Cloud Monitoring: Qwik Start

50 minutes1 Credit

Rate Lab

**GSP089**



**Overview**

Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Monitoring collects metrics, events, and metadata from Google Cloud, Amazon Web Services, hosted uptime probes, application instrumentation, and a variety of common application components including Cassandra, Nginx, Apache Web Server, Elasticsearch, and many others. Cloud Monitoring ingests that data and generates insights via dashboards, charts, and alerts. Cloud Monitoring alerting helps you collaborate by integrating with Slack, PagerDuty, HipChat, Campfire, and more.

This hands-on lab shows you how to monitor a Compute Engine virtual machine (VM) instance with Cloud Monitoring. You'll also install monitoring and logging agents for your VM which collects more information from your instance, which could include metrics and logs from 3rd party apps.

**Setup and Requirements**

**Before you click the Start Lab button**

Read these instructions. Labs are timed and you cannot pause them. The timer, which starts when you click **Start Lab**, shows how long Google Cloud resources will be made available to you.

This Qwiklabs hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that you use to sign in and access Google Cloud for the duration of the lab.

**What you need**

To complete this lab, you need:

* Access to a standard internet browser (Chrome browser recommended).
* Time to complete the lab.

**Note:** If you already have your own personal Google Cloud account or project, do not use it for this lab.

**Note:** If you are using a Pixelbook, open an Incognito window to run this lab.

**How to start your lab and sign in to the Google Cloud Console**

1. Click the **Start Lab** button. If you need to pay for the lab, a pop-up opens for you to select your payment method. On the left is a panel populated with the temporary credentials that you must use for this lab.



1. Copy the username, and then click **Open Google Console**. The lab spins up resources, and then opens another tab that shows the **Sign in** page.



***Tip:*** Open the tabs in separate windows, side-by-side.

If you see the **Choose an account** page, click **Use Another Account**. 

1. In the **Sign in** page, paste the username that you copied from the Connection Details panel. Then copy and paste the password.

***Important:*** You must use the credentials from the Connection Details panel. Do not use your Qwiklabs credentials. If you have your own Google Cloud account, do not use it for this lab (avoids incurring charges).

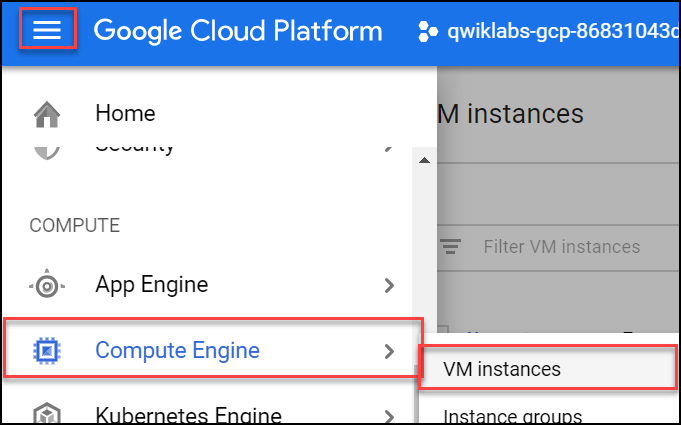
1. Click through the subsequent pages:
   * Accept the terms and conditions.
   * Do not add recovery options or two-factor authentication (because this is a temporary account).
   * Do not sign up for free trials.

After a few moments, the Cloud Console opens in this tab.

**Note:** You can view the menu with a list of Google Cloud Products and Services by clicking the **Navigation menu** at the top-left. 

**Create a Compute Engine instance**

1. In the Cloud Console dashboard, go to **Navigation menu** > **Compute Engine** > **VM instances**, then click **Create**.



1. Fill in the fields as follows, leaving all other fields at the default value:

|  |  |
| --- | --- |
| **Field** | **Value** |
| Name | lamp-1-vm |
| Region | us-central1 (Iowa) |
| Zone | us-central1-a |
| Series | N1 |
| Machine type | n1-standard-2 |
| Firewall | check Allow HTTP traffic |

1. Click **Create**.

Wait a couple of minutes, you'll see a green check when the instance has launched.

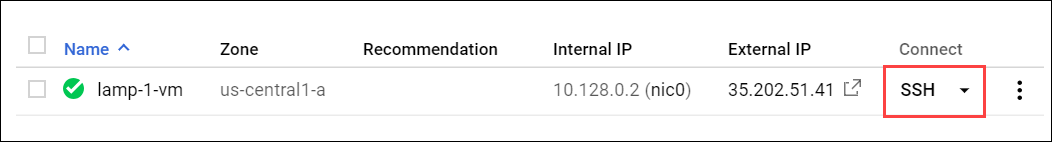
Click **Check my progress** below. A green check confirms you're on track.

Create a Compute Engine instance (zone: us-central1-a)

Check my progress

**Add Apache2 HTTP Server to your instance**

1. In the Cloud Console, click **SSH** to open a terminal to your instance.



1. Run the following commands in the SSH window to set up Apache2 HTTP Server:

sudo apt-get update

sudo apt-get install apache2 php7.0

When asked if you want to continue, enter **Y**.

**Note:** If you cannot install php7.0, use php5.

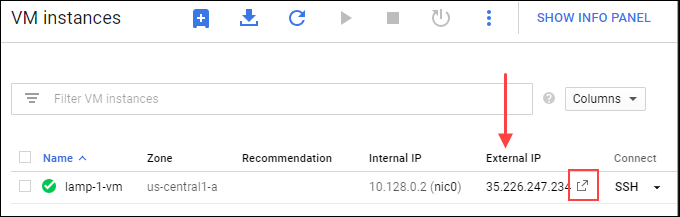
sudo service apache2 restart

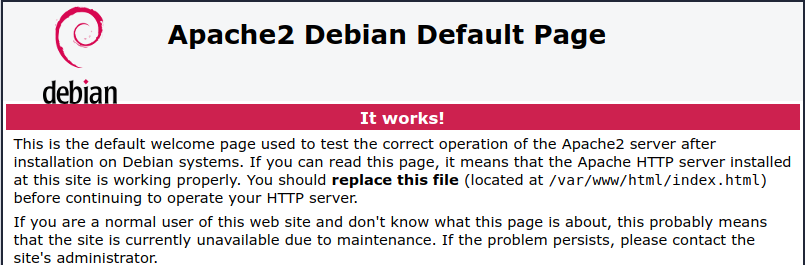
Click **Check my progress** below. A green check confirms you're on track.

Add Apache2 HTTP Server to your instance

Check my progress

1. Return to the Cloud Console, on the VM instances page. Click the External IP for lamp-1-vm instance to see the Apache2 default page for this instance.





Click **Check my progress** below. A green check confirms you're on track.

Get a success response over External IP of VM instance

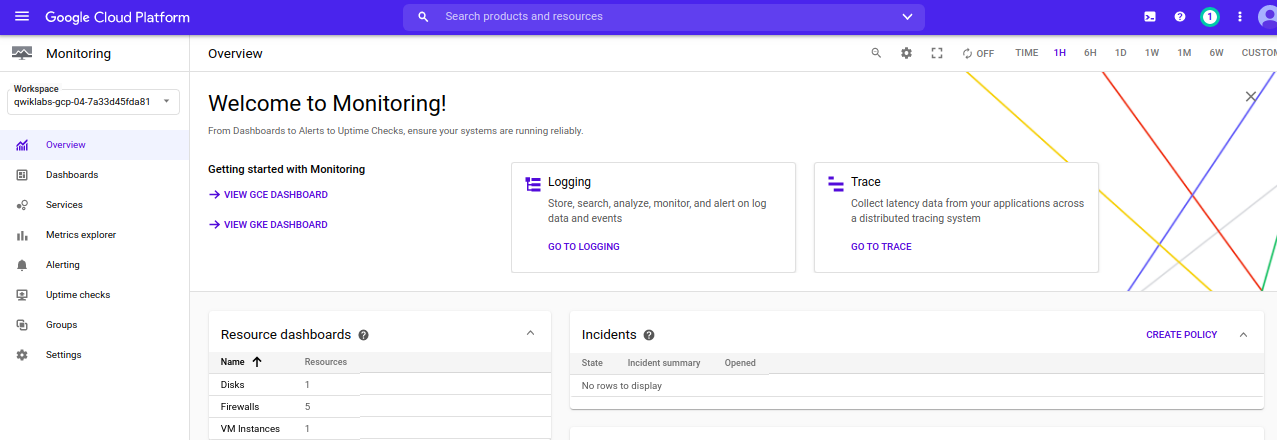
Check my progress

Create a Monitoring workspace

Now set up a Monitoring workspace that's tied to your Google Cloud Project. The following steps create a new account that has a free trial of Monitoring.

1. In the Cloud Console, click **Navigation menu** > **Monitoring**.
2. Wait for your workspace to be provisioned.

When the Monitoring dashboard opens, your workspace is ready.



Install the Monitoring and Logging agents

Agents collect data and then send or stream info to Cloud Monitoring in the Cloud Console.

The *Cloud Monitoring agent* is a collectd-based daemon that gathers system and application metrics from virtual machine instances and sends them to Monitoring. By default, the Monitoring agent collects disk, CPU, network, and process metrics. Configuring the Monitoring agent allows third-party applications to get the full list of agent metrics. See [Cloud Monitoring agent overview](https://cloud.google.com/monitoring/agent) for more information.

In this section, you install the *Cloud Logging agent* to stream logs from your VM instances to Cloud Logging. Later in this lab, you see what logs are generated when you stop and start your VM.

It is best practice to run the Cloud Logging agent on all your VM instances.

**Install agents on the VM:**

1. Run the Monitoring agent install script command in the SSH terminal of your VM instance to install the Cloud Monitoring agent.

curl -sSO https://dl.google.com/cloudagents/add-monitoring-agent-repo.sh

sudo bash add-monitoring-agent-repo.sh

sudo apt-get update

sudo apt-get install stackdriver-agent

When asked if you want to continue, enter **Y**.

1. Run the Logging agent install script command in the SSH terminal of your VM instance to install the Cloud Logging agent

curl -sSO https://dl.google.com/cloudagents/add-logging-agent-repo.sh

sudo bash add-logging-agent-repo.sh

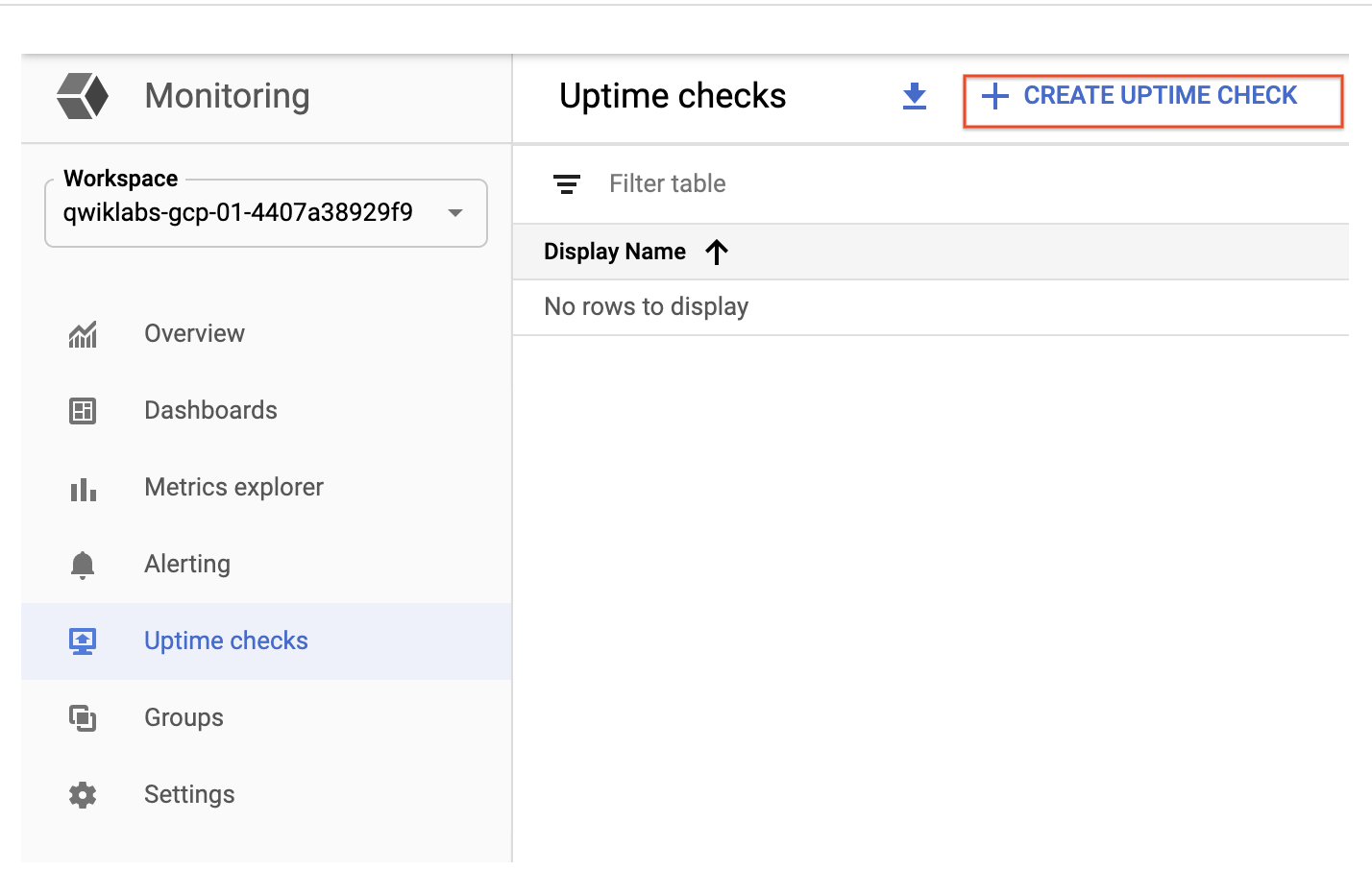
sudo apt-get update

sudo apt-get install google-fluentd

**Create an uptime check**

Uptime checks verify that a resource is always accessible. For practice, create an uptime check to verify your VM is up.

1. In the Cloud Console, in the left menu, click **Uptime checks**, and then click **Create Uptime Check**.



1. Set the following fields:

**Title**: Lamp Uptime Check, then click **Next**.

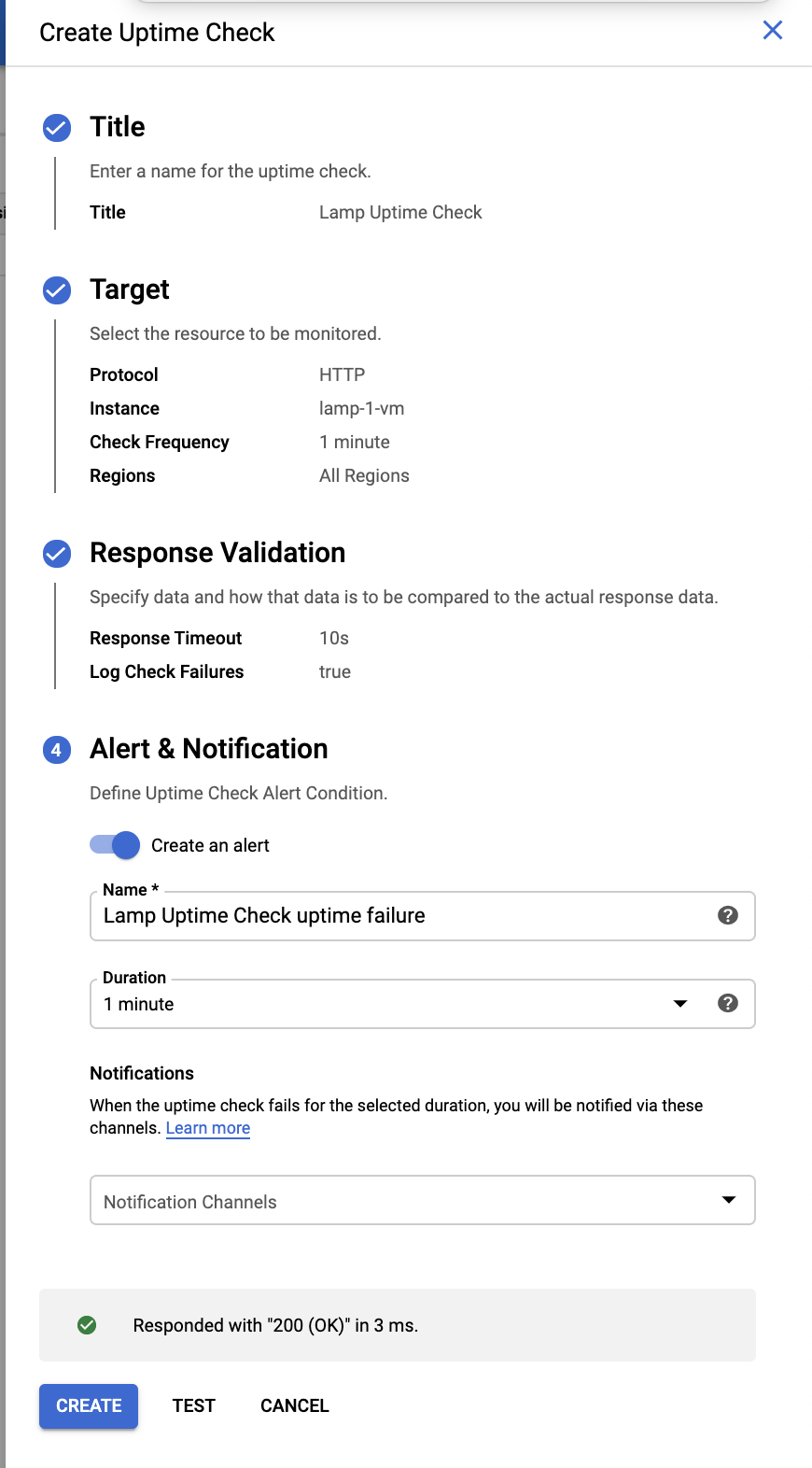
**Protocol**: HTTP

**Resource Type**: Instance

**Applies to**: Single, lamp-1-vm

**Path**: leave at default

**Check Frequency**: 1 min



1. Click on **Next** to leave the other details to default and click **Test** to verify that your uptime check can connect to the resource.
2. When you see a green check mark everything can connect. Click **Create**.

The uptime check you configured takes a while for it to become active. Continue with the lab, you'll check for results later. While you wait, create an alerting policy for a different resource.

**Create an alerting policy**

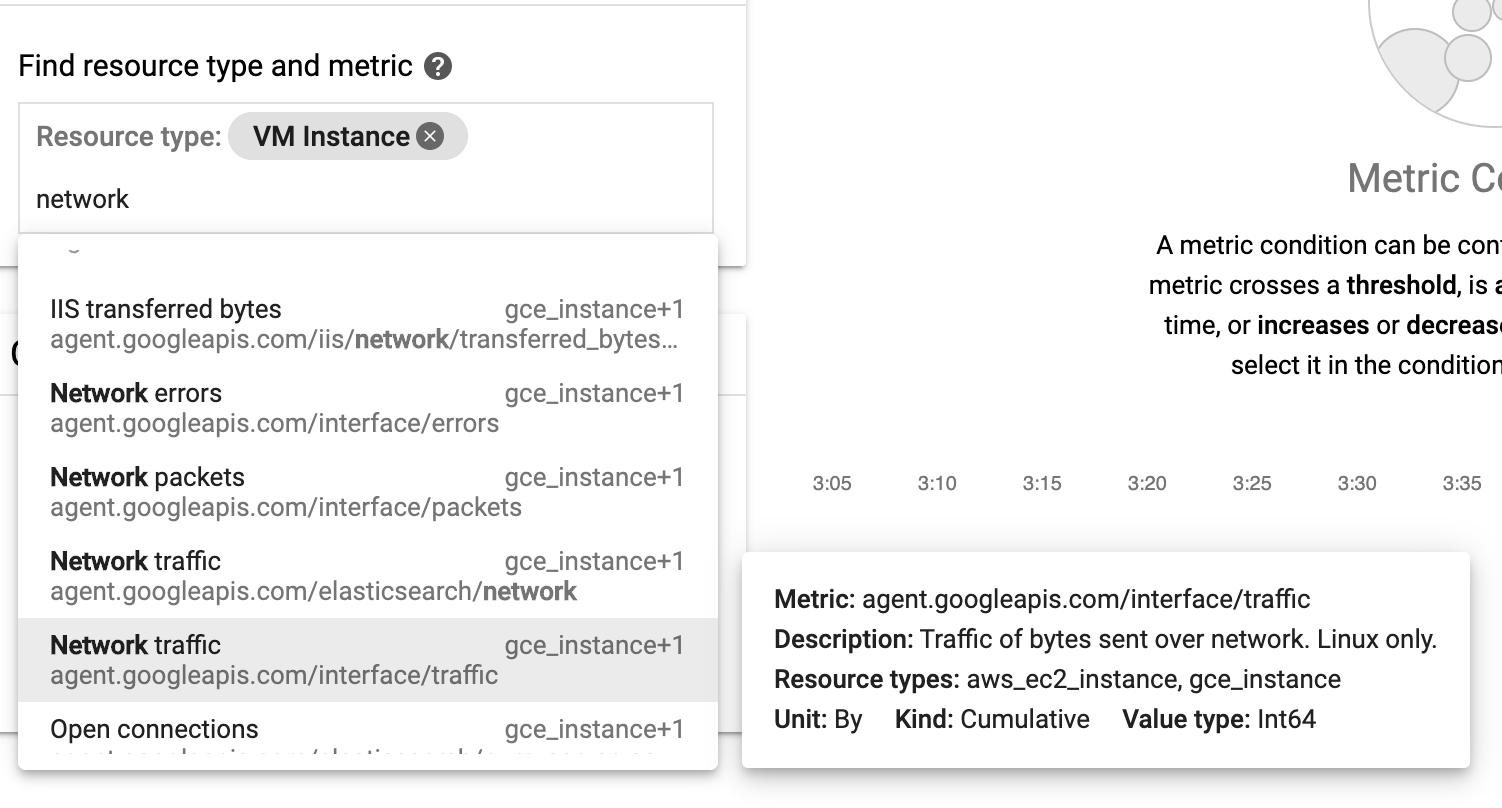
Use Cloud Monitoring to create one or more alerting policies.

1. In the left menu, click **Alerting**, and then click **Create Policy**.
2. Click **Add Condition**.

Set the following in the panel that opens, leave all other fields at the default value.

**Target**: Start typing "VM" in the resource type and metric field, and then select:

* **Resource Type**: VM Instance (gce\_instance)
* **Metric**: Type "network", and then select Network traffic (gce\_instance+1). Be sure to choose the Network traffic resource with agent.googleapis.com/interface/traffic:

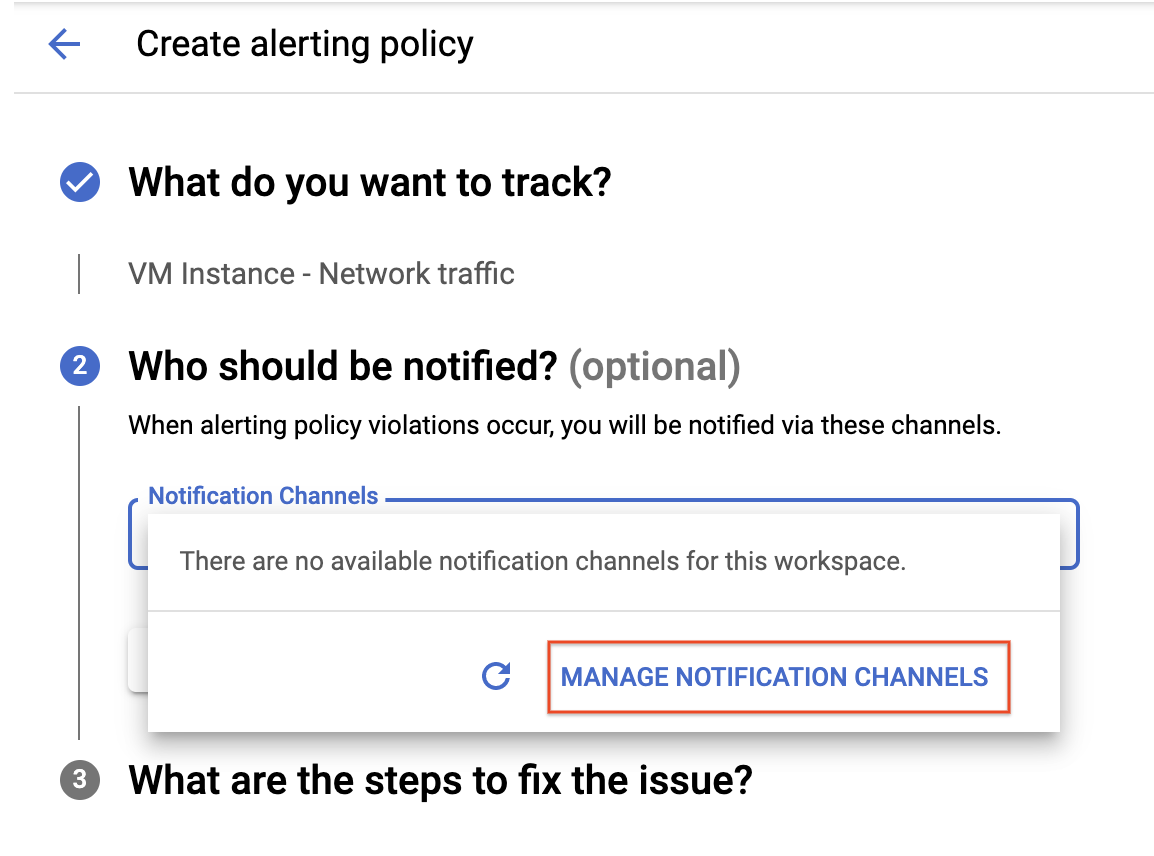


**Configuration**

* **Condition**: is above
* **Threshold**: 500
* **For**: 1 minute

Click **Add**.

1. Click on **Next**.
2. Click on drop down arrow next to **Notification Channels**, then click on **Manage Notification Channels**.

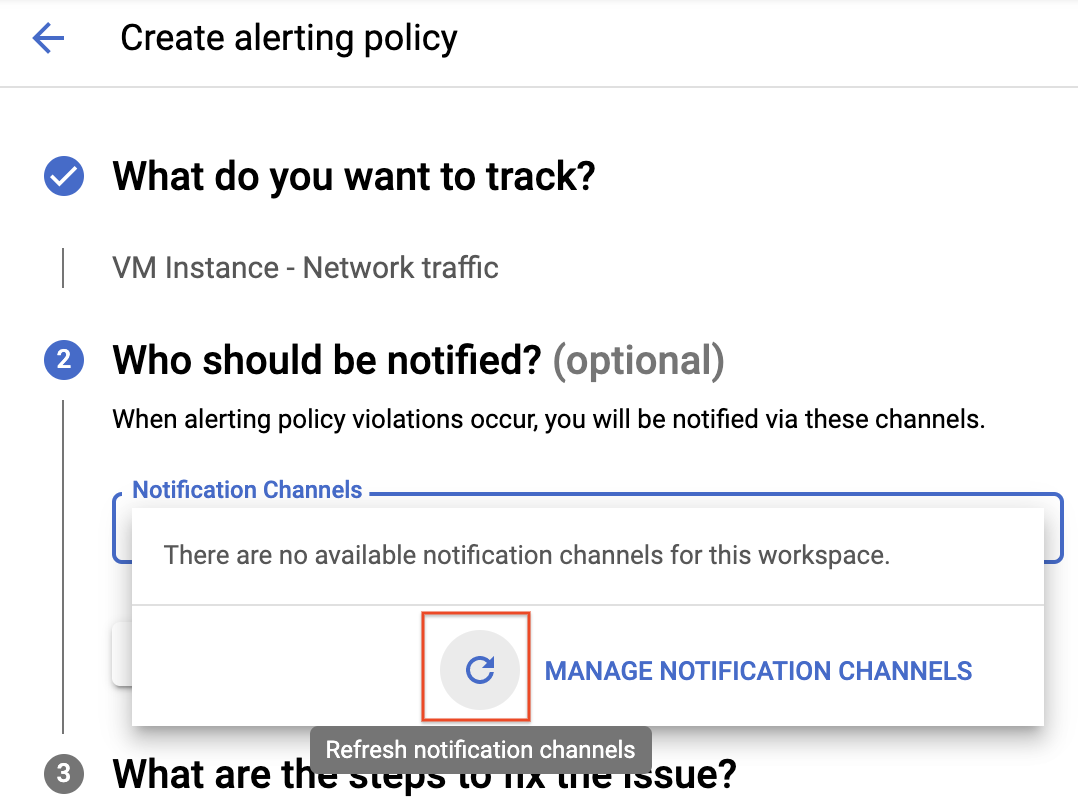


A **Notification channels** page will open in new tab.

1. Scroll down the page and click on **ADD NEW** for **Email**.



1. In **Create Email Channel** dialog box, enter your personal email address in the **Email Address** field and a **Display name**.
2. Click on **Save**.
3. Go back to the previous **Create alerting policy** tab.
4. Click on **Notification Channels** again, then click on the **Refresh icon** to get the display name you mentioned in the previous step.



1. Now, select your **Display name** and click **OK**.
2. Click **Next**.
3. Mention the **Alert name** as Inbound Traffic Alert.
4. Add a message in documentation, which will be included in the emailed alert.
5. Click on **Save**.

You've created an alert! While you wait for the system to trigger an alert, create a dashboard and chart, and then check out Cloud Logging.

Click **Check my progress** below. A green check confirms you're on track.

Create an uptime check and alerting policy

Check my progress

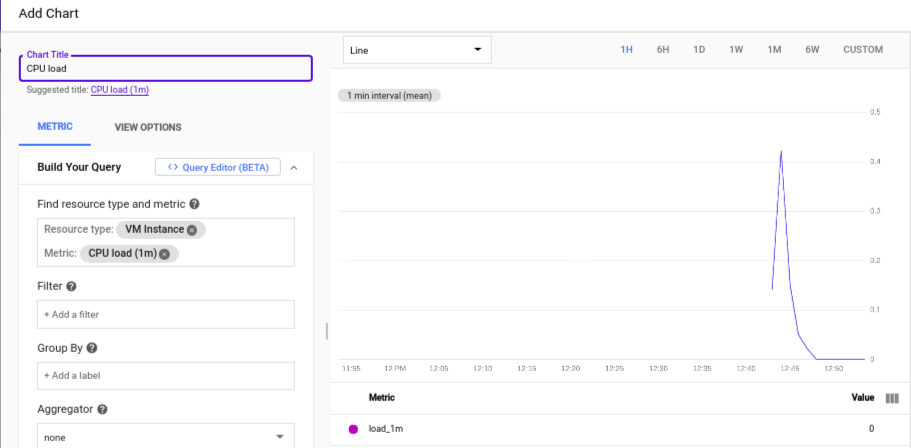
**Create a dashboard and chart**

You can display the metrics collected by Cloud Monitoring in your own charts and dashboards. In this section you create the charts for the lab metrics and a custom dashboard.

1. In the left menu select **Dashboards**, and then **Create Dashboard**.
2. Name the dashboard "Cloud Monitoring LAMP Qwik Start Dashboard", and then click **Confirm**.

Add the first chart

1. Click **Add Chart** in the top right of the screen.
2. Name the chart "CPU Load".
3. Click into the **Find resource type and metric** field and start typing "CPU load", then select CPU Load (1m).
4. Set the resource type to "VM Instance".



1. Click **Save**.

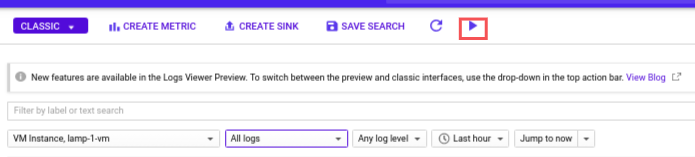
Add the second chart

1. Select **Add Chart** in the top right.
2. Name this chart "Received Packets".
3. Click into the **Find resource type and metric** field and start typing "Received packets", then select Received packets (gce\_instance).
4. Set the resource type to "VM Instance".
5. Leave the other fields at their default values. You see the chart data in the Preview section.
6. Click **Save**.

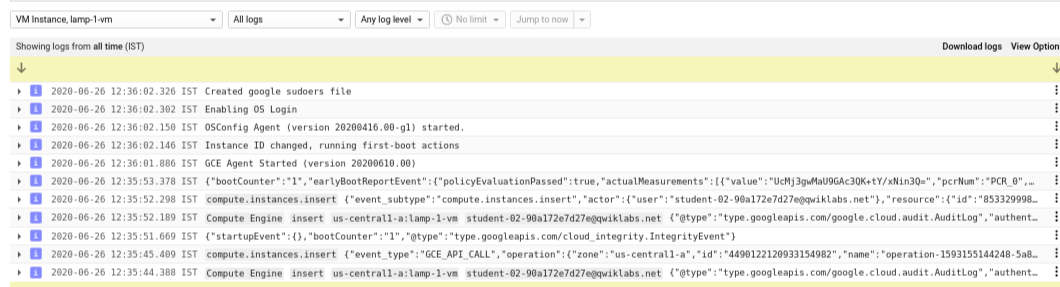
**View your logs**

Cloud Monitoring and Cloud Logging are closely integrated. Check out the logs for your lab.

1. Select **Navigation menu** > **Logging** > **Logs Explorer**.
2. Click on the **OPTIONS** drop down and select **Go back to the Legacy Logs Viewer**.
3. Select the logs you want to see, in this case, you select the logs for the lamp-1-vm instance you created at the start of this lab:

* Select **VM Instance** > **lamp-1-vm** in the Audited Resource (first) drop-down menu.
* Leave the other fields with their default values.
* Click the **Start streaming logs** icon. 

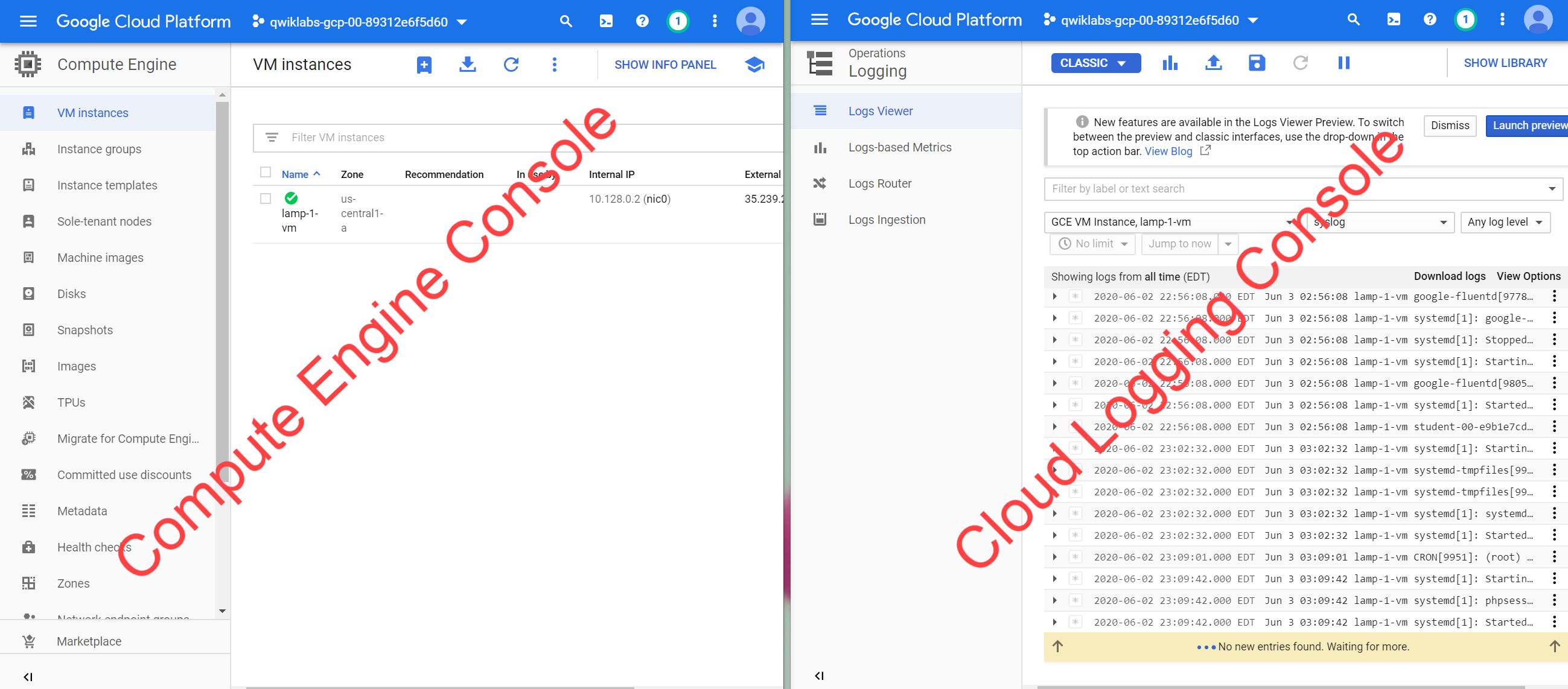
You see the logs for your VM instance:



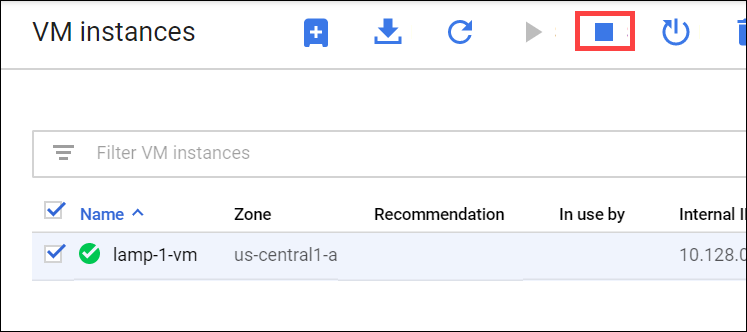
Check out what happens when you start and stop the VM instance.

To best see how Cloud Monitoring and Cloud Logging reflect VM instance changes, make changes to your instance in one browser window and then see what happens in the Cloud Monitoring, and then Cloud Logging windows.

1. Open the Compute Engine window in a new browser window. Select **Navigation menu** > **Compute Engine**, right-click **VM instances** > **Open link in new window**.
2. Move the Logs Viewer browser window next to the Compute Engine window. This makes it easier to view how changes to the VM are reflected in the logs.



1. In the Compute Engine window, select the lamp-1-vm instance, click **Stop** at the top of the screen, and then confirm to stop the instance.



It takes a few minutes for the instance to stop.

1. Watch in the Logs View tab for when the VM is stopped.
2. In the VM instance details window, click **Start** at the top of the screen, and then confirm. It will take a few minutes for the instance to re-start. Watch the log messages to monitor the start up.

**Check the uptime check results and triggered alerts**

1. In the Cloud Logging window, select **Navigation menu** > **Monitoring** > **Uptime checks**. This view provides a list of all active uptime checks, and the status of each in different locations.

You will see Lamp Uptime Check listed. Since you have just restarted your instance, the regions are in a failed status. It may take up to 5 minutes for the regions to become active. Reload your browser window as necessary until the regions are active.

1. Click the name of the uptime check, Lamp Uptime Check.

Since you have just restarted your instance, it may take some minutes for the regions to become active. Reload your browser window as necessary.

Check if alerts have been triggered

1. In the left menu, click **Alerting**.
2. You see incidents and events listed in the Alerting window.
3. Check your email account. You should see Cloud Monitoring Alerts.

**Note:** Remove the email notification from your alerting policy. The resources for the lab may be active for a while after the completion, and this may result in a few more email notifications getting sent out.