Monitoring in the Cloud

Agenda

- Development in the cloud
- Deployment: Infrastructure as code
- Monitoring: Cloud Operations basics
- Monitoring: Cloud Logging
- Monitoring: Cloud Operations monitoring
- Lab

Cloud Source Repositories

- Fully featured Git repositories hosted on Google Cloud Platform
- Supports collaborative development of cloud apps
- Includes integration with Stackdriver Debugger

Cloud Functions

- Create single-purpose functions that respond to events without a server or runtime
  - Event examples: New instance created, file added to Cloud Storage
- Written in Javascript; execute in managed Node.js environment on Google Cloud Platform

Agenda

- Development in the cloud
- Deployment: Infrastructure as code
- Monitoring: Cloud Operations basics
- Monitoring: Cloud Logging
- Monitoring: Cloud Operations monitoring
- Lab

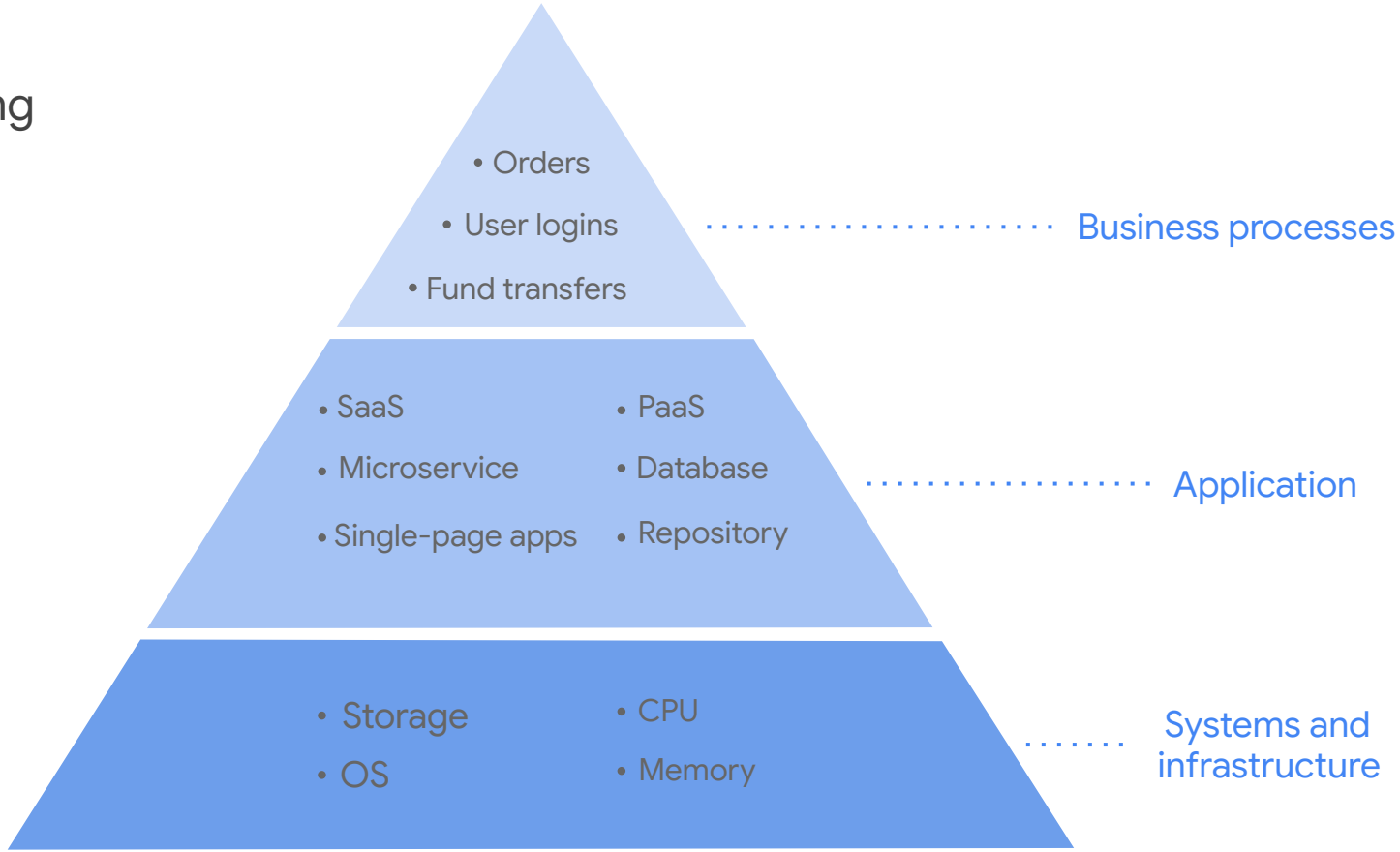
Deployment Manager

- Infrastructure management service
- Create a .yaml template describing your environment and use Deployment Manager to create resources
- Provides repeatable deployments

Agenda

- Development in the cloud
- Deployment: Infrastructure as code
- Monitoring: Cloud Operations basics
- Monitoring: Cloud Logging
- Monitoring: Cloud Operations monitoring
- Lab

Monitoring pyramid



Cloud Operations

Monitoring

- Endpoint checks to internet-facing services
- Uptime checks for URLs, groups, or resources
- Plugins for many major stacks (Apache, MySQL, CouchDB etc.)

Logging

- Filter, search, and view
- Define metrics, dashboards, and alerts
- Export to BigQuery, Google Cloud Storage, and Pub/Sub

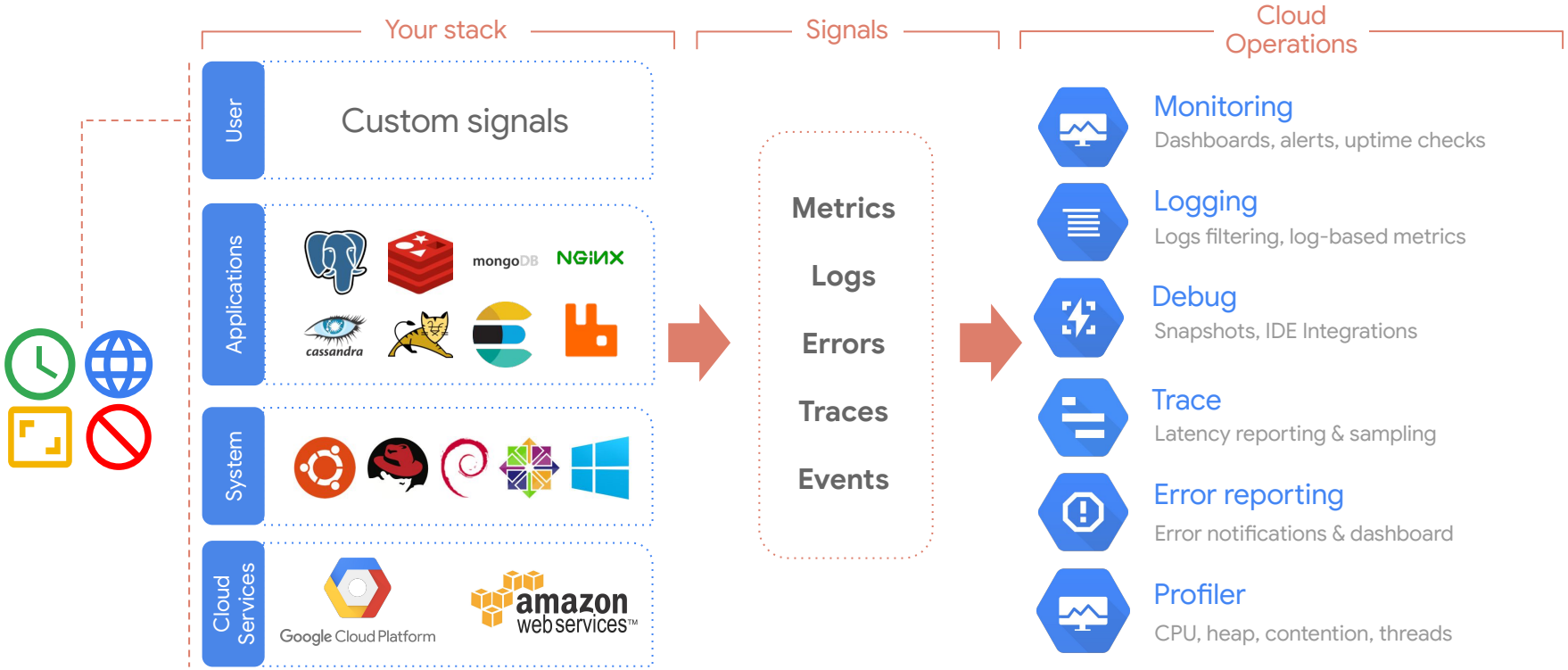
Performance

- Built on the same systems that power Google's global infrastructure
- Unprecedented scale, performance, and resiliency

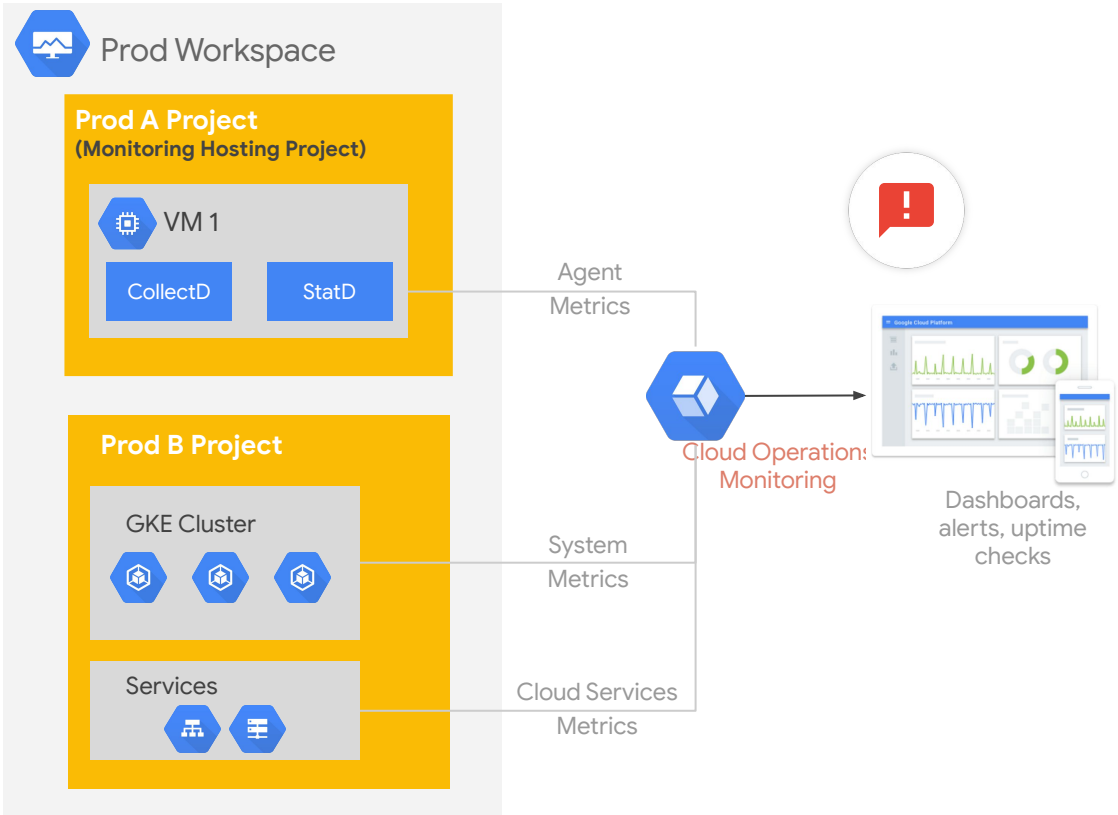
Multi-Cloud

- Google Cloud Platform Amazon Web Services Hybrid configuration
- Combines metrics, logs, and metadata

What Google offers

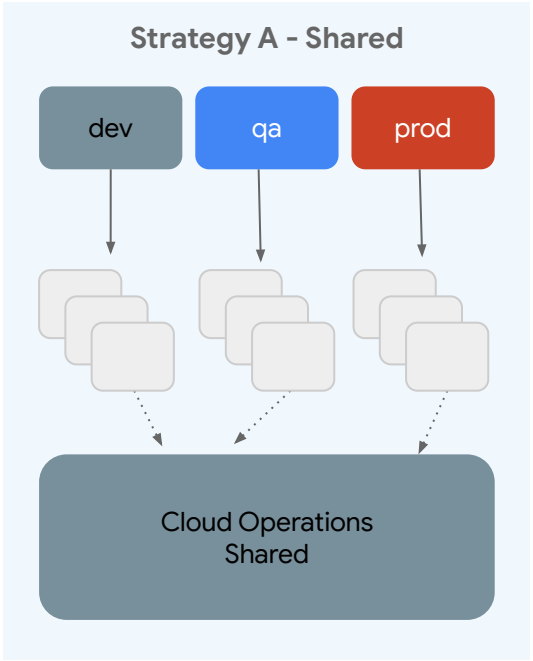


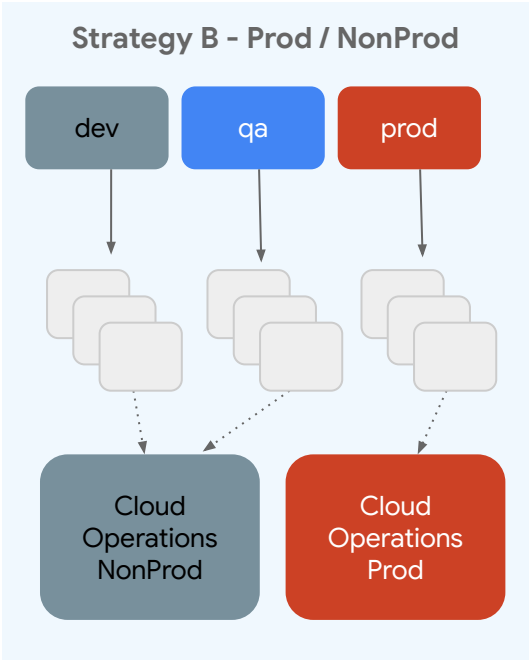
Cloud Operations architecture

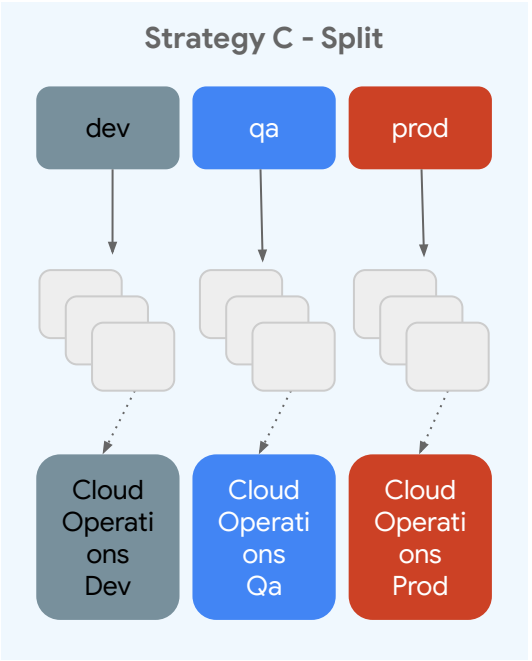


- **Workspaces** organize monitoring information in Cloud Operations Monitoring
- It contains the custom **dashboards**, **alerting** policies, **uptime checks** for monitored projects
- Metric data and log entries remain in the individual projects
- Each workspace can have up to 100 monitored projects

Cloud Operations workspace strategy







Cloud Operations pricing

Non-chargeable: Audit logs that are enabled by default as well as Access Transparency logs

Chargeable: Any other logs. e.g: Data Access except for BigQuery, VPC flow logs, Firewall logs, NAT logs

Free allotment for chargeable Cloud Operations products

- **Logging data** per **project** [GiB]
- **Monitoring data** per **billing account** [GiB]
- Monitoring **API calls**

Estimate, control, and reduce costs:

- **Sampling**
- **Log exclusions**
- **Logging quotas**

Cloud Monitoring: Qwik Start

50 minutes 1 Credit Rate Lab

GSP089

Google Cloud Self-Paced Labs

Agenda

- Development in the cloud
- Deployment: Infrastructure as code
- Monitoring: Cloud Operations basics
- Monitoring: Cloud Logging
- Monitoring: Cloud Operations monitoring
- Lab

Logging

Collect	**Automatic logging** to Cloud Operations on all GCE and GKE VMs Logs organized **by project** Additional **log parsing** through custom *fluentd* configuration
Export	Export to **Google Cloud Storage**, or **Pub/Sub**, or **BigQuery** Export **log-based metrics** to Cloud Operations Monitoring
Analyze	Analyze log data **in real-time** with **Pub/Sub**, **Dataflow** and **BigQuery** Analyze **archived logs** from **Cloud Storage**
Retain	Cloud Operations retains logs for **30 days** and admin logs for **400 days** **Longer retention** available in Google Cloud Storage or BigQuery

Logging type overview

Admin audit logs

- Admin console audits
- User audits
- Separate API and UI
- Export to BigQuery (eSKU and TT)

GCP audit logs

- Admin activity logs (always enabled)
- Data access logs (disabled by default)
- Access transparency (disabled by default)

Cloud Logging agent

- FluentD agent
- Common third-party applications
- System software

Network logs

- VPC flow
- Firewall rules
- NAT gateway

Access transparency logs

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

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

GCP audit logs

Admin activity

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

Default retention is **400 days**

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

Available at **no charge**

EXAMPLE RECORD

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

Always enabled

Data access

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

Default retention is **30 days**

EXAMPLE RECORD

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

Needs to be enabled

Access transparency

Audit Google access to your resources

Access justification

Resource identification

Available at **no charge**

Default retention is **400 days**

EXAMPLE RECORD

```
Object: /buckets/XYZ
Action: READ
Reason: Ticket #12345
```

Needs to be enabled

Cloud Operations OS logging agent

The logging agent streams logs from common third-party applications and system software to Cloud Logging:

- Supports third-party applications such as:
  - Apache/Tomcat/Nginx
  - Chef/Jenkins/Puppet
  - Cassandra/Mongodb/MySQL
- Based on fluentd log data collector - can add own Fluentd configuration files
- Supports major operating systems:
  - CentOS
  - Debian
  - Red Hat Enterprise Linux
  - Ubuntu LTS
  - Windows server

VPC flow logs

VPC flow logs aims to introduce granular VM flow level network telemetry on Google Cloud Platform

- Visibility into network availability and performance
- Understand why the traffic changes; traffic planning
- Billing: understand the expense and reduce the traffic cost
- Network forensics

Creating and Alerting on Logs-based Metrics

1 hour 30 minutes 5 Credits ★★★★½

GSP091

Google Cloud Self-Paced Labs

Agenda

- Development in the cloud
- Deployment: Infrastructure as code
- Monitoring: Cloud Operations basics
- Monitoring: Cloud Logging
- Monitoring: Cloud Operations monitoring
- Lab

VPC flow logs (cont.)

- **Flow record includes**
  - 5-tuple (src/dest ip:port and protocol)
  - Timestamp
- **Metrics**
  - Packets, bytes (throughput), RTT for TCP flows
  - VPC annotations: region, zone, VM name
  - Geo annotations: country, region, city
  - Logs is collected on each VM connection during the aggregated time interval (five seconds)
- **Log records based on filters defined in Cloud Operations**
  - Cloud Logging
  - Export to Pub/Sub
  - Export to BigQuery

Firewall rules logging

Field	Values
connection	src_ip=10.10.0.99, src_port=[EPHEMERAL_PORT], dest_ip=10.20.0.99, dest_port=80, protocol=tcp
disposition	DENIED
rule_details	Reference = "network:example-net/firewall:rule-a" priority = 10 action = DENY destination_range = 10.20.0.99/32 ip_port_info = tcp:80 direction = egress
instance	project_id="example-proj" instance_name=VM1 region=us-west1 zone=us-west1-a
vpc	project_id="example-proj" vpc_name=example-net subnetwork_name=west-subnet
remote_instance	project_id="example-proj" instance_name=VM2 region=us-east1 zone=us-east1-a
remote_vpc	project_id="example-proj" vpc_name=example-net subnetwork_name=east-subnet

Logging and monitoring

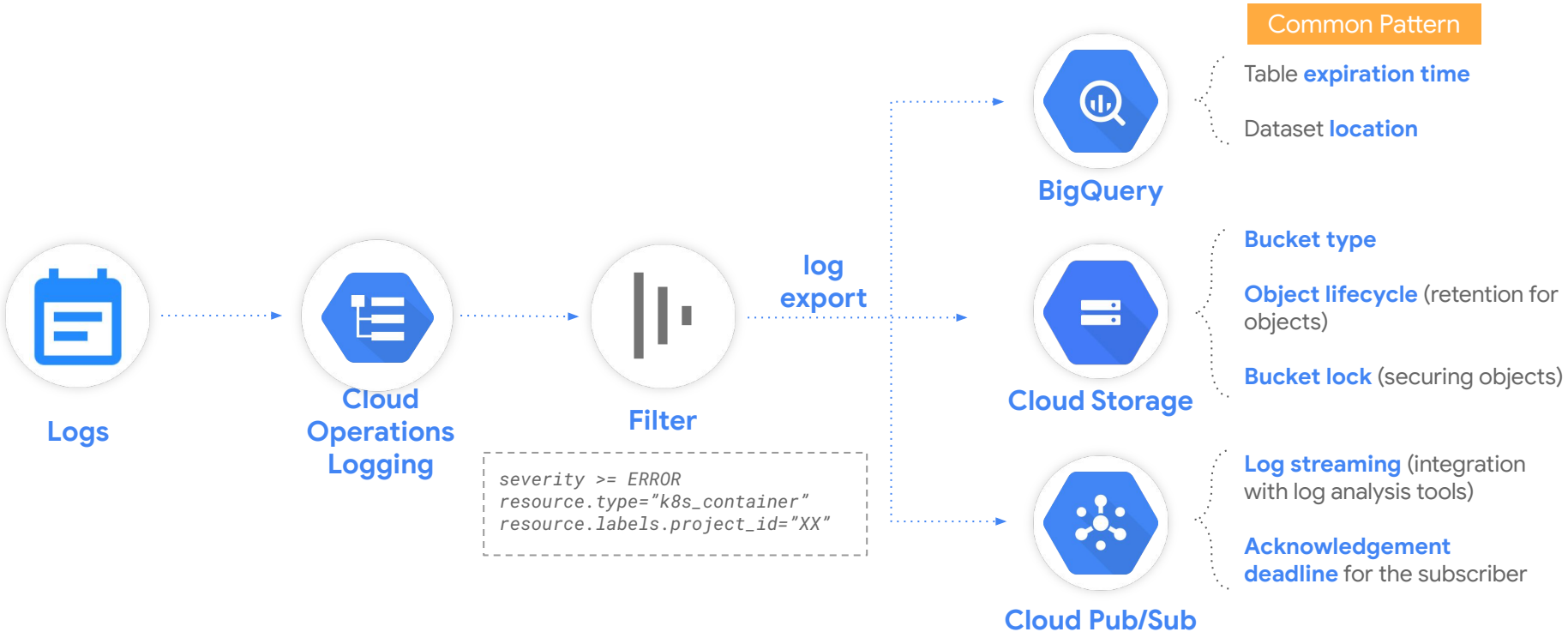
- You enable firewall rule logging individually for each firewall rule
- Firewall rule logging only records TCP and UDP connections.
- Log entries are written from the perspective of VM instances.

Cloud NAT logging

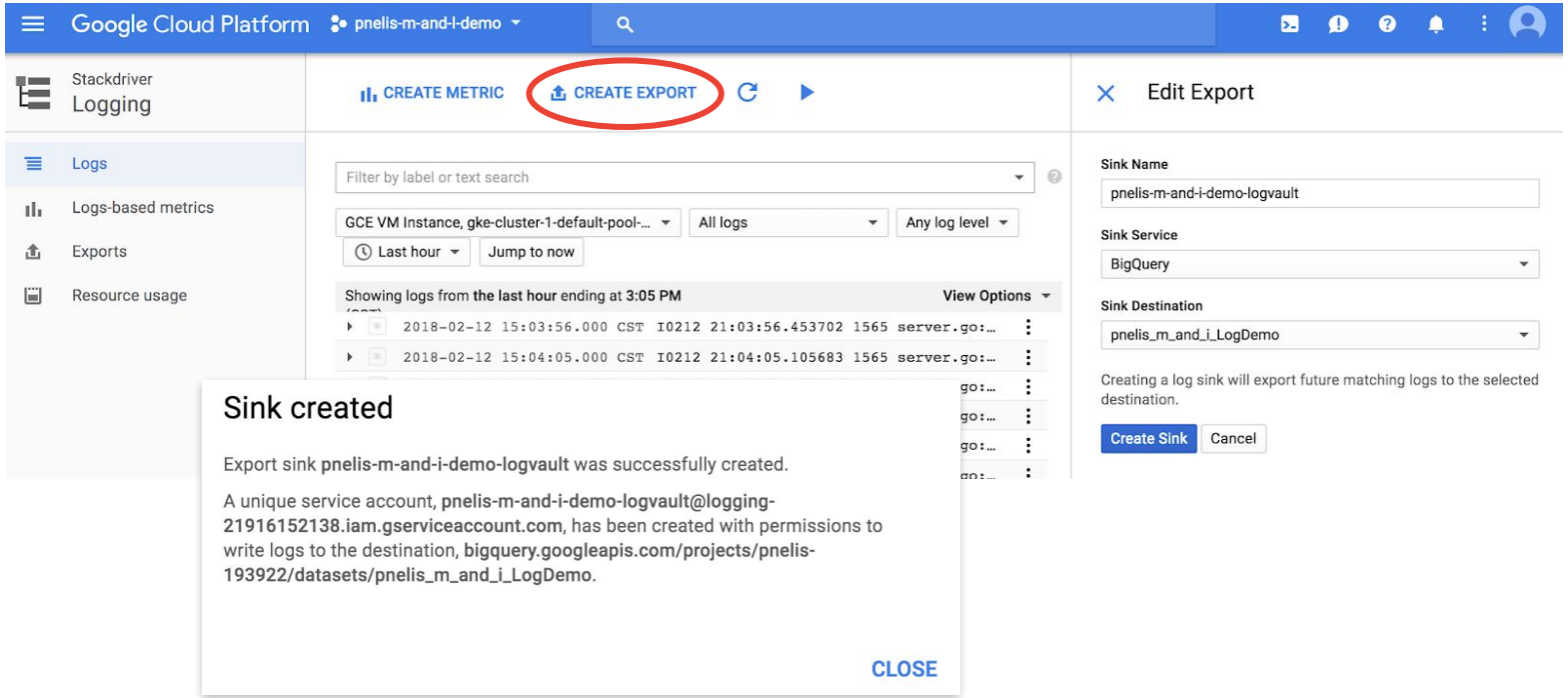
Allows logging NAT connections and errors

- Logs NAT connections and errors
- Understand why the traffic changes; traffic planning
- Billing: understand the expense and reduce the traffic cost
- Network forensics

Log exports

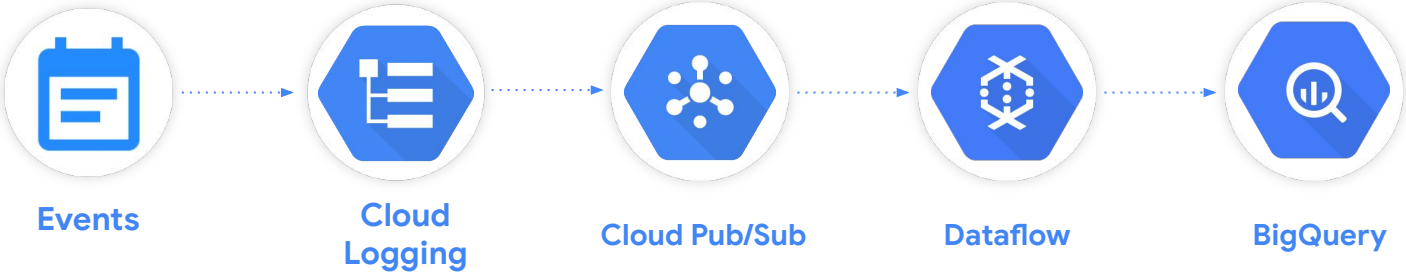

Common Pattern
Table expiration time
Dataset location
BigQuery
Bucket type
Object lifecycle (retention for objects)
Bucket lock (securing objects)
Cloud Storage
Log streaming (integration with log analysis tools)
Acknowledgement deadline for the subscriber
Cloud Pub/Sub
Logs
Cloud Operations Logging
Filter
log export
severity >= ERROR
resource.type="k8s_container"
resource.labels.project_id="XX"

Create a log export



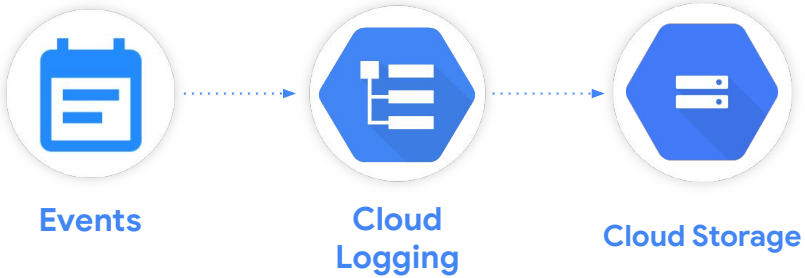
Real-time logs streaming

Example pipeline



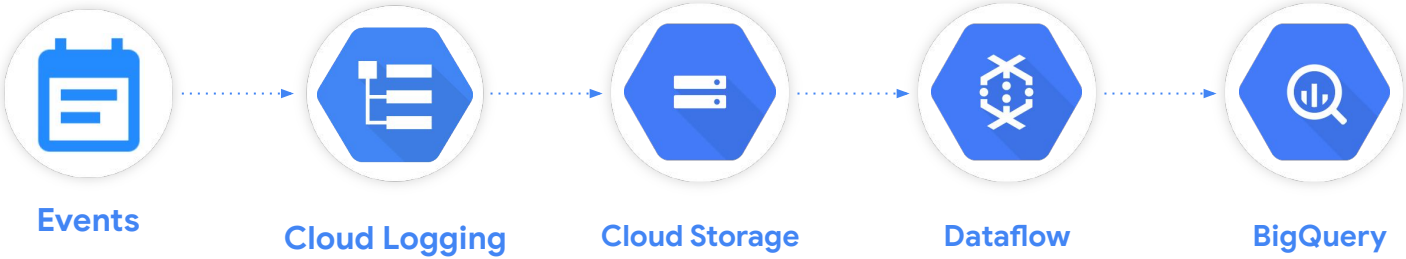
Log archiving

Example pipeline

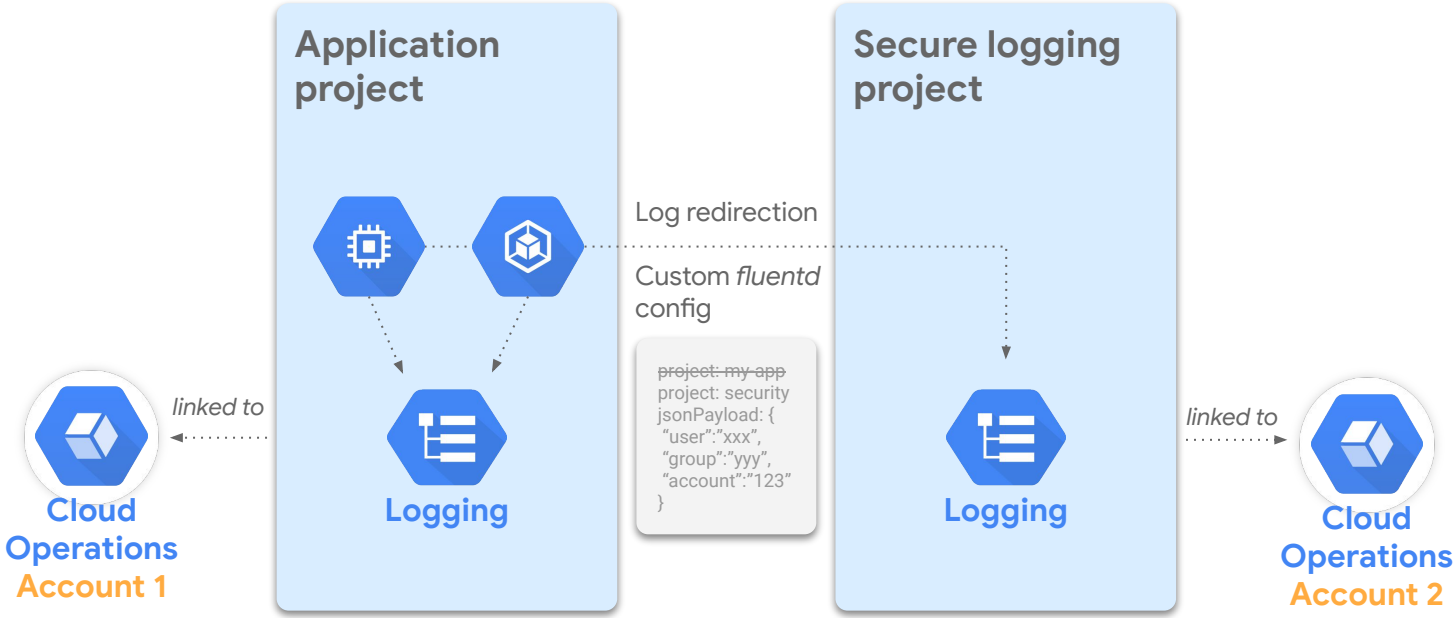


Log analysis

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).

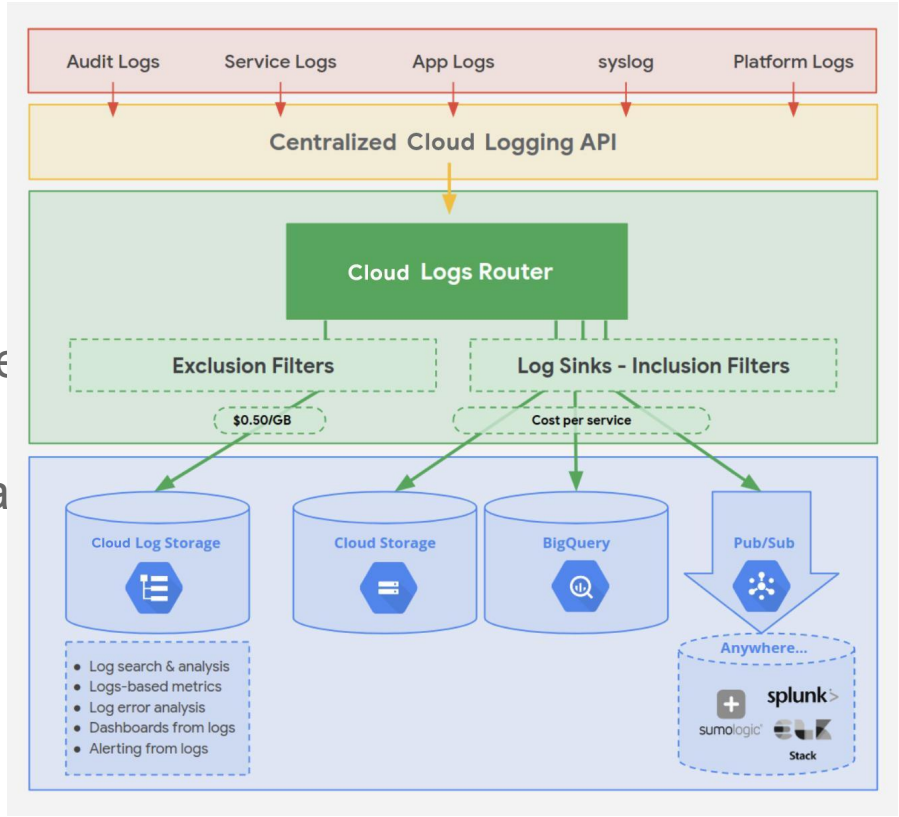
Organization

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

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

Log exclusions

- Specified by
  - exclusion **queries**
  - **resource-type** exclusions
- Admin logs are **not** excluded in ge
- Log exclusions can be **stopped**
- Logs can be sampled by percenta
- Excluded logs can be **exported**



Log compliance

Separation of duties (SoD)

- Use Aggregated Exports to centralise all logs from all projects into a single separate project, with different ownership than the source
- Choose Cloud Storage as the destination

Least privilege

- Only grant the right level of permissions required on the project / bucket containing the logs
- Avoid granting permissions to delete buckets / objects

Non-repudiation

- Cloud Storage automatically encrypts all data before it is written to disk
- Additional fortification can be implemented by **object-versioning** log buckets in conjunction with a **Bucket Lock**

Security Information and Event Management

An organization can export their logs to a third party SIEM solution

Integration through

- Agents @ SIEM side
- Add-on or connector

Example integrations

- **Splunk**

  Add-on for GCP

- **Elasticsearch**

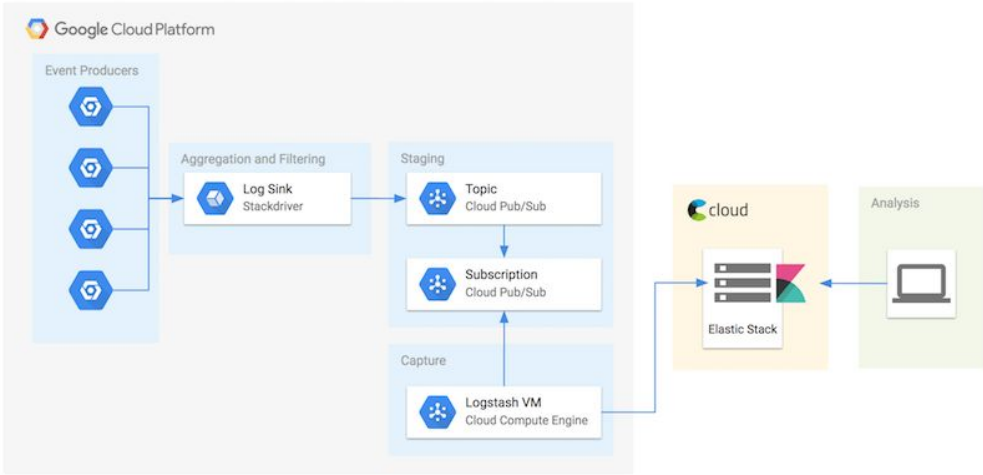
  Cloud Pub/Sub -> Logstash|Beats -> ES -> Kibana

- **Sumo Logic**

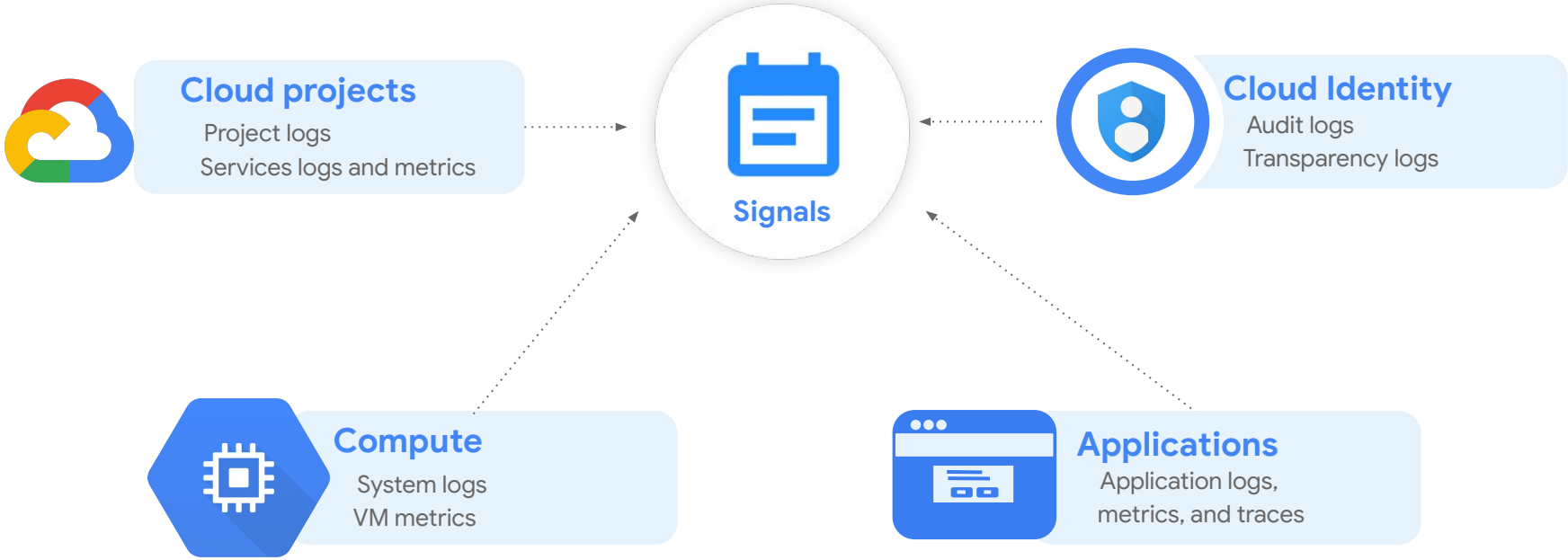
  Cloud Pub/Sub -> API webhook -> Sumo

- **ArcSight**

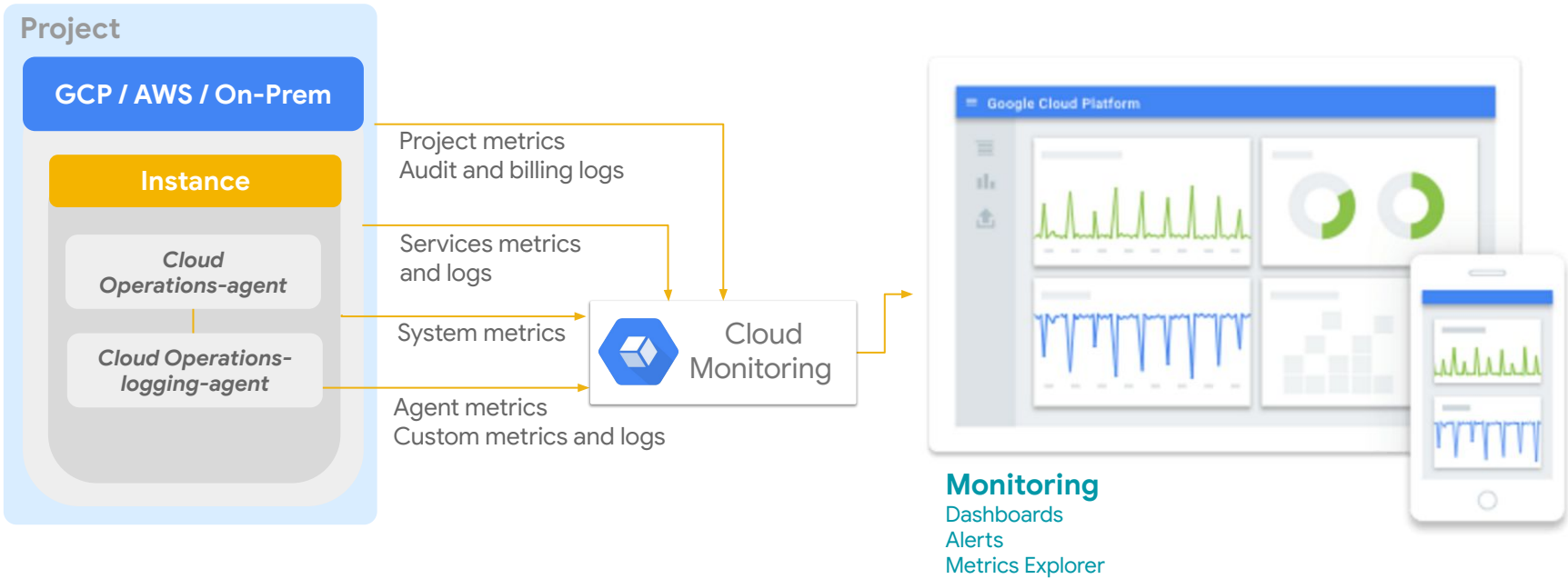
  FlexConnector for REST



Metrics sources



Resource monitoring



What metrics are collected by default?

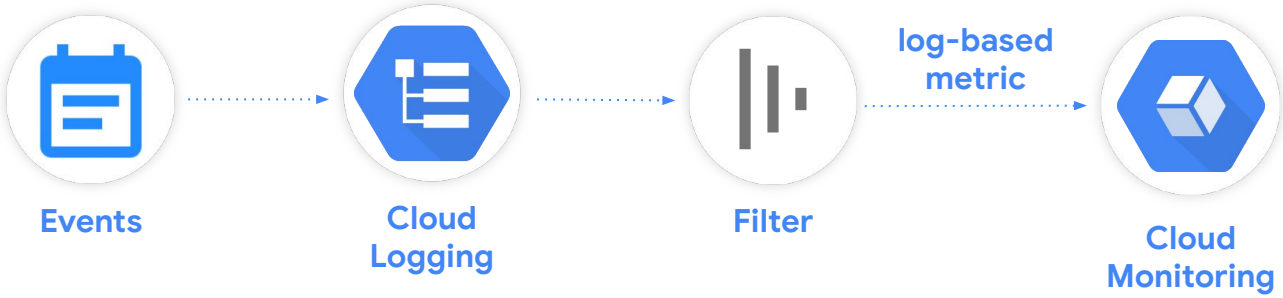
- Metrics on usage of **system resources** are collected on the following resources
  - CPU
  - Memory
  - Disk
- Extensive list of **services metrics** including monitoring and alerting on:
  - HTTP(s) IOPS
  - HTTP(s) response times
  - HTTP(s) error rates — average and max
  - Connections
  - Traffic
  - Database queries
  - Full list of metrics

Cloud Operations OS monitoring agent

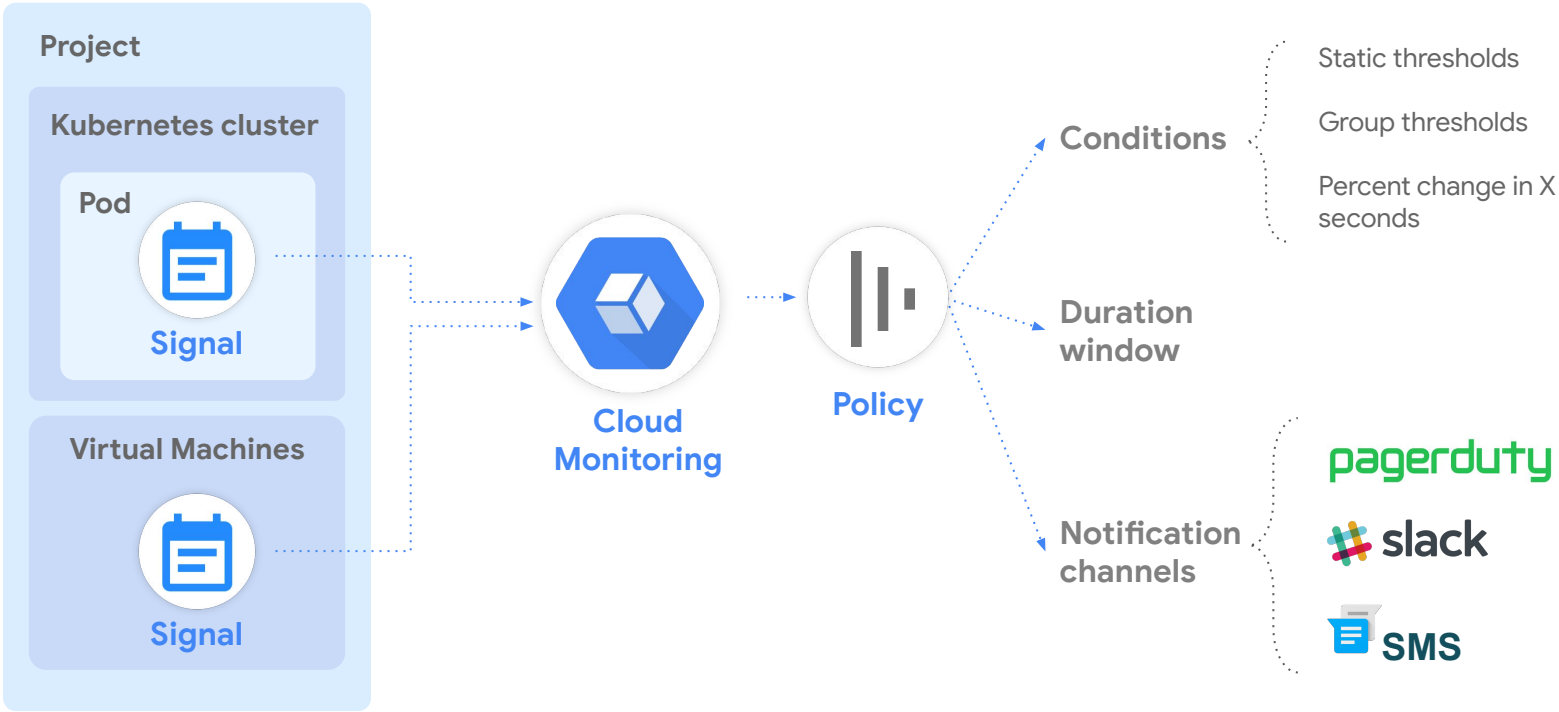
The monitoring agent gathers system and application metrics from virtual machine instances and sends them to Monitoring

- Optional, but recommended
- Gathers additional system resources and application metrics
- Based on collectd
- Supports third-party applications such as:
  - Apache/Tomcat/Nginx
  - Cassandra/Mongodb/MySQL
- Supports major operating systems:
  - CentOS
  - Debian
  - Red Hat Enterprise Linux
  - Ubuntu LTS
  - SUSE Linux Enterprise Server
  - Windows server

Log-based metrics



Alerting


Project
Kubernetes cluster
Pod
Signal
Virtual Machines
Signal
Cloud Monitoring
Policy
Conditions
Static thresholds
Group thresholds
Percent change in X seconds
Duration window
Notification channels
pagerduty
slack
SMS

Integration with external monitoring solutions

Metrics can be sent from Cloud Operations to external monitoring solutions via Cloud Monitoring API

Integration through

- Plugins/support from external monitoring solution side

Example integrations

- Datadog
- New Relic
- BlueMedora, a Cloud Operations Partner, can gather metrics from Cloud Operations and write into many supported destinations.

Monitoring and Logging for Cloud Functions

45 minutes 1 Credit

GSP092

Google Cloud Self-Paced Labs

You can view your Cloud Functions with their execution times, execution counts, and memory usage in the Cloud Console using Cloud Monitoring, where you can set up custom alerting on these metrics.