Log Metric Filter and Alerts Exist for VPC Network Changes (Automated)

1. Go to Logging/Logs-based Metrics by visiting

<https://console.cloud.google.com/logs/metrics>

and click "CREATE METRIC".

2. Click the down arrow symbol on Filter Bar at the rightmost corner and select

Convert to Advanced Filter.

3. Clear any text and add:

resource.type="gce\_network" AND (protoPayload.methodName:"compute.networks.insert" OR protoPayload.methodName:"compute.networks.patch" OR protoPayload.methodName:"compute.networks.delete" OR protoPayload.methodName:"compute.networks.removePeering" OR protoPayload.methodName:"compute.networks.addPeering")

Click Submit Filter. Display logs appear based on the filter text entered by the user.

5. In the Metric Editor menu on the right, fill out the name field. Set Units to 1

(default) and Type to Counter. This ensures that the log metric counts the number of log entries matching the user's advanced logs query.

6. Click Create Metric.

Create the prescribed alert policy:

1. Identify the newly created metric under the section User-defined Metrics at

<https://console.cloud.google.com/logs/metrics>

2. Click the 3-dot icon in the rightmost column for the new metric and select Create alert from Metric. A new page appears.

3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a

threshold of 0 for the most recent value will ensure that a notification is triggered for every owner change in the project:

Set `Aggregator` to `Count` Set `Configuration`: - Condition: above - Threshold: 0 - For: most recent value

4. Configure the desired notification channels in the section Notifications.

5. Name the policy and click Save.

From Google Cloud CLI

Create the prescribed Log Metric:

• Use the command: gcloud logging metrics create

Create the prescribed alert policy:

• Use the command: gcloud alpha monitoring policies create