Lab:

Create the prescribed log metric:

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 the Filter Bar at the rightmost corner and select Convert to Advanced Filter.

3. Clear any text and add:

protoPayload.methodName="SetIamPolicy" AND protoPayload.serviceData.policyDelta.auditConfigDeltas:\*

4. 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 will ensure that the log metric counts the number of log entries matching the user's advanced logs query.

6. Click Create Metric.

Lab

Create a prescribed Alert Policy:

1. Identify the new metric the user just created, 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 opens.

3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the organization. For example, a threshold of zero(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 notifications channels in the section Notifications.

5. Name the policy and click Save.

Lab

Create the prescribed log metric:

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 the Filter Bar at the rightmost corner and select Convert to Advanced Filter.

3. Clear any text and add:

resource.type="iam\_role" AND (protoPayload.methodName = "google.iam.admin.v1.CreateRole" OR protoPayload.methodName="google.iam.admin.v1.DeleteRole" OR protoPayload.methodName="google.iam.admin.v1.UpdateRole")

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

2. 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 advanced logs query.

3. Click Create Metric

Lab

Create a prescribed Alert Policy:

1. Identify the new metric that was just created 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 metric and select Create alert from Metric. A new page displays.
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 zero(0) for the most recent value ensures 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

Configure the desired notification channels in the section Notifications.

Name the policy and click Save.