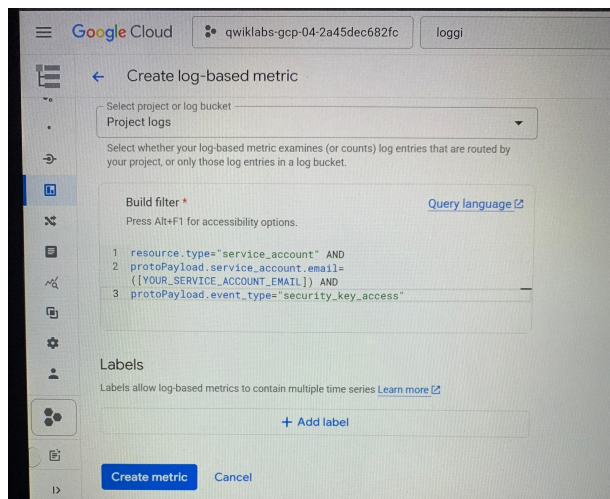# LOG BASED ALERT POLICY

Log-based alerting policies are most useful for monitoring security-related events since they monitor log data. You can use them to notify you anytime a specific event appears in a log. For example, I created an alert that's triggered when a user account accesses the security key of a service account. Here are steps I used to create, configure, and test such a log-based notification system on google cloud console.

log-based alerting policy can be created from the **Logs Explorer** page in the Google Cloud console or by using the Monitoring API. I described how to create log-based alerting policies by using Logs Explorer.

First step: I created a log based metric

This metric will count the number of log entries matching a specific filter that indicates a user has accessed the security key of a service account.

Second step: I created a log based alert

This alert will trigger a notification whenever the newly created " security key access" metric reports a value greater than a specified threshold.

Third step: The alert was tested

This step stimulates the event that the metric and alert are designed to track.