

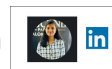


BigQuery Alerting



Google
BigQuery

Diksha Chourasiya



Big Query query notifications using Cloud Logging and Monitoring

Step-1

Write a Query

This is a stored procedure which is checking whether the table contains any record or not. If not, then it is forcefully raising an Exception.

- A variable for storing our number of rows and an EXCEPTION to allow us to reraise an exception which will automatically be logged in Cloud Logging.
- If our row_count is as expected the query completes, if the count is zero we are forcing an error to raise(dividing by 0)
- Then again raising an exception which we can filter in Cloud Logging using the custom message used in the Exception.
- After this we can schedule this query using the Scheduling option of Bigquery and then accordingly the logs will be stored in Cloud Logging.

```
BEGIN
  DECLARE row_count INT64;

  SET row_count = (
    SELECT count(*) FROM [REDACTED] where
date(bq_insert_ts) =CURRENT_DATE()-1
  );

  IF row_count = 0 THEN
    SELECT 1/0; -- force an error to be raised
  END IF;

  -- force an error to be raised
EXCEPTION WHEN ERROR THEN
  RAISE USING MESSAGE = 'Table has 0 count!';
END;
```

NOTE: Mention the Table Name in which you want to apply Alert! .

Also mention the custom message carefully!

Step-2

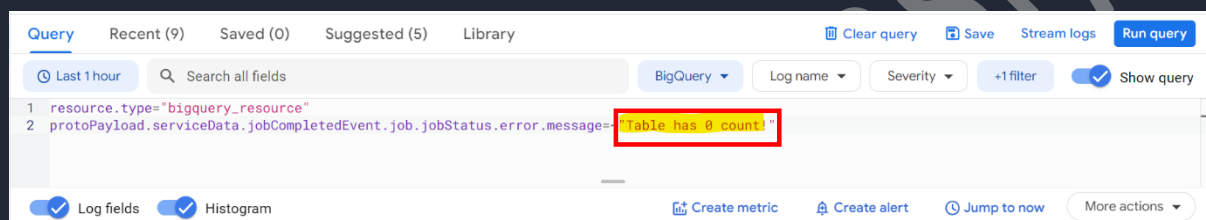
Filtering logs in Cloud Logging

As part of BigQuery Audit logging each query is logged into the Cloud Logging service.

That's the reason we have added custom message in the Stored Procedure so that we can easily filter out the log associated with the Error.

Query to be used to filter the logs in the Logging.

```
resource.type="bigquery_resource"
protoPayload.serviceData.jobCompletedEvent.job.jobStatus.error.message=~"Table has 0 count!"
```



NOTE: The Highlighted part should be the message used in the Stored Procedure.

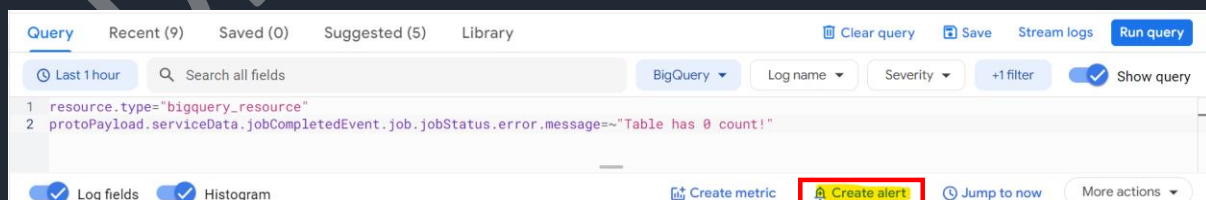
So, whenever any message got logged into the Cloud Logging an alert should be triggered.

Step-3

Create Alerts

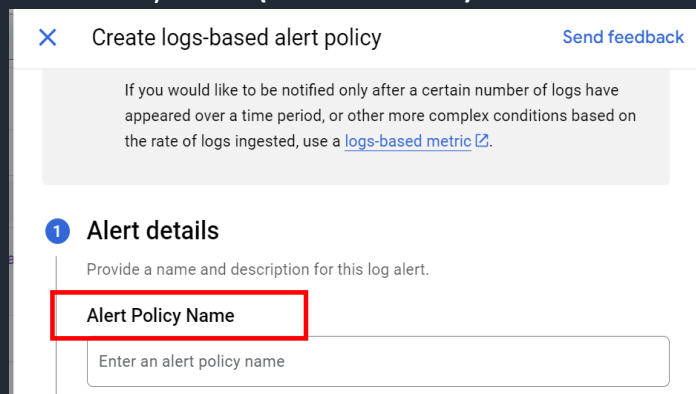
So, we can create an alert every time we see an instance that matches this line.

Step-1 :



Step-2 The Following window will appear wherein you have to fill the information to create the alert.

a) Give the Alert Policy Name (Ex: No Records)



×

 Create logs-based alert policy [Send feedback](#)

If you would like to be notified only after a certain number of logs have appeared over a time period, or other more complex conditions based on the rate of logs ingested, use a [logs-based metric](#).

1 Alert details

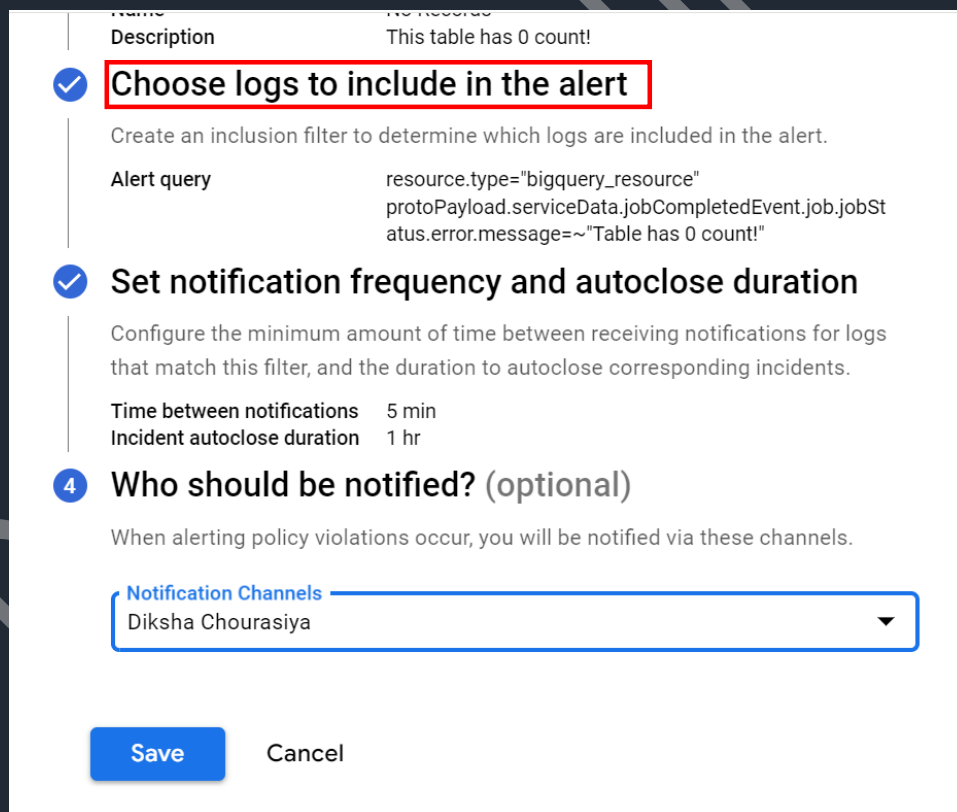
Provide a name and description for this log alert.

Alert Policy Name

Enter an alert policy name

255 characters

b) Choose the Logs to be included in which you want to set the alert.



Name: No Records

Description: This table has 0 count!

✓ **Choose logs to include in the alert**

Create an inclusion filter to determine which logs are included in the alert.

Alert query: resource.type="bigquery_resource"
protoPayload.serviceData.jobCompletedEvent.job.jobStatus.error.message=~"Table has 0 count!"

✓ **Set notification frequency and autoclose duration**

Configure the minimum amount of time between receiving notifications for logs that match this filter, and the duration to autoclose corresponding incidents.

Time between notifications: 5 min
Incident autoclose duration: 1 hr

4 **Who should be notified? (optional)**

When alerting policy violations occur, you will be notified via these channels.

Notification Channels: Diksha Chourasiya

Save Cancel

This is the condition when met, the alarm will be triggered.(The Condition is same which is used to filter the logs In the Cloud Logging)

2 Choose logs to include in the alert

Create an inclusion filter to determine which logs are included in the alert.

i Alert will be scoped to logs generated by the following project:
[Redacted]

Define log entries to alert on **?** [Preview logs](#)

```
resource.type="bigquery_resource"  
protoPayload.serviceData.jobCompletedEvent.job.jobStatus.error.message=~"Table has 0 count!"
```

- c) Set the Email Frequency you want to send out the Email and its auto close duration (The time at which the incident which occurred will be auto close)

3 Set notification frequency and autoclose duration

Configure the minimum amount of time between receiving notifications for logs that match this filter, and the duration to autoclose corresponding incidents.

Time between notifications *
5 min

Incident autoclose duration
7 days

Select a duration after which the incident will close automatically when matching log entries are absent.

[Next](#)

- d) Then you have to set the notification channel to whom you want to send out the Email (Either you can select Single Person's Email ID or group of ID ,a channel)

4 Who should be notified? (optional)

When alerting policy violations occur, you will be notified via these channels.

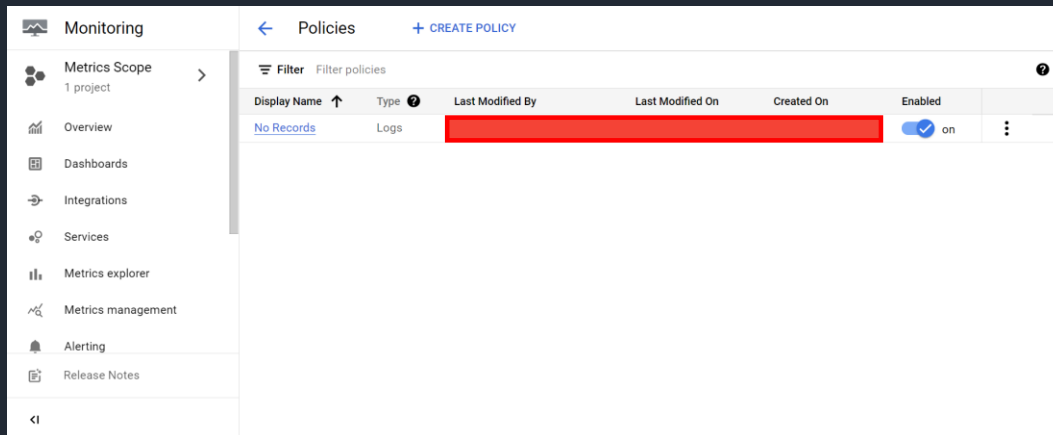
Notification Channels

[Save](#) [Cancel](#)

Step-4

Manage Alerts

Once the alert is created you can manage it from the Monitoring window shown as below.



Alerts

The Alert will look like this which we sent to the Email which you have mentioned above while creating the Alert Policy.

