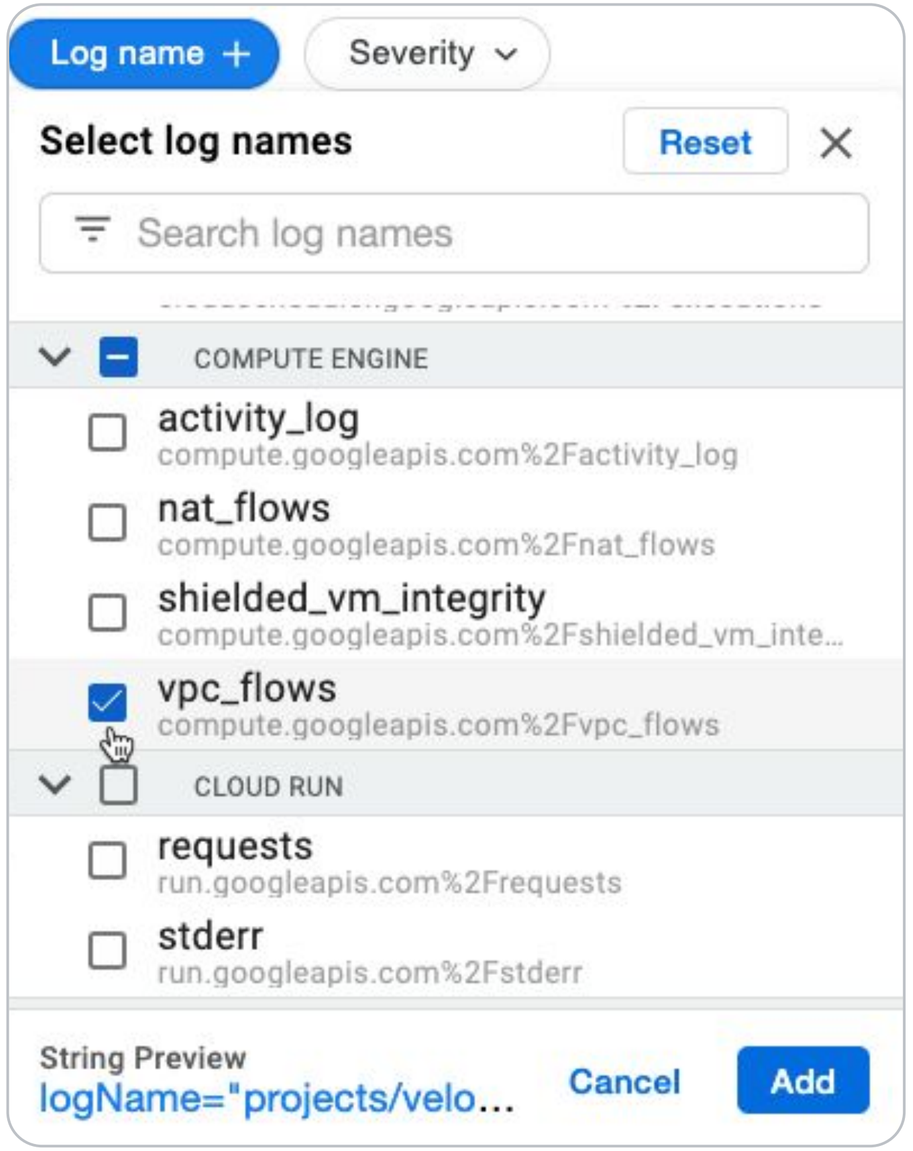
You can enable VPC Flow Logs during subnet creation.

You can optionally adjust log sampling and aggregation to adjust the metadata and sample rate written to logs.

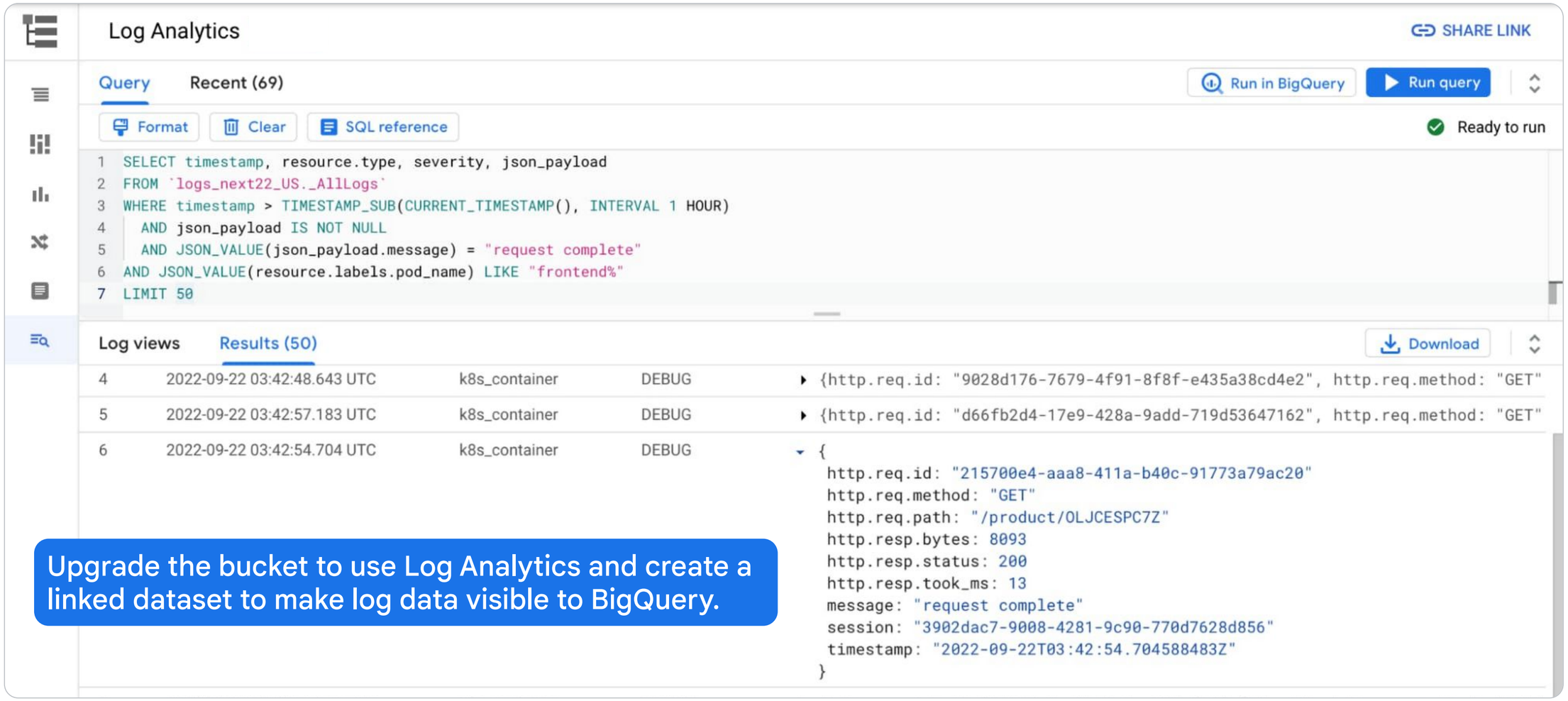
Log entries contain many useful fields

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

Analyzing VPC Flow Logs with Logging



Analyze logs with Log Analytics



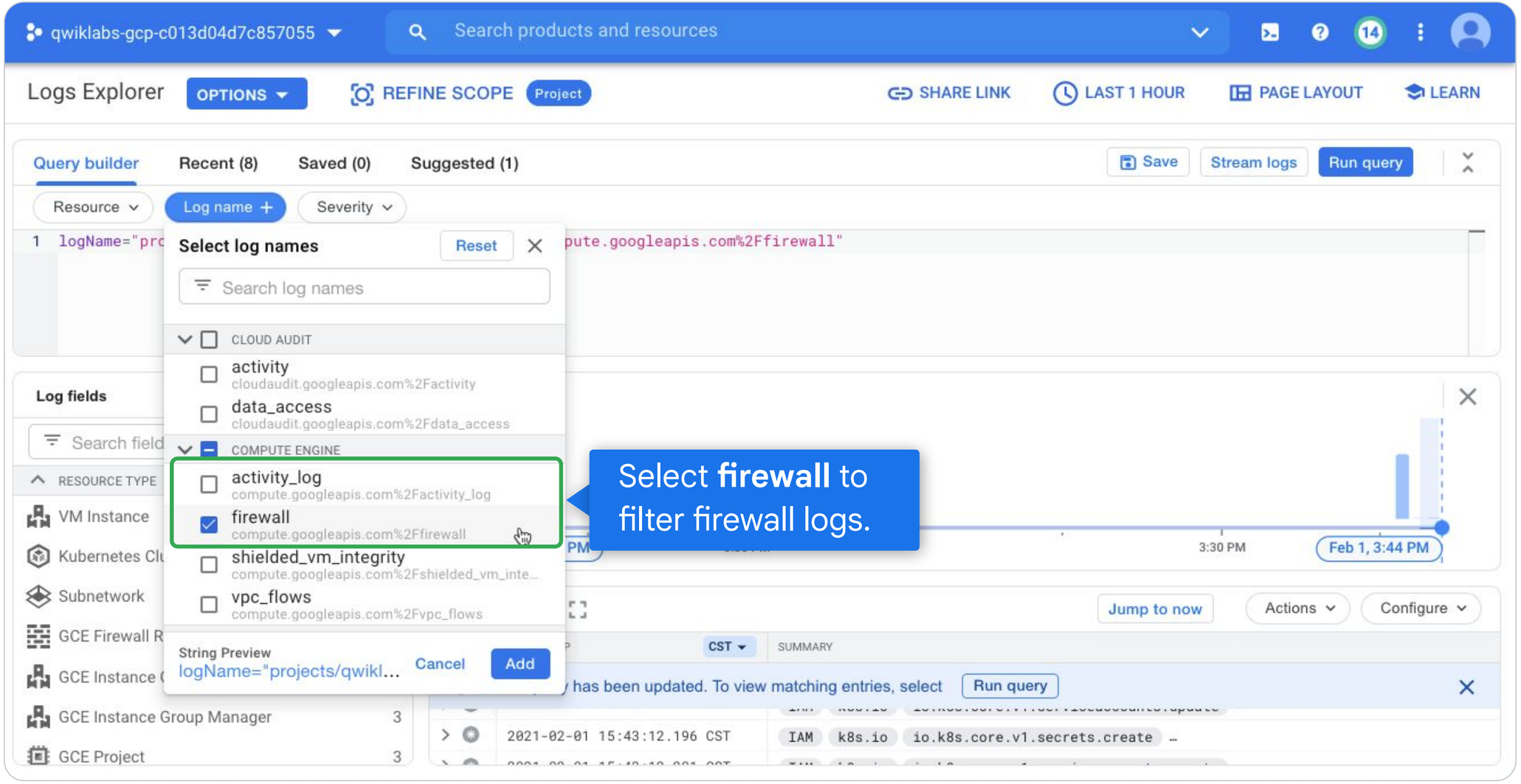
Firewall Rules Logging

01 Did my firewall rules cause that application outage?

02 How many connections match the rule I just created?

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

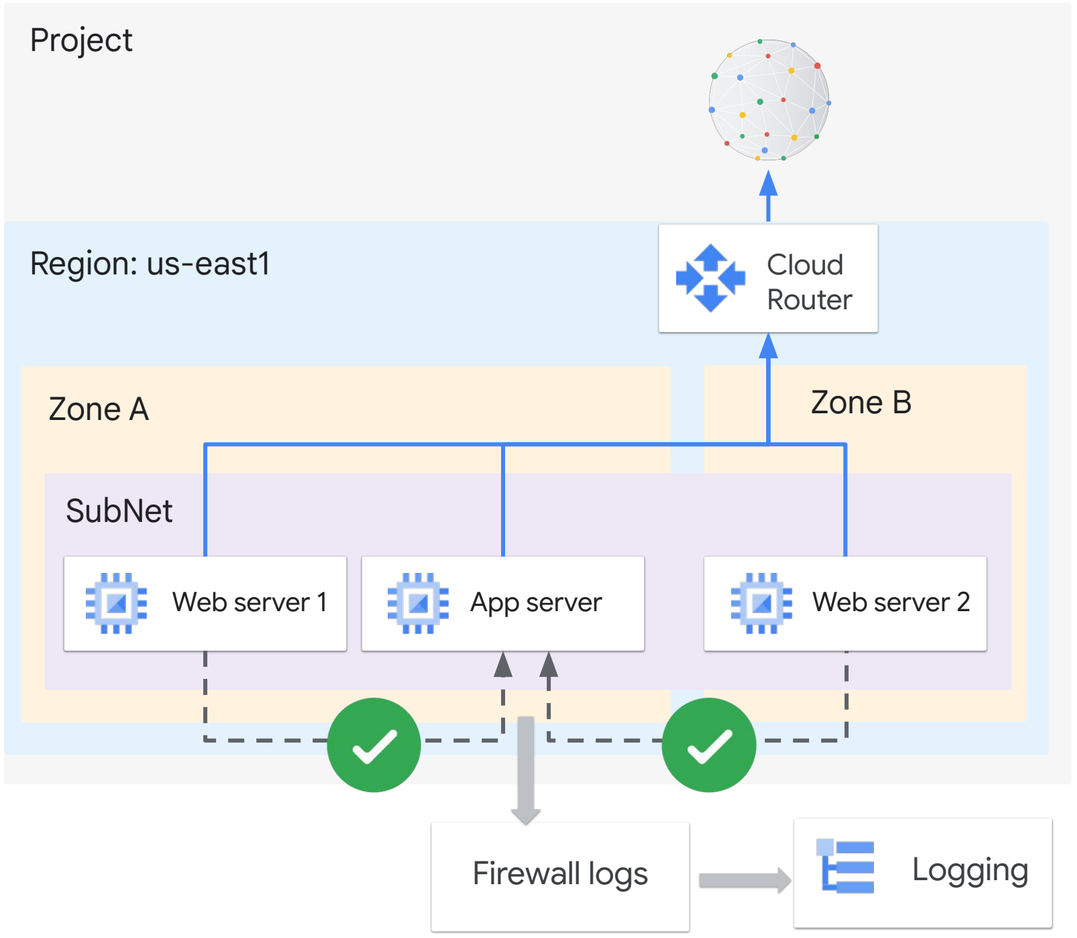
Viewing the Firewall Rules logs



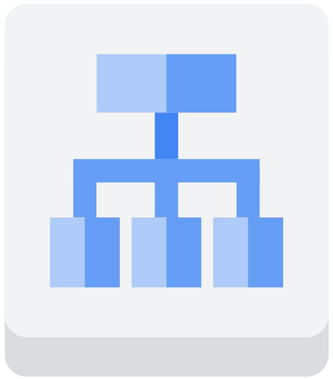
Troubleshooting

Using rules to catch incorrect traffic

- Logging all denied connections will create too many log entries.
- Temporarily create a high-priority rule (low-priority value) to allow traffic to the server. Enable Cloud Logging.
- If traffic now gets through, examine the logs to find the root cause.



Load balancer support for Cloud Logging



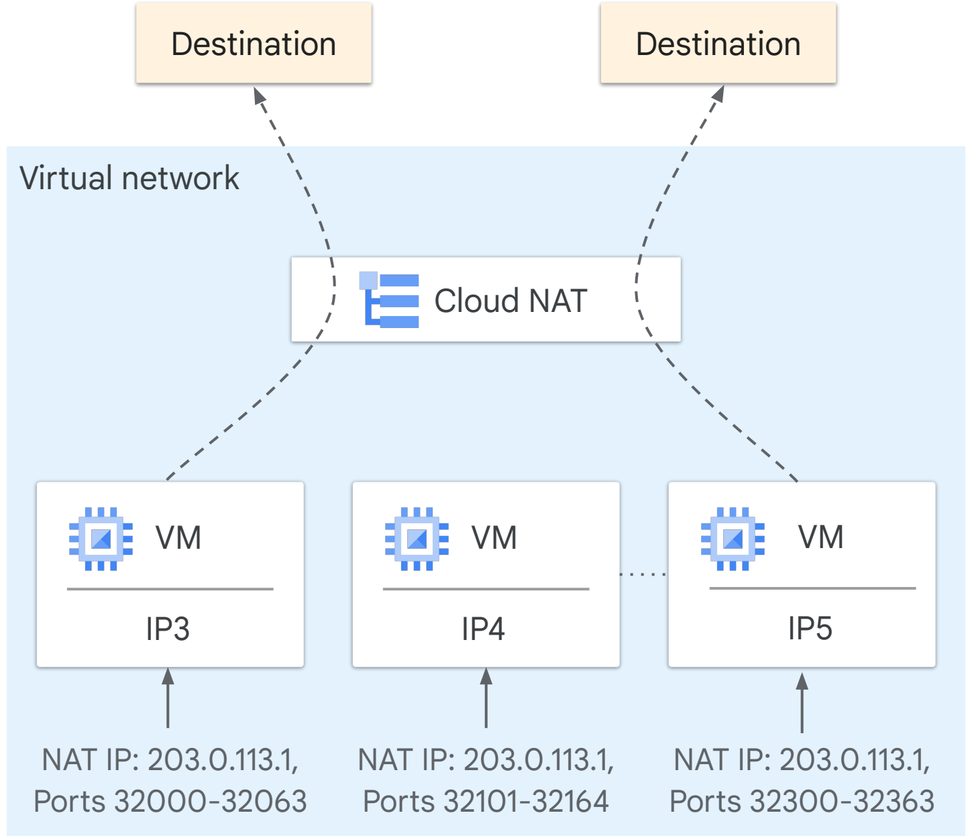
- All the Google Cloud load balancers support Cloud Logging and Cloud Monitoring:
  - Internal and external Application Load Balancers
  - Internal and external Network Load Balancers
  - Internal and external Proxy Load Balancers
- The log type, log fields, and metrics supported vary based on the the load balancer type.
- Load balancing logs can be used to debug and analyze user traffic.

The internal and external Application Load Balancers support logging

- **Activated and deactivated on a per backend service basis**
  - For external Application Load Balancers with backend buckets, logging is automatically enabled and cannot be deactivated.
  - Logging can be enabled on a per backend service basis.
  - URL map might reference more than one backend service.
  - Use exclusion, if you do not want the logs to be stored in Cloud Logging.

Cloud NAT overview

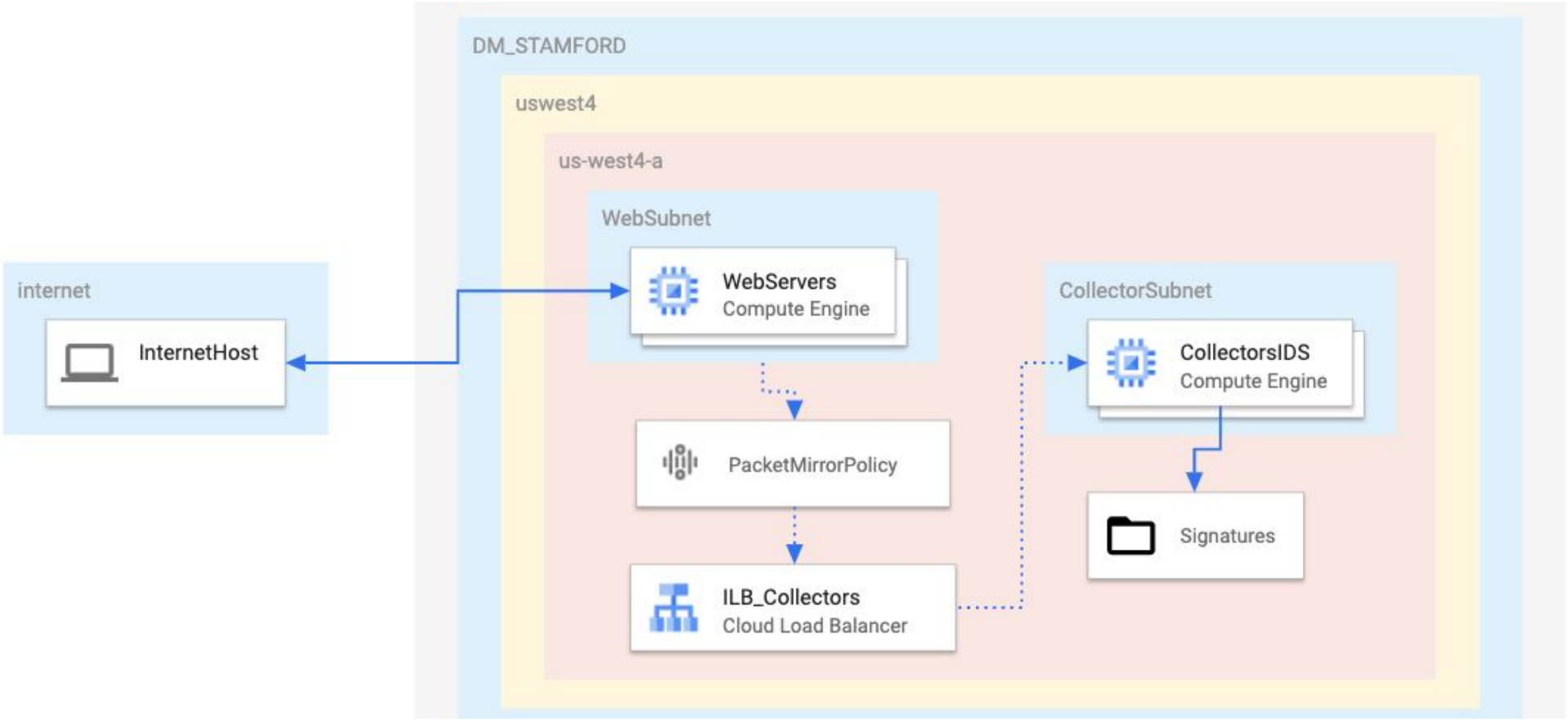
- It allows Google Cloud Compute workload with no external IP to send packets to the internet.
- It's a fully managed, proxyless NAT service in Andromeda.
- These are some of its benefits:
  - Reduces the need for individual VMs to each have external IP addresses.
  - Automatically scales the number of NAT IP addresses that it uses.
  - Is not dependent on a single physical gateway device.



Cloud NAT logging

- A NAT log is created when:
  - A network connection using NAT is created.
  - A packet is dropped due to port unavailability
- It lets you log NAT **connections** and/or **errors.**
  - TCP and UDP traffic only.
  - 50-100 entries per second, per vCPU.

Packet Mirroring: Visualize and protect your network



Packet Mirroring: Overcoming bandwidth limitations

Packet Mirroring consumes the egress bandwidth of the mirrored instances.

01

Use filters to reduce the bandwidth on mirrored instances.

02

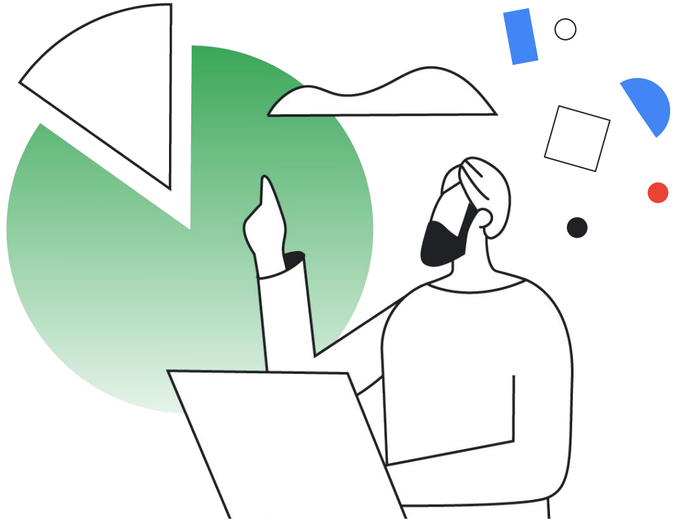
Filters can be based on protocol, IP ranges, traffic directions, etc.

03

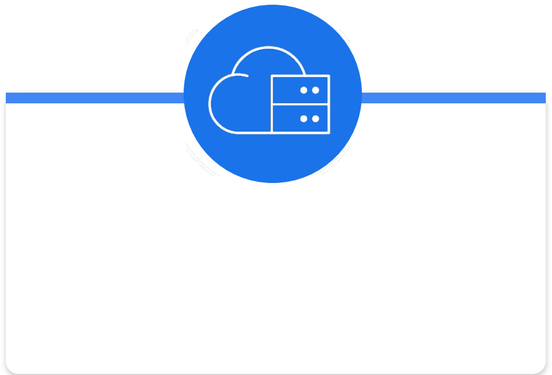
The current maximum of filters for Packet Mirroring is 30.

Packet Mirroring: Use cases

- Network and application **monitoring**:
  - Maintain integrity of deployment.
  - Fix packet loss issues.
  - Fix reconnection and latency issues.
- **Security and compliance**:
  - Intrusion detection systems.
  - Deep Packet Inspection engines.
- **Forensics:**
  - Collect, process, and preserve network forensics.



Cloud Audit Logs: Who did what, where, and when?



Admin Activity audit logs

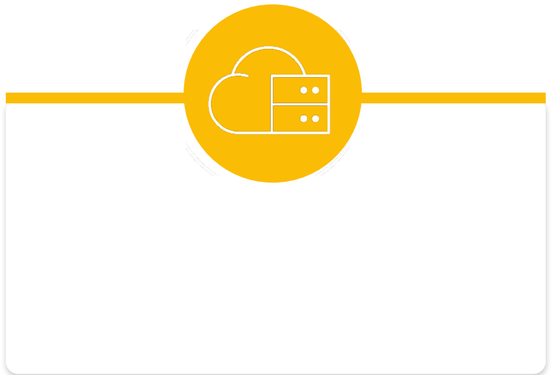
- Records modifications to configuration or metadata.
- Helps answer questions such as “Who added that VM?”

Cloud Audit Logs: Who did what, where, and when?

System Event audit logs

- Records Google Cloud non-human admin actions that modify configurations.
- Helps answer questions such as “Did a live-migration event occur?”

Cloud Audit Logs: Who did what, where, and when?



Data Access audit logs

- Records calls that read metadata, configurations, or that create, modify, or read user-provided data.
- Helps answer questions such as “Who modified that Cloud Storage file?”

Cloud Audit Logs: Who did what, where, and when?

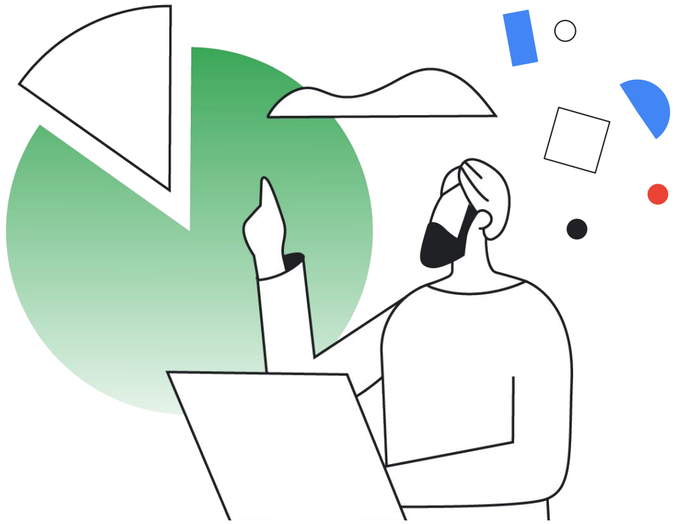
Policy Denied audit logs

- Records a security policy violation.
- Helps answer question such as “Who tried to breach a security policy?”

Access Transparency logs

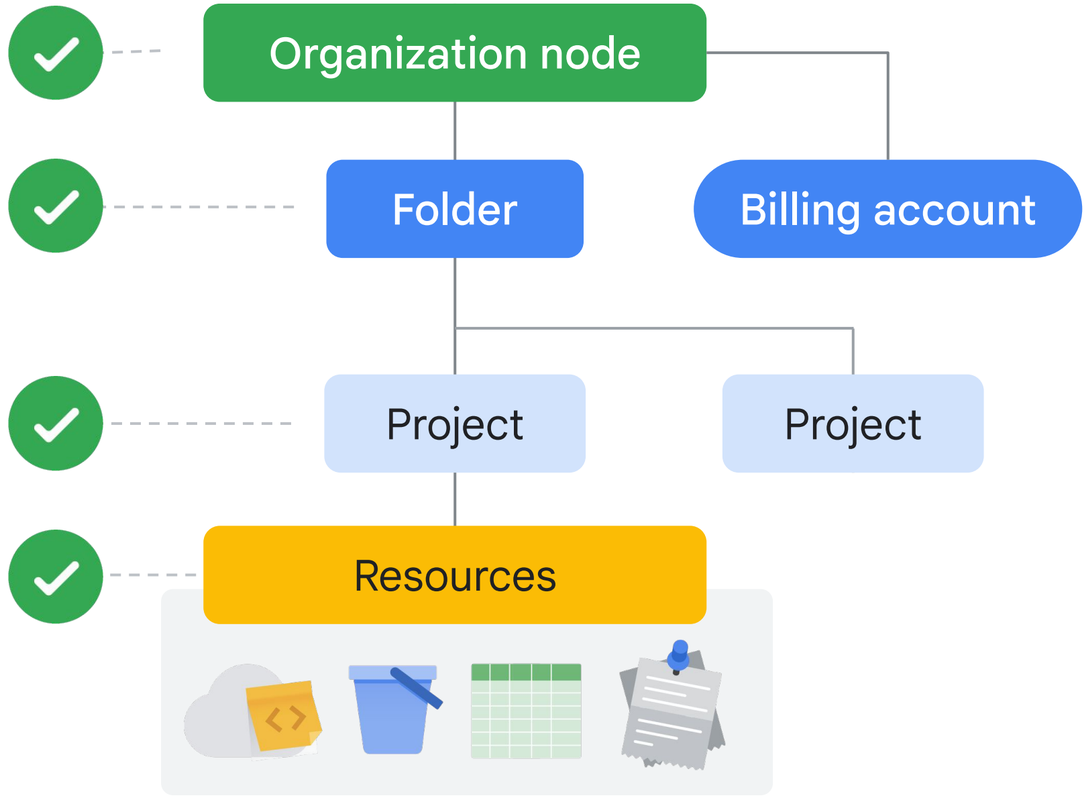
Show **how** and **why** customer data is accessed once it has been stored in Google Cloud.

- Logs actions of accesses
- Tracks actions by Google personnel
- Supports approval and surfaced through App APIs and UIs, Security Command Center

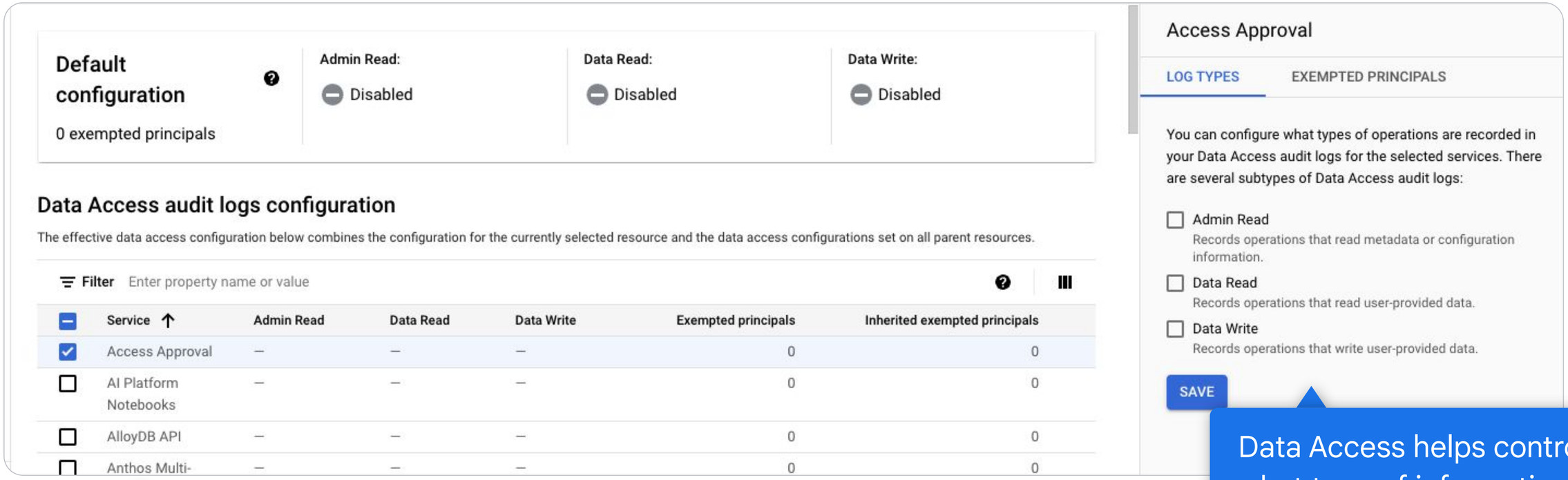


Enabling Data Access audit logs in the organization

- Data Access audit logs can be enabled at:
  - Organization
  - Folder
  - Project
  - Resource
  - Billing accounts
- You can even exempt principals from recording data access logs
- Final scope is the union of the configurations



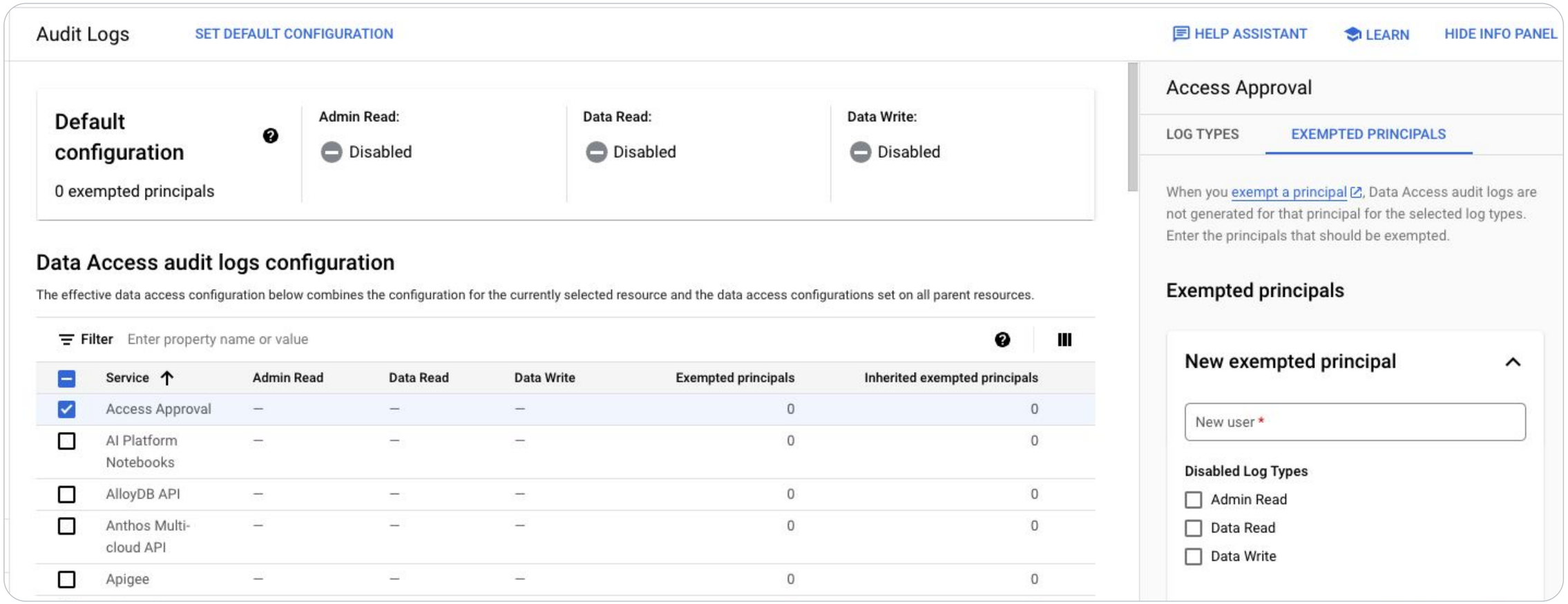
Enabling Data Access logs per Google Cloud service



Data Access logs can be enabled and configured at the service level.

Data Access helps control what type of information is **recorded** in the Data Access audit logs.

Exempt specific users or groups



Plan and create test project

- Create a plan for Data Access audit logs.
- Create a test project and test plan.
- Roll out the plan.

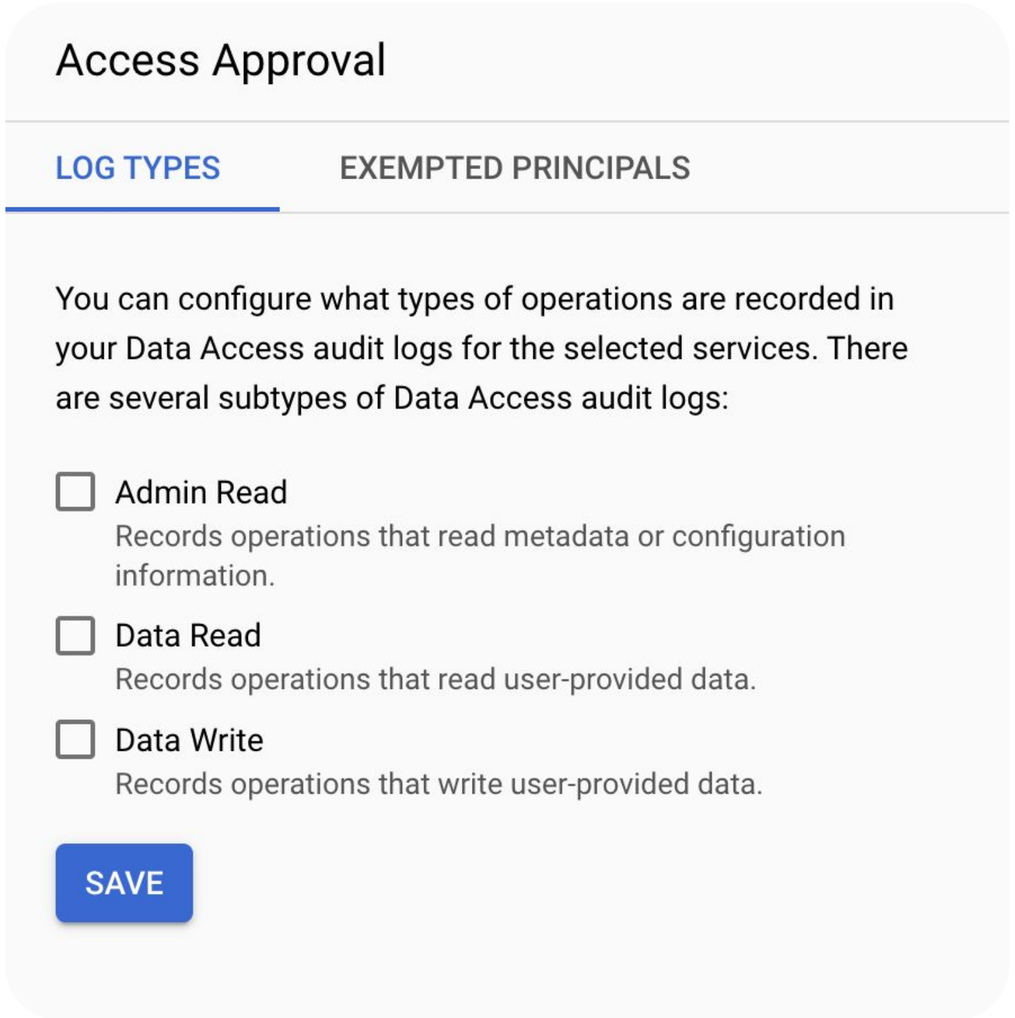
Decide and set org level data access

Advantages:

- Detailed information on who, accessed/edited/deleted what, and when
- Free tier
- Some logs are free

Disadvantage:

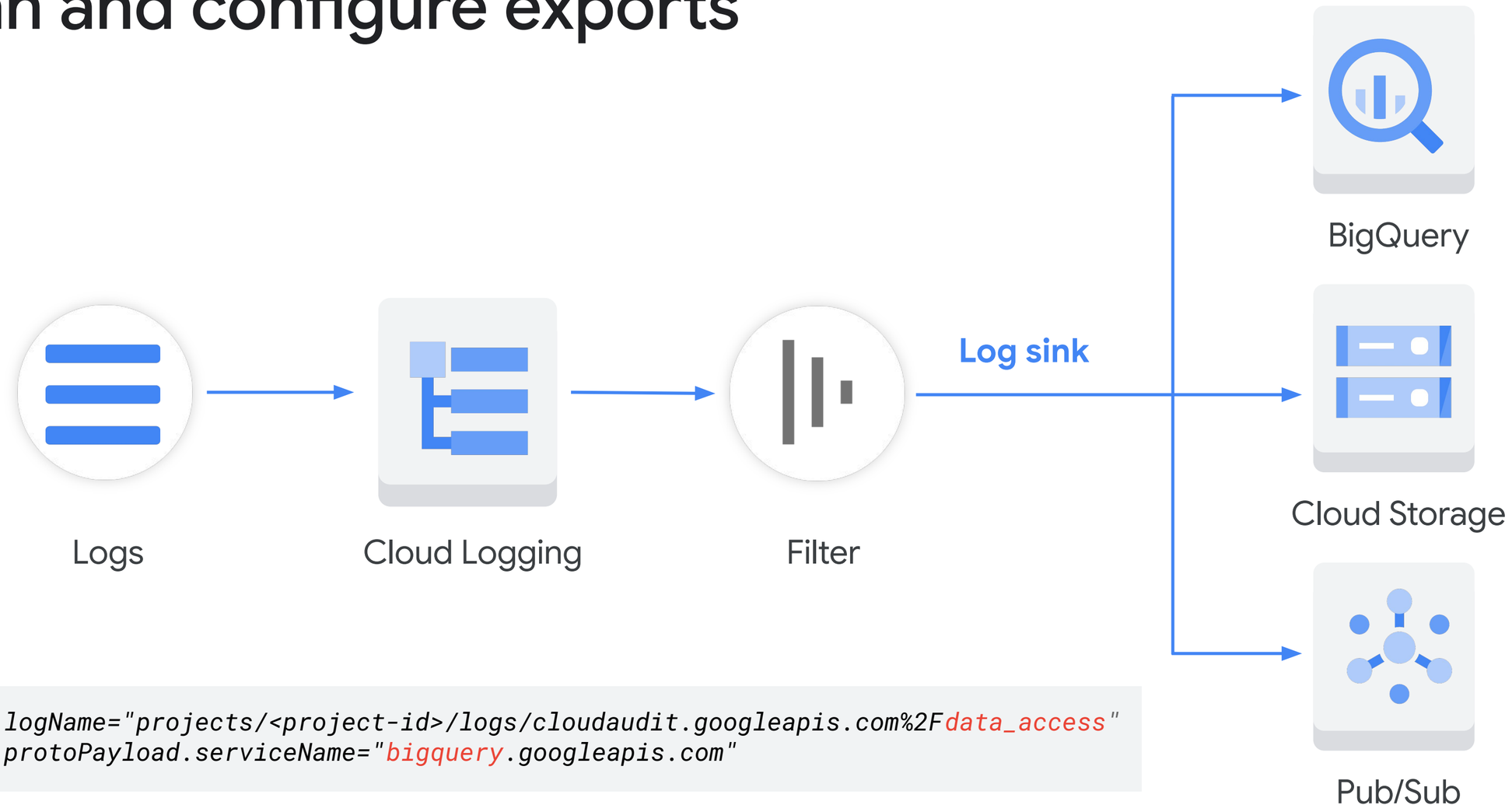
- Logs can be large and the Queries Per Second (QPS) can be high based on the number data access requests



Aggregate and store your organization's logs

- Centralize or subdivide log storage by creating user-defined buckets
- This helps meet latency, compliance and availability requirements
- Configure a default storage location at the organization level to automatically apply a region
- Protect your audit logs storage by configuring CMEK.

Plan and configure exports




```
logName="projects/<project-id>/logs/cloudaudit.googleapis.com%2Fdata_access"
protoPayload.serviceName="bigquery.googleapis.com"
```

Principle of least privilege

PII
Data Access audit logs contain Personally Identifiable Information (PII).

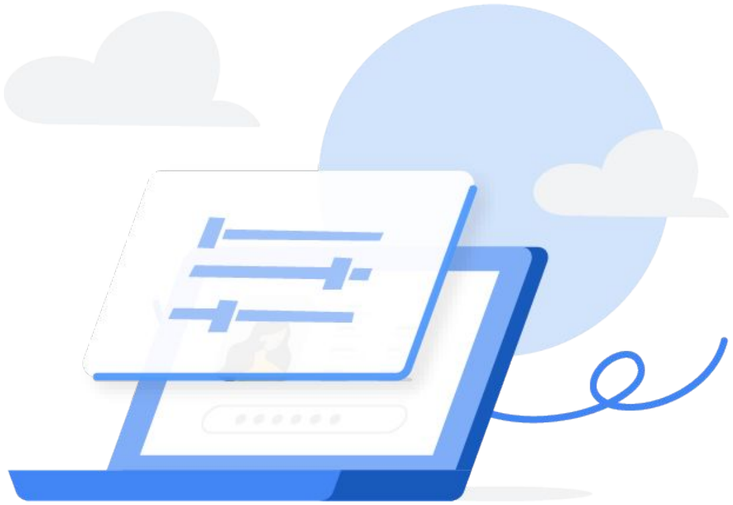
Controls
Use appropriate IAM controls on both Google Cloud-based and exported logs.

Data leakage
Side-channel leakage of data through logs is a common issue.

Project planning
Plan the project to monitoring project relationships.

Configure log views

- Log views help control access to logs in a log bucket
- It helps control access specific to a project or a set of users
- It also help protect sensitive log data
- It ensures only authorized users have access to.



Scenario

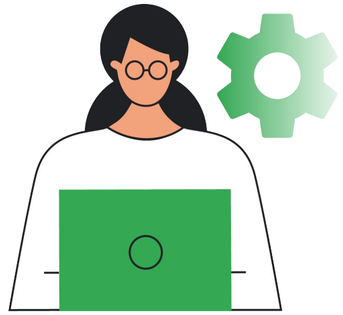
Operational monitoring

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

Scenario

Dev teams monitoring Audit Logs

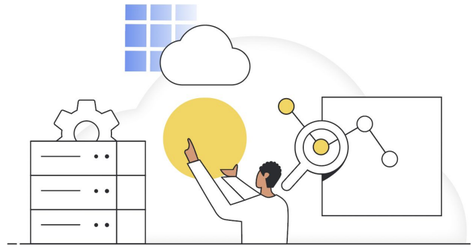
- Security team, same:
  - **logging.viewer**, **logging.privateLogViewer**
- Dev team: **logging.viewer** at folder level
  - See Admin Activity audit logs by dev projects in folder.
- Dev team: l**ogging.privateLogViewer** at folder
  - See Data Access audit logs.
- Use Cloud Storage or BigQuery IAM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



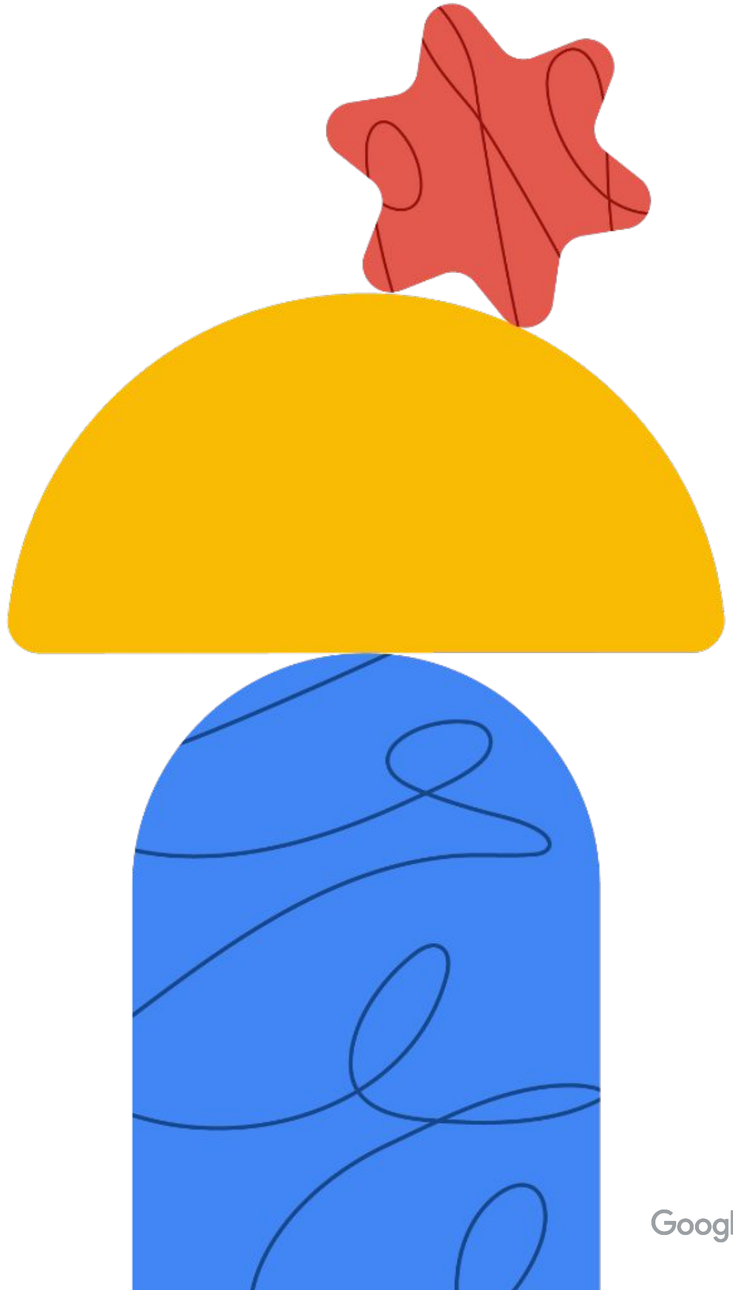
Scenario

External auditors

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



Managing incidents



Incident response

Alert

A signal that a Service Level Objective (SLO) may be violated.

Incident

The formal start of an incident response process, triggered by an alert requiring action.

Decision making

Determining if an alert is serious enough to warrant an incident response.

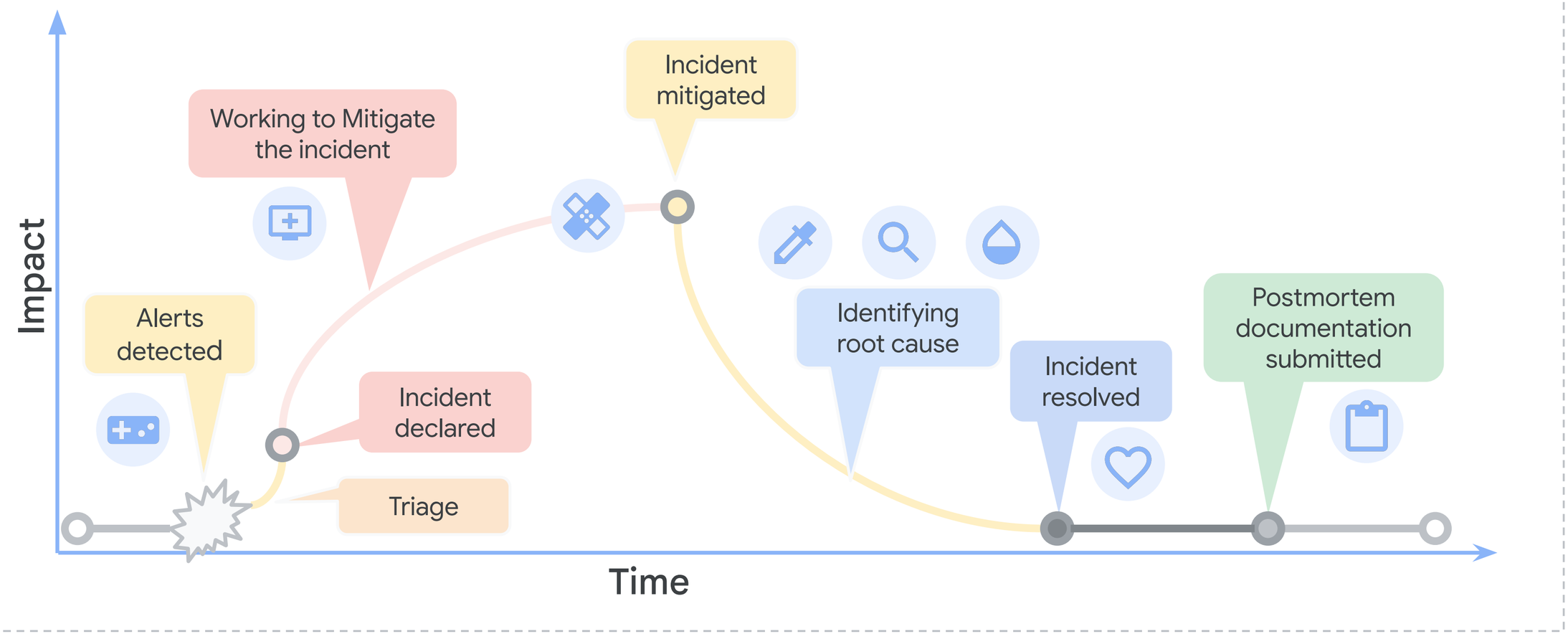
Incident response methodology

A standardized procedure outlining the steps to be taken when an incident is declared.

Incident response

- Organizations should strive for formal incident response, not just ad hoc problem-solving.
- Formal incident response utilizes checklists to ensure issues are fixed correctly.
- Documentation is crucial to prevent recurrence and improve future responses.
- The goal is a fast, organized incident resolution methodology.

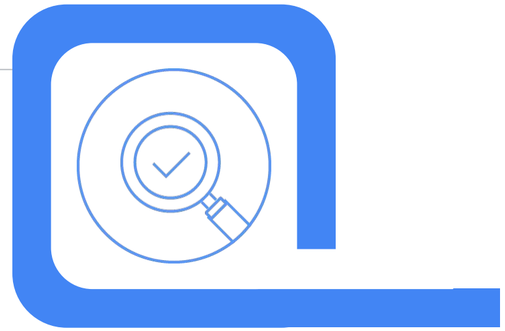
Incident lifecycle



Incident response basic principles

Early declaration

- Declare incidents early and often.



Clear chain of command

- Maintain a clear chain of command.

Real-time documentation

- Keep a working record of debugging and mitigation.

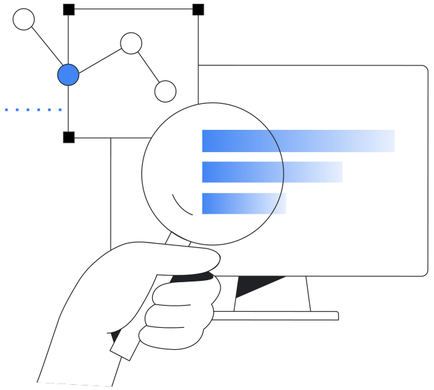
Defined roles

- Designate clearly defined roles.

Postmortem report

It is a blameless report detailing:

- Impact
- Route cause
- Triggering event
- Resolution
- Quantifiable metrics
- Action items
- Lessons learned
- Timeline



It is a detailed and organized document outlining the events of the incident.


Google Cloud