Cloud Monitoring: Qwik Start

Activate Cloud Shell

Cloud Shell is a virtual machine that is loaded with development tools. It offers a persistent 5GB home directory and runs on the Google Cloud. Cloud Shell provides command-line access to your Google Cloud resources.

1. Click **Activate Cloud Shell** at the top of the Google Cloud console.

2. Click through the following windows:

   - Continue through the Cloud Shell information window.
   - Authorize Cloud Shell to use your credentials to make Google Cloud API calls.

When you are connected, you are already authenticated, and the project is set to your **Project_ID**, `qwiklabs-gcp-02-972df1b473f9`. The output contains a line that declares the **Project_ID** for this session:

```
Your Cloud Platform project in this session is set to qwiklabs-gcp-02-
972df1b473f9
```

`gcloud` is the command-line tool for Google Cloud. It comes pre-installed on Cloud Shell and supports tab-completion.

3. (Optional) You can list the active account name with this command:

```
gcloud auth list
```

Copied!

content_copy

4. Click **Authorize**.

Output:

```
ACTIVE: *
ACCOUNT: student-01-744e2e3fa309@qwiklabs.net

To set the active account, run:
    $ gcloud config set account `ACCOUNT`
```

5. (Optional) You can list the project ID with this command:

```
gcloud config list project
```

Copied!

content_copy

Output:

```
[core]
project = qwiklabs-gcp-02-972df1b473f9
```

Set your region and zone

Certain Compute Engine resources live in regions and zones. A region is a specific geographical location where you can run your resources. Each region has one or more zones.

Note: Learn more about regions and zones and see a complete list in Regions & Zones documentation.

Run the following gcloud commands in Cloud Shell to set the default region and zone for your lab:

```
gcloud config set compute/zone "us-east4-a"
export ZONE=$(gcloud config get compute/zone)

gcloud config set compute/region "us-east4"
export REGION=$(gcloud config get compute/region)
```

Copied!

content_copy

Task 1. Create a Compute Engine instance

1. In the **Cloud console**, on the **Navigation menu** (☰), click **Compute Engine** > **VM Instances**, then click **Create instance**.

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

2. In the **Machine configuration**

   Enter the values for the following fields:

Field	**Value**
Name	`lamp-1-vm`
Region	`us-east4`
Zone	`us-east4-a`
Series	`E2`
Machine	`e2-medium`

3. Click **OS and storage**

   Select Boot Disk:

   - **Boot Disk**: Debian GNU/Linux 12 (bookworm)
4. Click **Networking**

   Select the values for Firewall:

   - **Firewall**: Allow HTTP traffic
5. Once all sections are configured, scroll down and click **Create** to launch your new virtual machine instance.

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

Task 2. Add Apache2 HTTP Server to your instance

1. In the Console, click **SSH** in line with `lamp-1-vm` to open a terminal to your instance.

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

```
sudo apt-get update
```

Copied!

content_copy

```
sudo apt-get install apache2 php7.0
```

Copied!

content_copy

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

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

```
sudo service apache2 restart
```

Copied!

content_copy

4. 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.

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.

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 collected-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. On the Google Cloud, Operations website, see Cloud Monitoring Documentation 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.

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

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-google-cloud-ops-agent-repo.sh
```

Copied!

content_copy

```
sudo bash add-google-cloud-ops-agent-repo.sh --also-install
```

Copied!

content_copy

2. If asked if you want to continue, press **Y**.

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

```
sudo systemctl status google-cloud-ops-agent"*"
```

Copied!

content_copy

Press **q** to exit the status.

```
sudo apt-get update
```

Copied!

content_copy

Task 3. 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**.

2. For **Protocol**, select **HTTP**.

3. For **Resource Type**, select **Instance**.

4. For **Instance**, select **lamp-1-vm**.

5. For **Check Frequency**, select **1 minute**.

6. Click **Continue**.

7. In Response Validation, accept the defaults and then click **Continue**.

8. In Alert & Notification, accept the defaults, and then click **Continue**.

9. For Title, type **Lamp Uptime Check**.

10. Click **Test** to verify that your uptime check can connect to the resource.

    When you see a green check mark everything can connect.

11. 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.

Task 4. 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 on **Select a metric** dropdown. Uncheck the **Active**.
3. Type **Network traffic** in filter by resource and metric name and click on **VM instance > Interface**. Select `Network traffic` (agent.googleapis.com/interface/traffic) and click **Apply**. Leave all other fields at the default value.
4. Click **Next**.
5. Set the **Threshold position** to `Above threshold`, **Threshold value** to `500` and **Advanced Options > Retest window** to `1 min`. Click **Next**.
6. Click on the drop down arrow next to **Notification Channels**, then click on **Manage Notification Channels**.

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

7. Scroll down the page and click on **ADD NEW** for **Email**.
8. In the **Create Email Channel** dialog box, enter your personal email address in the **Email Address** field and a **Display name**.
9. Click on **Save**.
10. Go back to the previous **Create alerting policy** tab.
11. Click on **Notification Channels** again, then click on the **Refresh icon** to get the display name you mentioned in the previous step.
12. Click on **Notification Channels** again if necessary, select your **Display name** and click **OK**.
13. Add a message in documentation, which will be included in the emailed alert.
14. Mention the **Alert name** as `Inbound Traffic Alert`.
15. Click **Next**.

16. Review the alert and click **Create Policy**.

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.

Task 5. 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 Custom Dashboard**.
2. Name the dashboard `Cloud Monitoring LAMP Qwik Start Dashboard`.

Add the first chart

1. Click on **+ ADD WIDGET**
2. Select the **Line** option under **Visualization** in the **Add widget**.
3. Name the Widget title **CPU Load**.
4. Click on **Select a metric** dropdown. Uncheck the **Active**.
5. Type **CPU load (1m)** in filter by resource and metric name and click on **VM instance > Cpu**. Select `CPU load (1m)` and click **Apply**. Leave all other fields at the default value. Refresh the tab to view the graph.

Add the second chart

1. Click **+ Add WIDGET** and select **Line** option under **Visualization** in the **Add widget**.

2. Name this Widget title **Received Packets**.

3. Click on **Select a metric** dropdown. Uncheck the **Active**.

4. Type **Received packets** in filter by resource and metric name and click on **VM instance > Instance**. Select `Received packets` and click **Apply**. Refresh the tab to view the graph.

5. Leave the other fields at their default values. You see the chart data.

Task 6. 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. 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:

   - Click on **All Resource**.

   - Select **VM Instance** > **lamp-1-vm** in the Resource drop-down menu.

   - Click **Apply**.

In the results section you can 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

3. In the Compute Engine window, select the `lamp-1-vm` instance, click the three vertical dots at the right of the screen and then click **Stop**, and then confirm to stop the instance.

   It takes a few minutes for the instance to stop.

4. Watch in the Logs View tab for when the VM is stopped.

5. In the VM instance details window, click the three vertical dots at the right of the screen and then click **Start/resume**, and then confirm. It will take a few minutes for the instance to re-start. Watch the log messages to monitor the start up.

Task 7. 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.

2. 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 you finish, and this may result in a few more email notifications getting sent out.