

# Monitoring Multiple Projects with Cloud Monitoring

## Task 1. Create Project 2's virtual machine

1. At the top of the screen, click on the dropdown arrow next to Project 1's name.



2. Make sure that you're on the **All** tab, then click on the name of **Project 2** to go into it.



3. Select **Navigation menu** > **Compute Engine** > **VM instances** to open the VM instances window.
4. Click **Create Instance** to create a new instance.
5. In the **Machine configuration**:

Enter the values for the following fields:

Field	Value (type or select)
Name	instance2
Region	us-west1
Zone	us-west1-a

Leave all of the options at the default settings.

6. Click **Create**.

Now you have resources to monitor in both of your projects.

## Create a Monitoring Metrics Scope

Set up a Monitoring Metrics Scope that's tied to your Google Cloud Project. The following steps create a new account that has a free trial of Monitoring.

- In the Cloud Console, click **Navigation menu** (☰) > View All Products > Observability > **Monitoring**.  
When the Monitoring **Overview** page opens, your metrics scope project is ready.

Now add both projects to Monitoring.

1. In the left panel, click **Settings** and in the Settings window navigate to **Metric Scope** tab, click **+Add projects** in the **Google Cloud Projects** section.
2. Click **Select Projects**.
3. Check Project ID 1 and click **Select**.

4. Click **Add projects**.

## Task 2. Monitoring Overview

Click on **Overview** in the left menu. You'll be adding a lot of good information here as the lab goes along. First, you'll create a [Cloud Monitoring Group](#) for visibility across both projects.

### About Cloud Monitoring groups

Cloud Monitoring lets you define and monitor groups of resources, such as VM instances, databases, and load balancers. Groups can be based on names, tags, regions, applications, and other criteria. You can also create subgroups, up to six levels deep, within groups.

### Create a Cloud Monitoring group

1. In the left menu, click **Groups**, then click **+Create group**.
2. Name your group **DemoGroup**.

The **Criteria** is a set of rules that will dynamically evaluate which resources should be part of this group.

Cloud Monitoring dynamically determines which resources belong to your group based on the filter criteria that you set up.

- In the first dropdown field (Type), **Name** is selected by default.
  - In the second dropdown (Operator), **Contains** is selected by default.
  - In the third field (Value), type in "instance" since both of the instance names in both of your projects start with the word `instance`.
3. Click **Done**, then click **Create**.

## Task 3. Uptime check for your group

Uptime checks let you quickly verify the health of any web page, instance, or group of resources. Each configured check is regularly contacted from a variety of locations around the world. Uptime checks can be used as conditions in alerting policy definitions.

1. In the left menu, click **Uptime checks**, then click **+Create uptime check**.
2. Create your uptime check with the following information:

**Protocol:** TCP

**Resource Type:** Instance

**Applies To:** Group, and then select **DemoGroup**.


**Port:** 22

**Check frequency:** 1 minute, then click **Continue**.

3. Click **Continue** again.
4. Leave the slider **ON** state for **Create an alert** option in **Alert & notification** section, then click **Continue**.
5. For **Title:** enter `DemoGroup uptime check`.
6. Click **TEST** to verify that your uptime check can connect to the resource.
7. When you see a green check mark everything can connect, click **Create**

## Task 4. Alerting policy for the group

Use Cloud Monitoring to create one or more alerting policies.

1. In the left menu, click **Uptime checks**.
2. Click the three dots  at the far right of your Display Name and click **Add alert policy**.
3. Click **+Add alert condition**.
4. Select the previously created **Uptime health check on DemoGroup** condition from the left section and click **Delete alert condition**.
5. In your **New condition**, click **Select a metric**.
6. Uncheck the **Active**.
7. In the **Select a metric** field, search `check_passed` and click **VM Instance > Uptime\_check > Check passed**. Click **Apply**.
8. Click **Add a filter**, set the **Filter** to **check\_id** and select **demogroup-uptime-check-id** as the **Value**. Click **Done**.

**Note:** If `demogroup-uptime-check-id` `check_id` is unavailable, please wait for a few seconds and try.

9. In the left panel, click on the arrow button next to **VM Instance-Check passed**, then click on **Configure trigger**.
10. Select **Metric absence** as Condition type and click **Next**.
11. Turn off **Configure notifications**.
12. In the **Alert policy name** field, enter the **Name** as **Uptime Check Policy**. Click **Next**.
13. Click **Create policy**.

## Task 5. Custom dashboard for your group



Create a custom dashboard so you can monitor your group easily.

1. In the left menu, click **Dashboards**, then click **+Create Custom dashboard**.
2. Name your dashboard.
3. Click **+Add Widget** and select **Line** option in **Visualization**.
4. In the **Metric** field, Uncheck the **Active**.
5. Search **uptime** (compute.googleapis.com/instance/uptime) and click **VM Instance > Instance > Uptime**. Click **Apply**.

The dashboard should look like:

6. Again click on **Apply**.

## Task 6. Remove one instance to cause a problem

1. In the console, select **Navigation menu** () > Compute Engine\*\*.
2. Check the box next to **instance2**, then click on the 3 vertical dots  at the top of the page and click **Stop**. Click **Stop** again to turn off the machine.
3. Wait a minute or 2 for the instance to stop and violate the uptime check you just set up. After a couple of minutes, turn your machine back on by clicking **Start/Resume**, then **Start**.

4. Click **Navigation menu** (☰) > View All Products > Observability > **Monitoring** > **Alerting** and refresh your browser. It may take a few more minutes to show that you have issues in the Summary section. Refresh until you see an Incident similar to this:

Incidents

State

Policy name

Incident summary

Opened

Uptime Check Policy

An uptime check on qwiklabs-gcp-04-a2882939812c instance2 is failing.

Dec 22, 2020, 4:16:46 PM

→

See all incidents

[SHOW CLOSED INCIDENTS](#)

**Optional:** Using the left menu, look at **Dashboards** to view your custom dashboard. This provides details on both VMs. If you mouse over your chart, you can see which of your instances was stopped and restarted.

## Incidents

When the alerting policy conditions are violated, an "incident" is created and displayed in the Incident section.

Responders can acknowledge receipt of the notification and can close the incident when it has been taken care of.

1. In the **Incidents** section, click on the name of the alerting policy that was violated to go into it.

You've already **fixed** your problem by turning the VM back on, so the incident was cleared and you no longer see an incident in the Incidents section.

2. To see the cleared incident, scroll down and click on the **Show closed incidents** link. Your incident should have a **Closed** status. You can read through the incident details.

3. You can also click on the **Uptime Check Policy** link to explore the metrics it gives you. In several more minutes the Monitoring Overview page will all go back to green when the instance in Project 2 passes the Uptime Check