Monitoring

Memi Lavi
www.memilavi.com

Monitoring

- There are a lot of moving parts in the cloud
- VMs, App Engine, Functions, DBs, GKE and lots more
- It's important to know what's the status of the various components in the cloud
- Identify problems even before they occur and act accordingly
- Done using Monitoring

Monitoring

- Done using two main mechanisms:

Logs

- Text records indicating status of service
- Contains whatever data the service puts in
- Can be queried
- Can be analyzed
- Can define alerts

Metrics

- Numeric data indicating status of service
- ie. Number of errors / min, % of CPU utilization
- Can be viewed and analyzed
- Can define alerts

- Extremely important to have logs and metrics available
- The cornerstone of cloud monitoring

Cloud Logging

- Real time log management in the cloud
- Receives logs from various sources
- Stores the logs
- Allow search, analysis and monitoring
- Can collect logs also from your apps, on-prem resources and other cloud providers

Log Categories

Platform logs

- Written by Google Cloud services
- Helpful for debugging and troubleshooting services behavior
- Example: VPC Flow Logs

Component logs

- Written by Google Cloud software
- Example: GKE software components

Security logs

- “Who did what, where and when”
- Cloud Audit logs: Document actions and access to services
- Access Transparency: Document actions done by Google staff

User written logs

- Logs generated by custom apps and services
- Created using Logging API, client library or Ops Agent

Audit Logs

Admin Activity

- Log entries for actions that modify services
- ie. Creating a VM instance
- Always written, can't be disabled

Data Access

- Log entries for any read access to configuration or metadata
- Can become very large
- Disabled by default

System Event

- Log entries for actions initiated by Google
- Aren't driven by user action
- Always written, can't be disabled

Policy Denied

- Records access denied events
- Generated when a user or service accounts try to access service and the access is denied
- Can't be disabled

Log Storage

- By default logs are stored in two log buckets

`_Required`

- Receives logs routed by the `_Required` sink
- For log types:
  - Admin Activity audit logs
  - System Event audit logs
  - Login audit logs
  - Access transparency logs
- Retention:
  - 400 days
  - Can't be configured
- Can't be deleted or modified

`_Default`

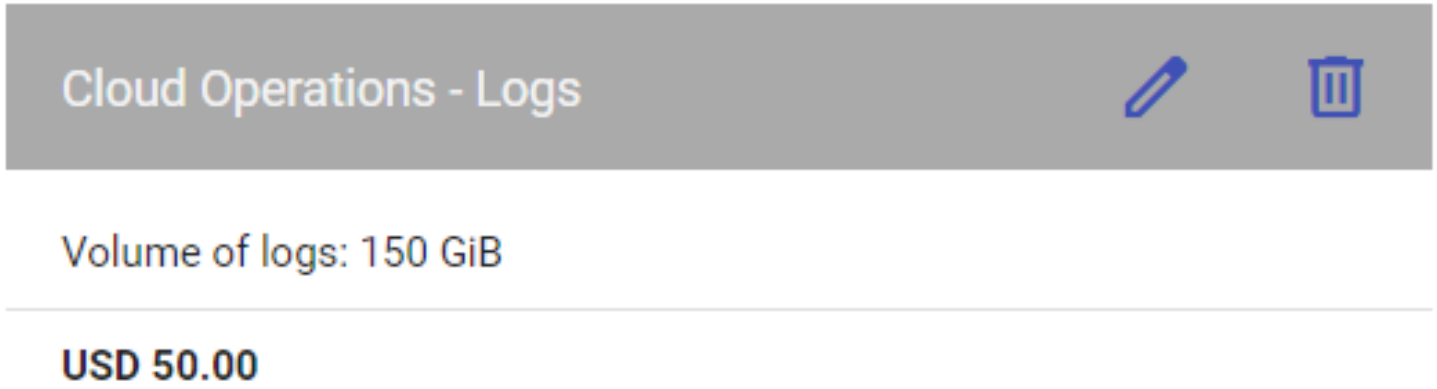
- Receives logs routed by the `_Default` sink
- For all the log types not routed to `_Required`
- Retention:
  - 30 days
  - Configurable
- Can't be deleted, can be modified

Additional buckets can be configured

Cloud Logging

- SLA: 99.95%
- Pricing:
  - Based on:
    - Storage (no cost for _Required logs, first 50GB free)
    - Retention (if configured to more than default)

Cloud Logging Pricing



Viewing Logs

- Two ways to view logs:

Logs Explorer

Log Analytics

Logs Explorer

- Used to troubleshoot and analyze performance of services and applications
- Great for querying logs
- Shows histograms of the data
- Supports the Logging Query Language
- No support for aggregate queries

Log Analytics

- Used to analyze log
  - Find patterns, see trends and more
- Supports aggregation
- Uses SQL to query logs
- Includes charts

Log Analytics

- Requires upgrade to the log bucket
- Not supported in all regions
- No cost

Metrics

- Numeric, time-series data
- Helps identify problems and patterns in a resource
- Built-in in most resources
- Can define alerts based on metrics

Dashboards

- GCP automatically creates dashboards for resources deployed in the cloud
- The dashboards show various metrics and actions of the resources
- Cannot be customized
- Custom dashboards can be created with custom data

ReadIt!

Architecture: ReadIt Cloud System