logging in GCP

20 May 2021   12:44

```
                        cloud logging api
cloud logging -----------------------------> log router --------------> destination
```

In GCP log will be configured as below.

1. Log router help to move the logs from log explorer to destinations (like pub/sub, storage bucket, splunk, BigQuery dataset, and other project)
    logs which are written to cloud logging api are pass through the log router. whenevr logs are entry arrives. logging compares the log entry to the filters of the sinks associated with resource

 So now, will learn about SINKS,

    1. sink in log router check each log entry against existing inclusion and exclusion filters that determine if the log entry should be sent to storage destinations or any other destinations.

    2. sinks route logs entries to storage destinations and used to exclude logs entries that are being written to cloud logging(filter and destination)

    3. Two pre-defined log sinks for each google cloud project
        1. _Required
           admin activity audit logs, system event audit logs, access transparency logs are moved to _required logs
        2. _Default
          the logs which doesn't fit to _required will be moved to _default(automatically logs will be moved these log sinks)
    4. you can create exclusion filters, which excludes the matching log entries.

 properties of sinks:-
    1. sinks identifier :- Name of the sink.
    2. Parent Resource :- Google cloud resource in which we create sink.
        1. projects 2. Folders 3. billing ac
    3. inclusion filter :- selects which log entries to pass through
    4. exclusion filter :- selects which log entries not to pass through
    5. Destination : - A place to send and store logs
    6. writter identity : - A service account name where it has the permision to write the destination
    7. include children :- comes in aggregated sinks

How to create sinks:-
   Go to console --> logging --> Create sinks --> create sink as follows (here we are moving logs to storage bucket)

← Create logs routing sink

✓ **Sink details**

Provide a name and description for logs routing sink

Name	kavya-021
Description	

✓ **Sink destination**

Select the service type and destination for logs routing sink

Service	Cloud Storage bucket
Destination	storage.googleapis.com/test-python-bu [copy] t

✓ **Choose logs to include in sink**

Create an inclusion filter to determine which logs are included in logs routing sink

Inclusion filter

```
resource.type=nat_gateway
resource.labels.project_id="my-first-proj
```

④ **Choose logs to filter out of sink** (optional)

Create exclusion filters to determine which logs are excluded from logs routing sink