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.

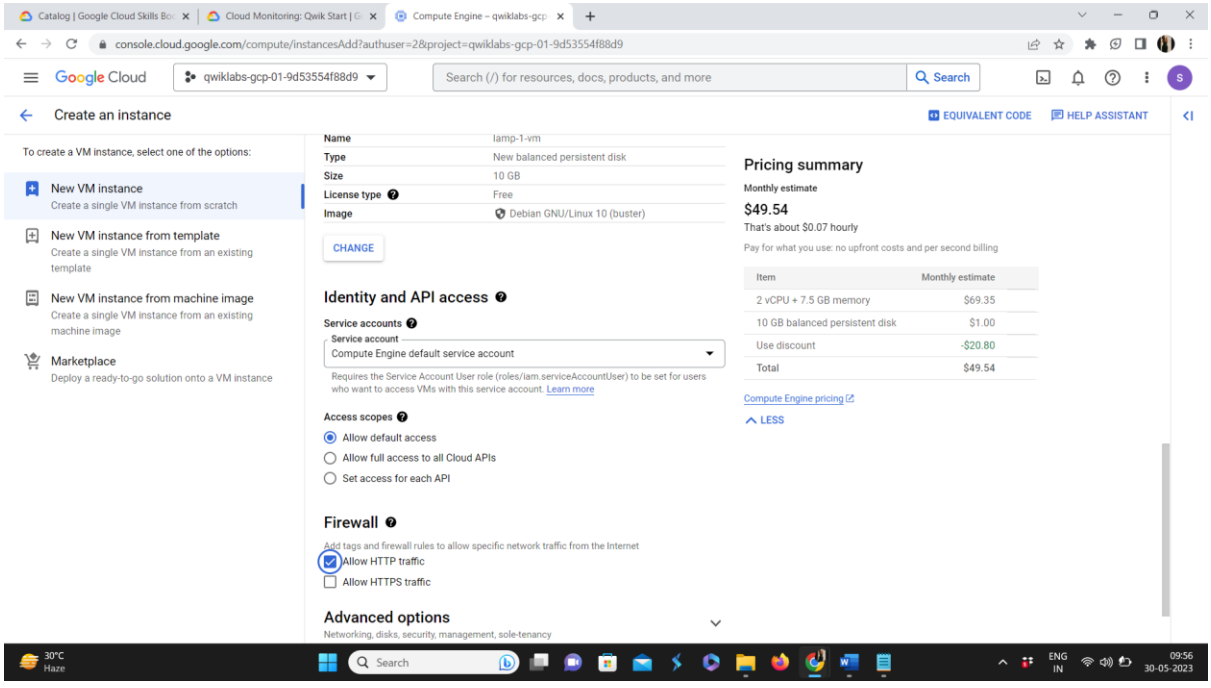
This hands-on lab shows you how to monitor a Compute Engine virtual machine (VM) instance with Cloud Monitoring. You will also install monitoring and logging agents for your VM which collects more information from your instance, which could include metrics and logs from 3rd party apps.

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

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

Field	Value
Name	lamp-1-vm
Region	us-central1
Zone	us-central1-a
Series	N1
Machine type	n1-standard-2
Boot disk	Click Change. Select version Debian GNU/Linux 10 (buster) for Debian OS and click Select.
Firewall	check Allow HTTP traffic

Click Create.



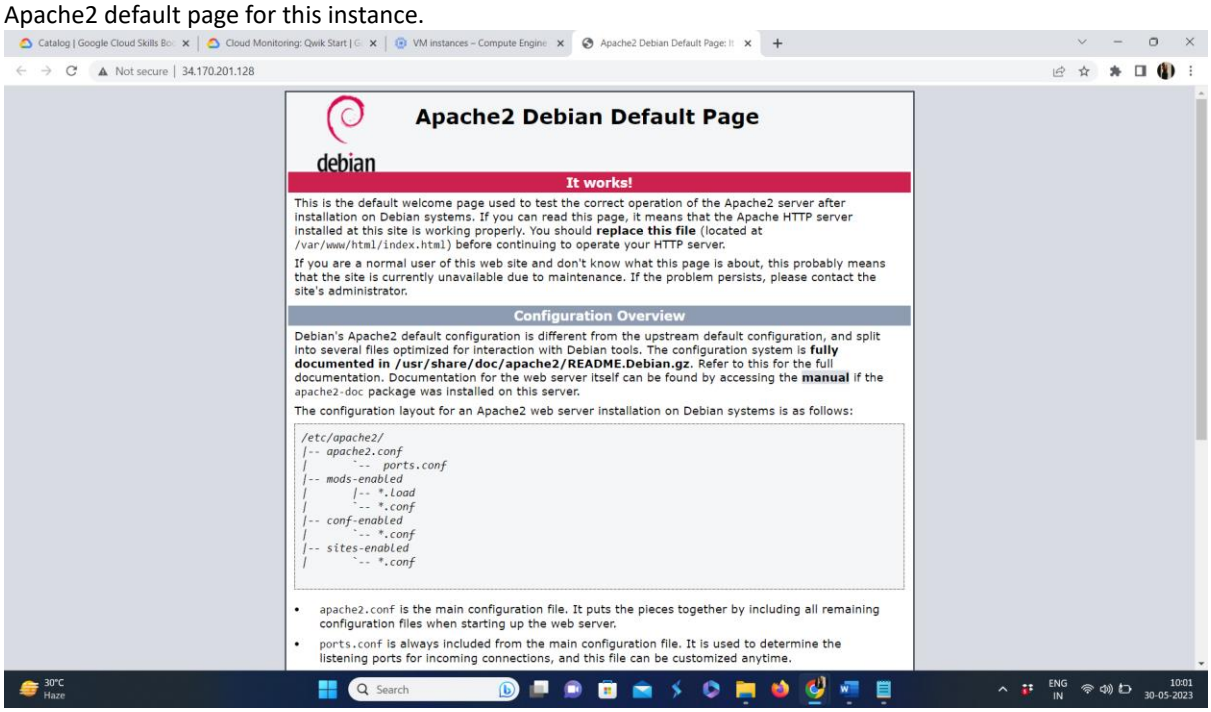
Task 2. Add Apache2 HTTP Server to your instance
In the Console, click SSH in line with lamp-1-vm to open a terminal to your instance.

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
sudo service apache2 restart
```

```
student-00-f19bb2545ade@lamp-1-vm:~$ history
    1  sudo apt-get update
    2  sudo apt-get install apache2 php7.0
    3  sudo service apache2 restart
    4  history
```

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 Navigation menu icon > 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.
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
sudo bash add-google-cloud-ops-agent-repo.sh --also-install

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"*"

sudo apt-get update

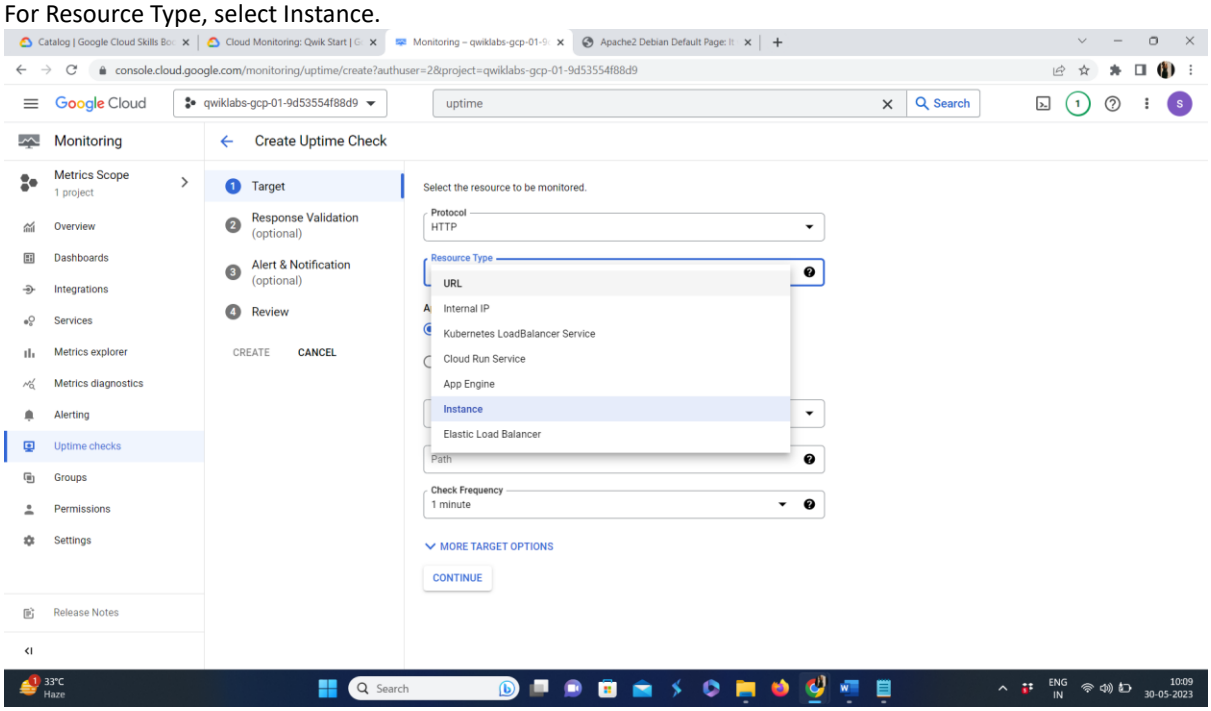
```
Reading package lists... Done
student-00-f19bb2545ade@lamp-1-vm:~$ history
    1  sudo apt-get update
    2  sudo apt-get install apache2 php7.0
    3  sudo service apache2 restart
    4  history
    5  curl -sSO https://dl.google.com/cloudagents/add-google-cloud-ops-agent-repo.sh
    6  sudo bash add-google-cloud-ops-agent-repo.sh --also-install
    7  sudo systemctl status google-cloud-ops-agent"*"
    8  sudo apt-get update
    9  history
student-00-f19bb2545ade@lamp-1-vm:~$
```

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.

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

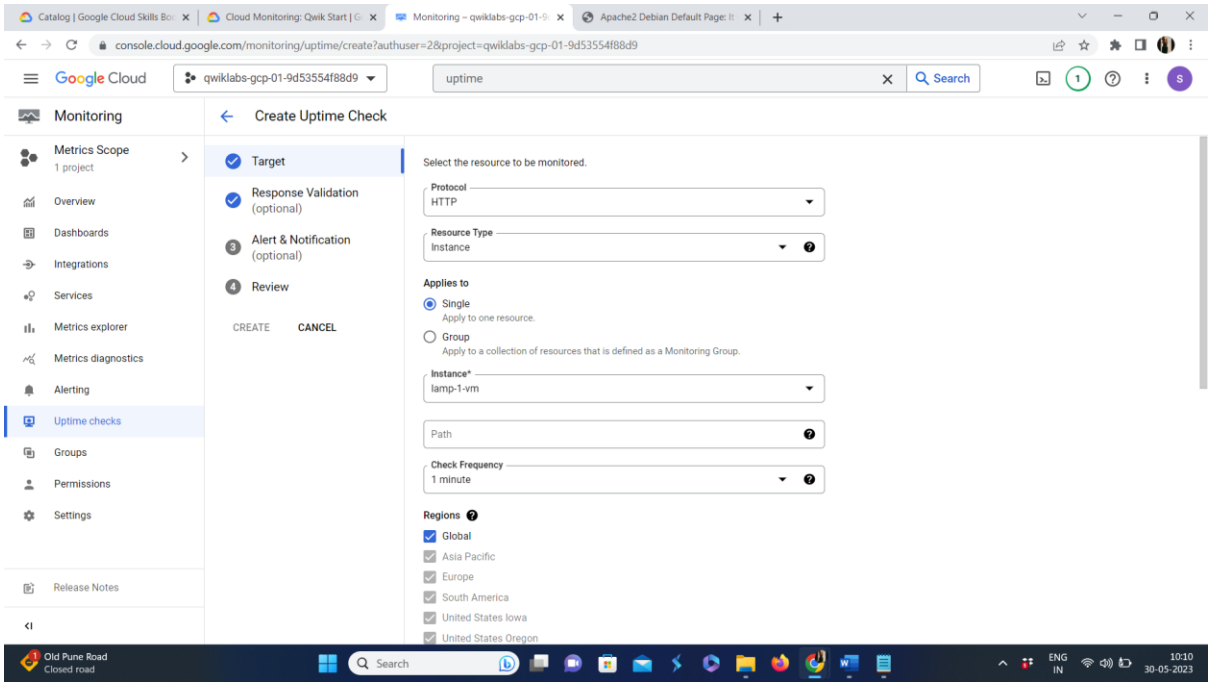
For Protocol, select HTTP.

For Resource Type, select Instance.



For Instance, select lamp-1-vm.

For Check Frequency, select 1 minute.



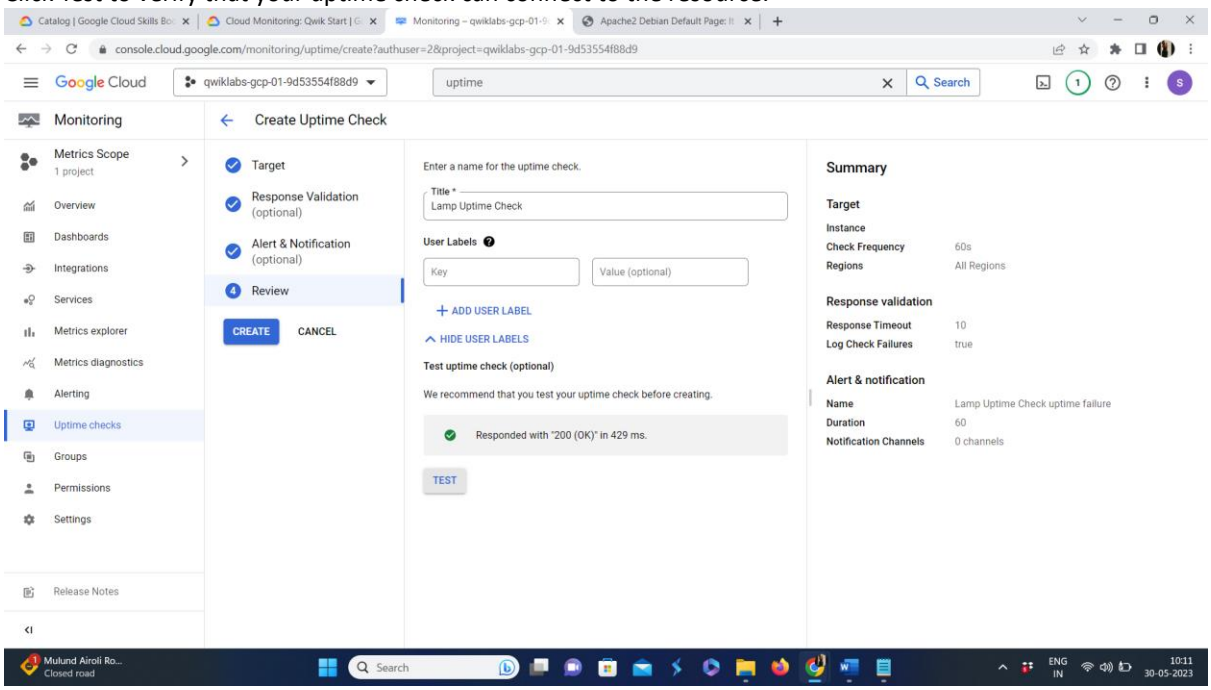
Click Continue.

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

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

For Title, type Lamp Uptime Check.

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



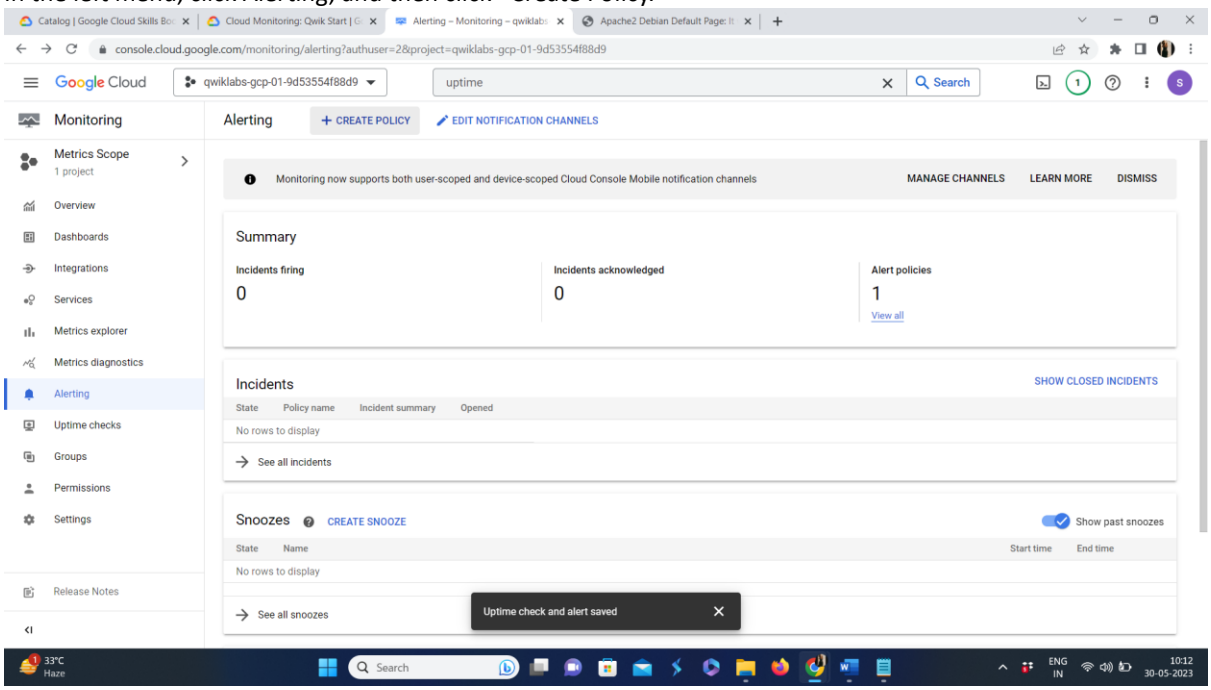
When you see a green check mark everything can connect.

Click Create.

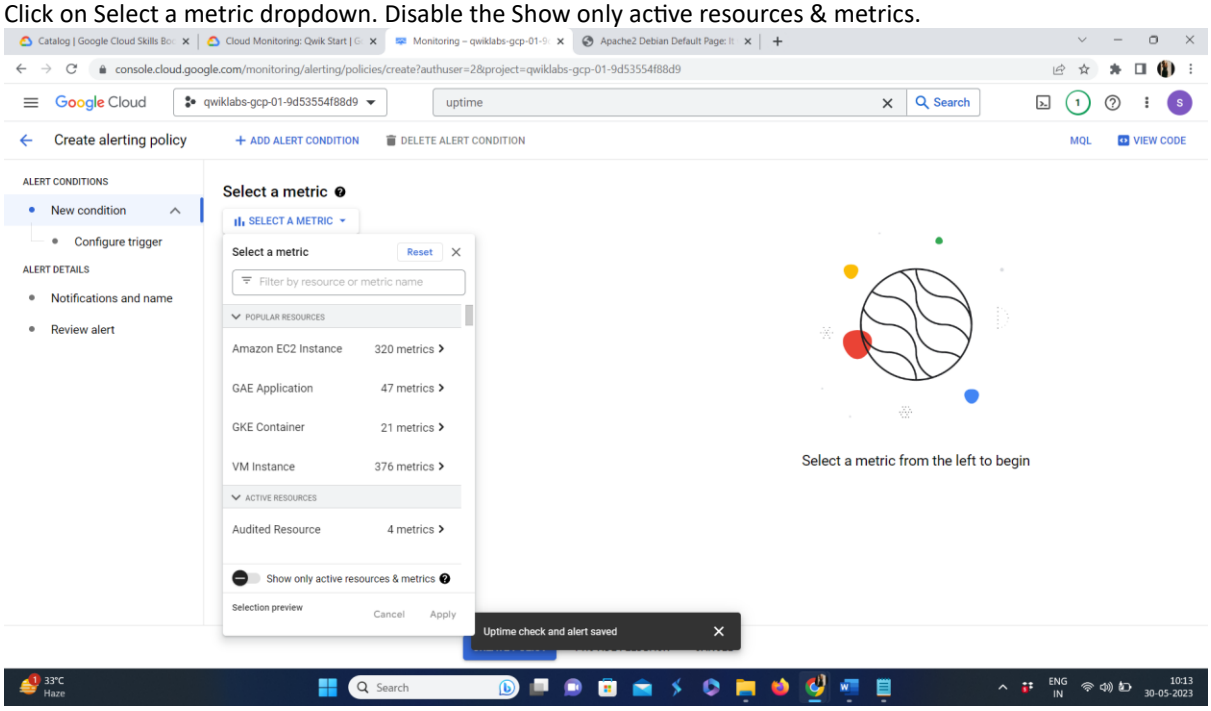
The uptime check you configured takes a while for it to become active. Continue with the lab, you'll check for results later. While you wait, create an alerting policy for a different resource.

Task 4. Create an alerting policy
Use Cloud Monitoring to create one or more alerting policies.

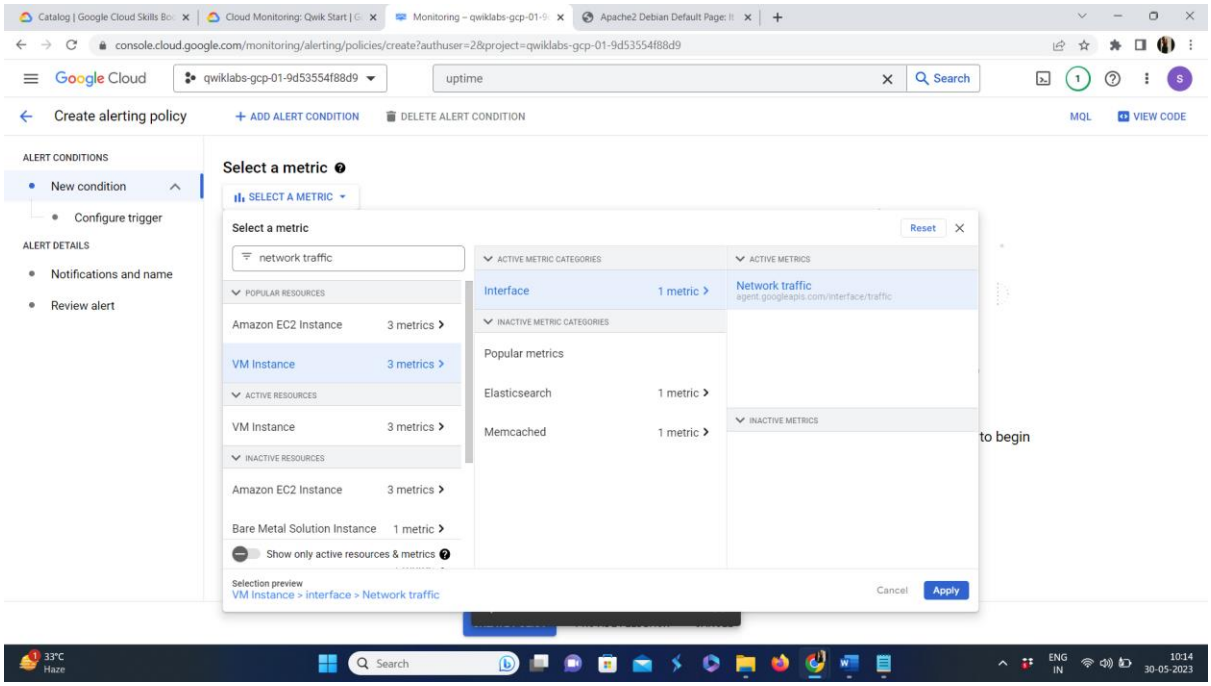
In the left menu, click Alerting, and then click +Create Policy.



Click on Select a metric dropdown. Disable the Show only active resources & metrics.

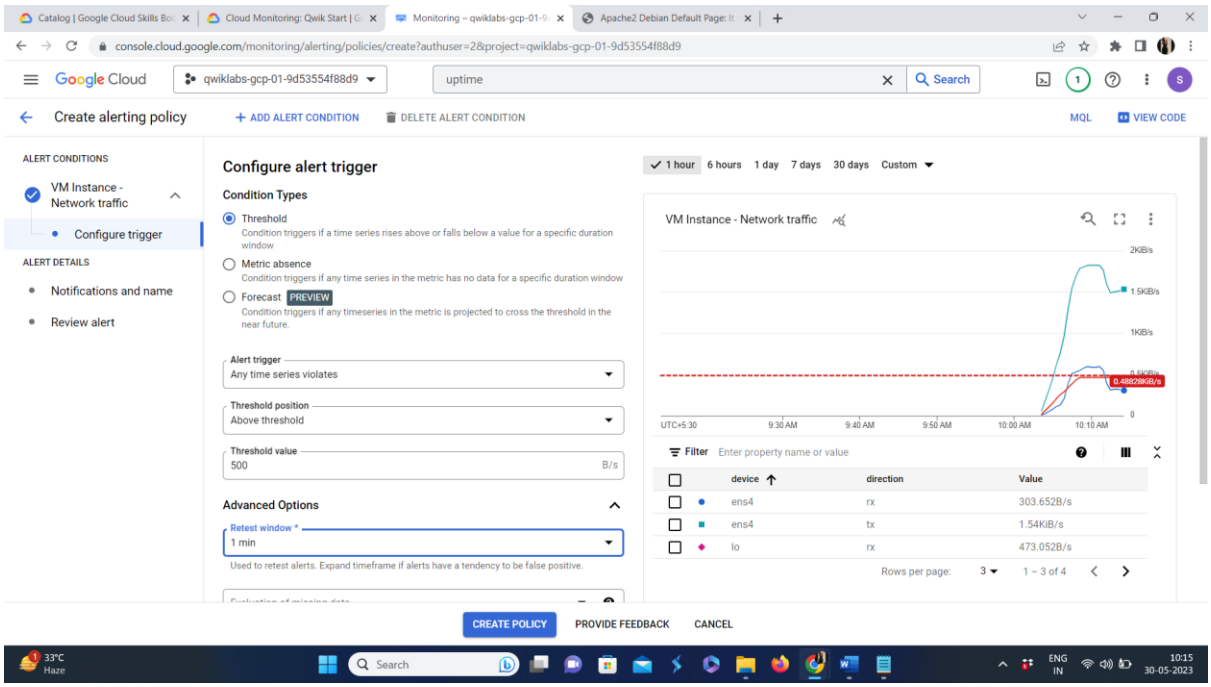


Type Network traffic in filter by resource and metric name and click on VM instance > Interface. Select Network traffic (agent.googleapis.com/interface/traffic) and click Apply. Leave all other fields at the default value.

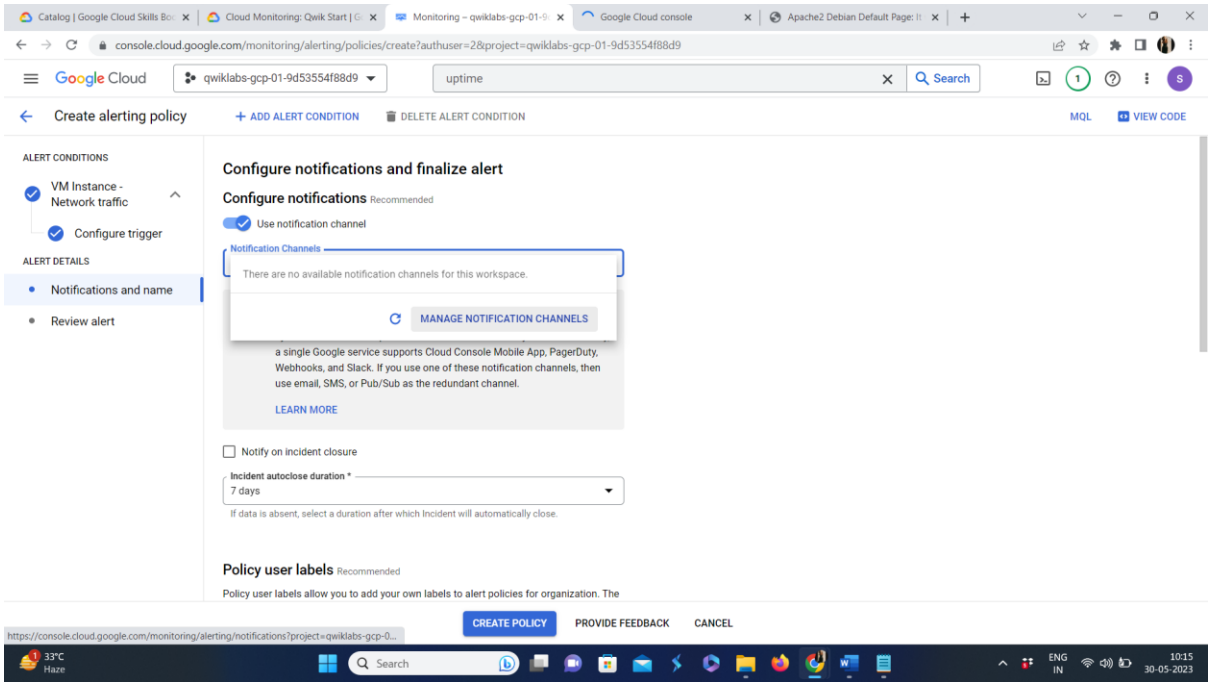


Click Next.

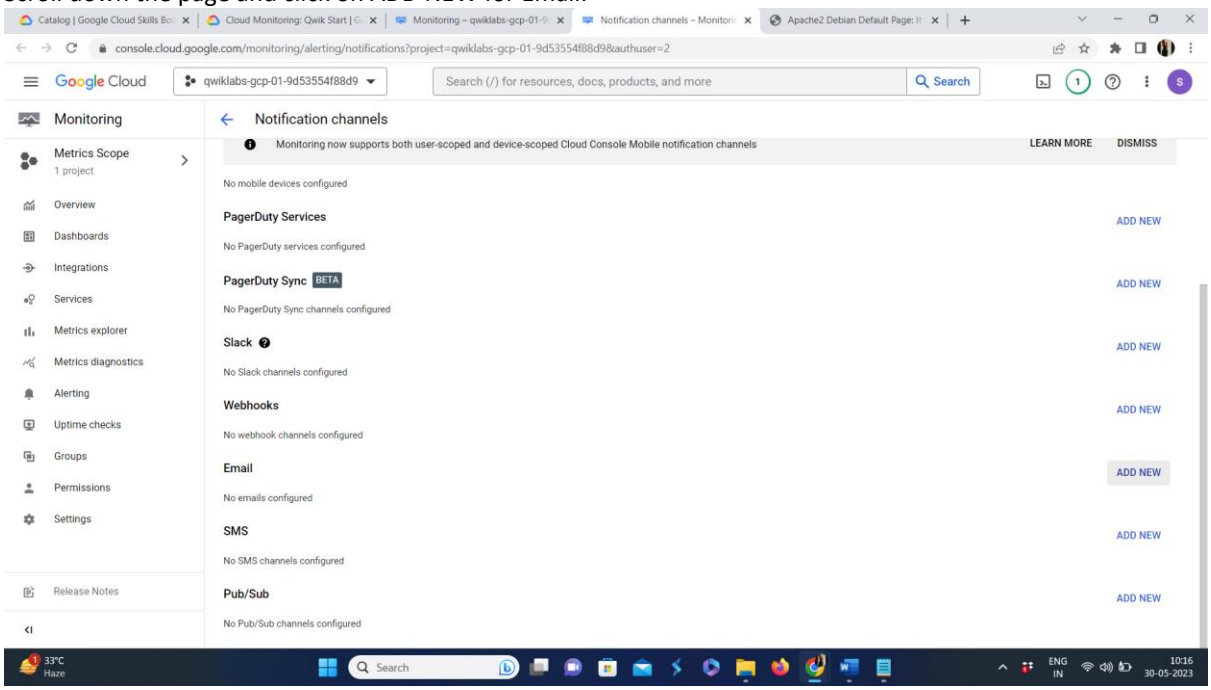
Set the Threshold position to Above threshold, Threshold value to 500 and Advanced Options > Retest window to 1 min. Click Next.



Click on the drop down arrow next to Notification Channels, then click on Manage Notification Channels.

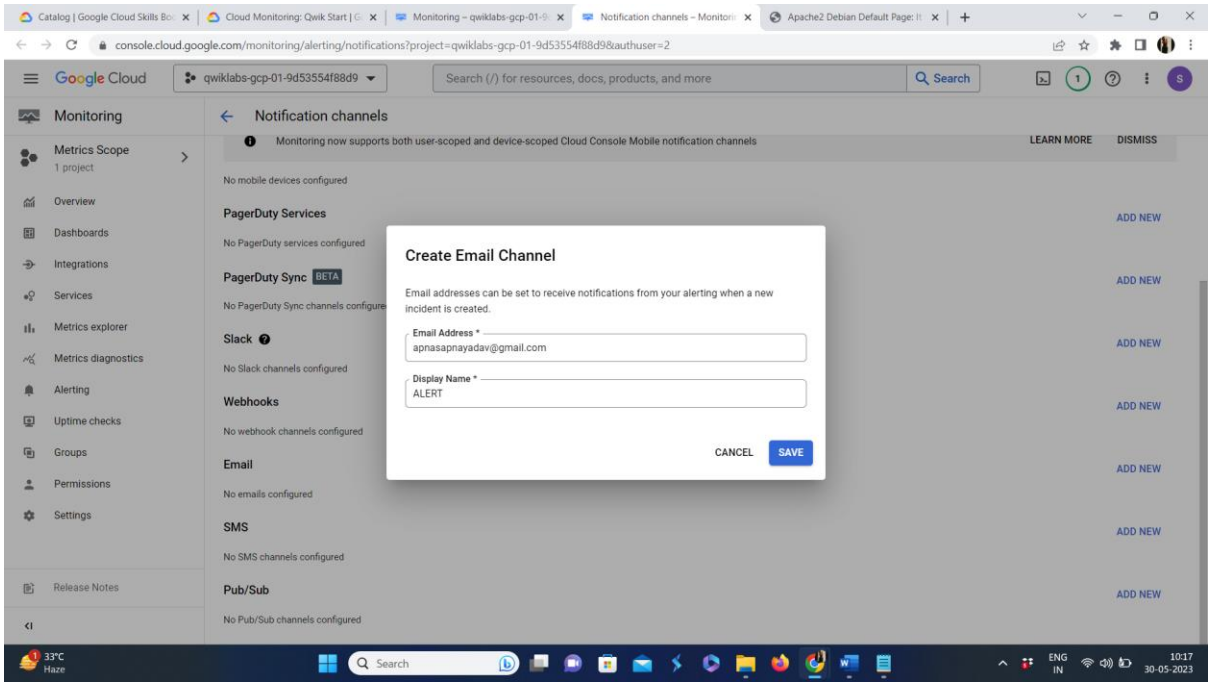


Notification channels page will open in a new tab.
Scroll down the page and click on ADD NEW for Email.



In the Create Email Channel dialog box, enter your personal email address in the Email Address field and a Display name.

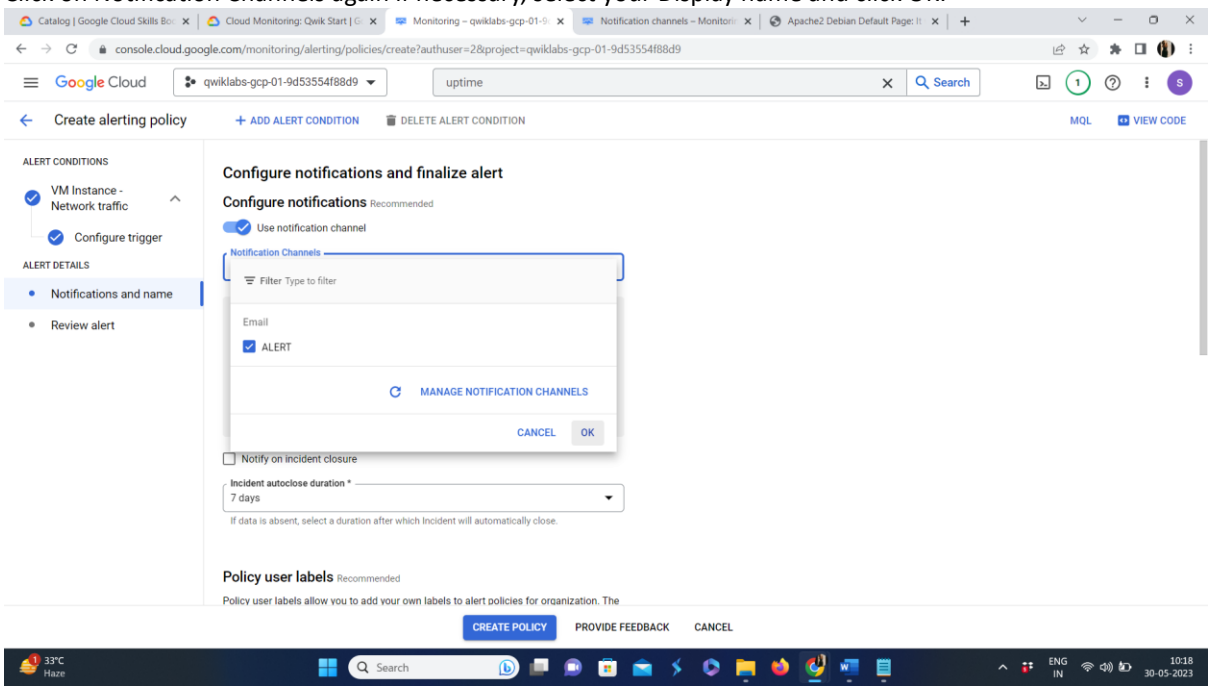
Click on Save.



Go back to the previous Create alerting policy tab.

Click on Notification Channels again, then click on the Refresh icon to get the display name you mentioned in the previous step.

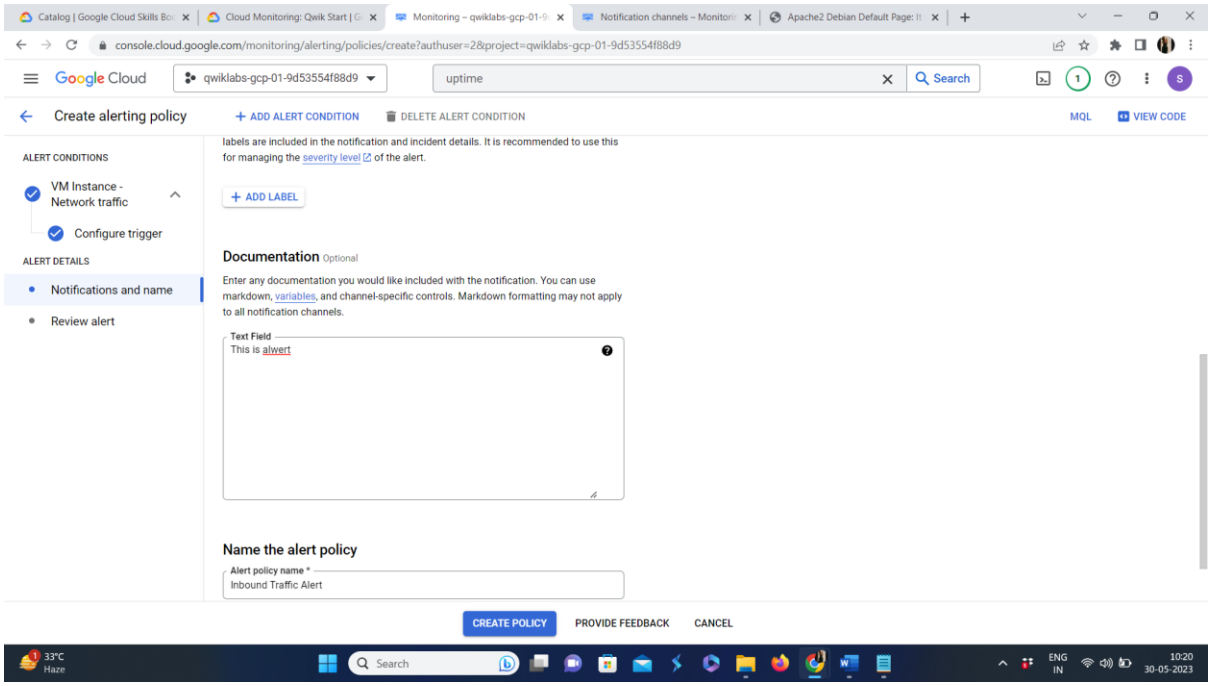
Click on Notification Channels again if necessary, select your Display name and click OK.



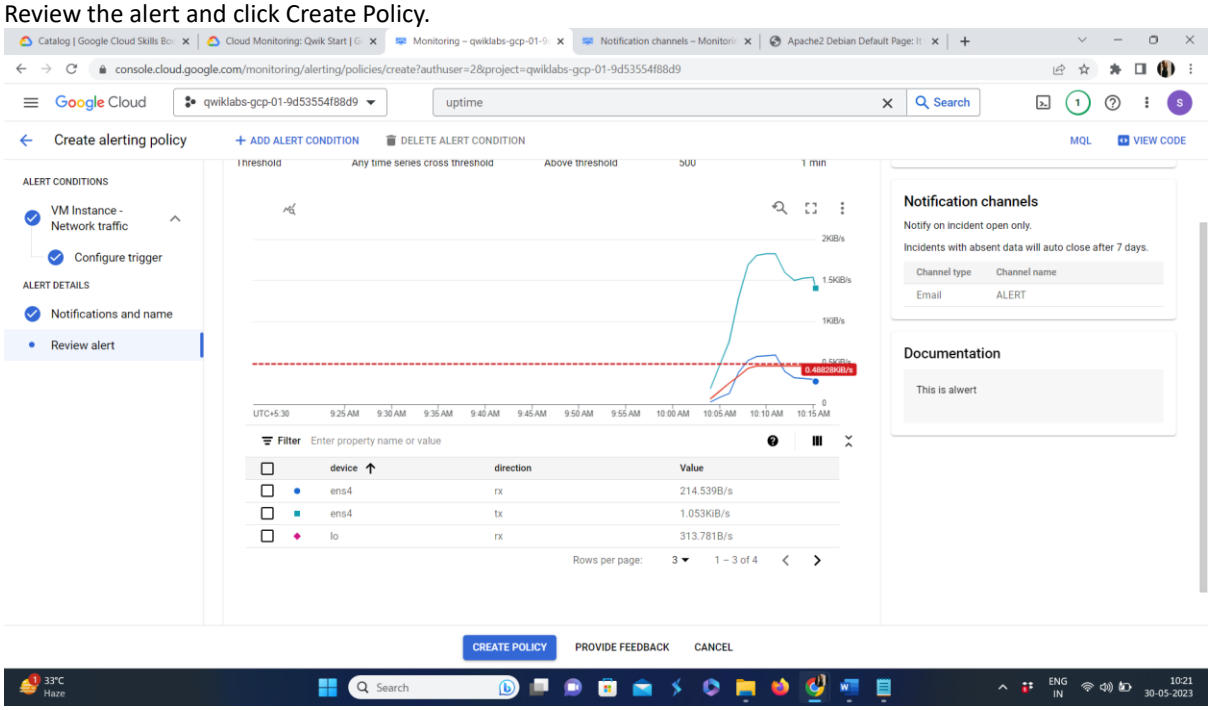
Add a message in documentation, which will be included in the emailed alert.

Mention the Alert name as Inbound Traffic Alert.

Click Next.



Review the alert and click Create Policy.

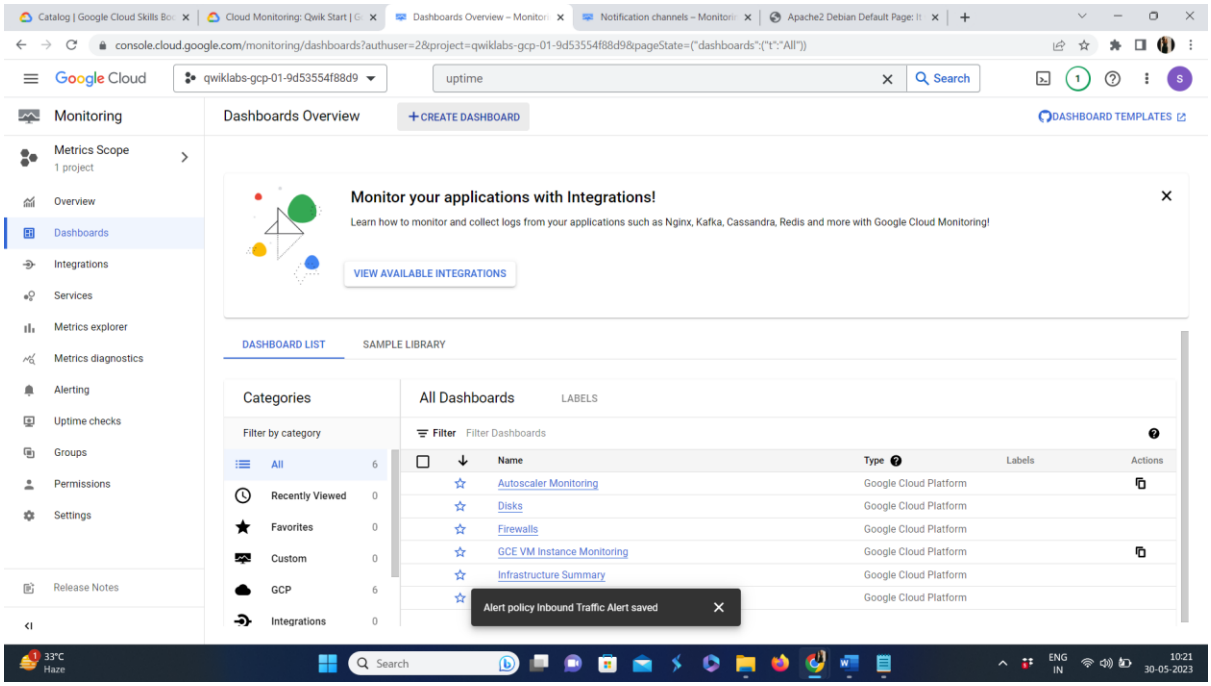


You've created an alert! While you wait for the system to trigger an alert, create a dashboard and chart, and then check out Cloud Logging.

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.

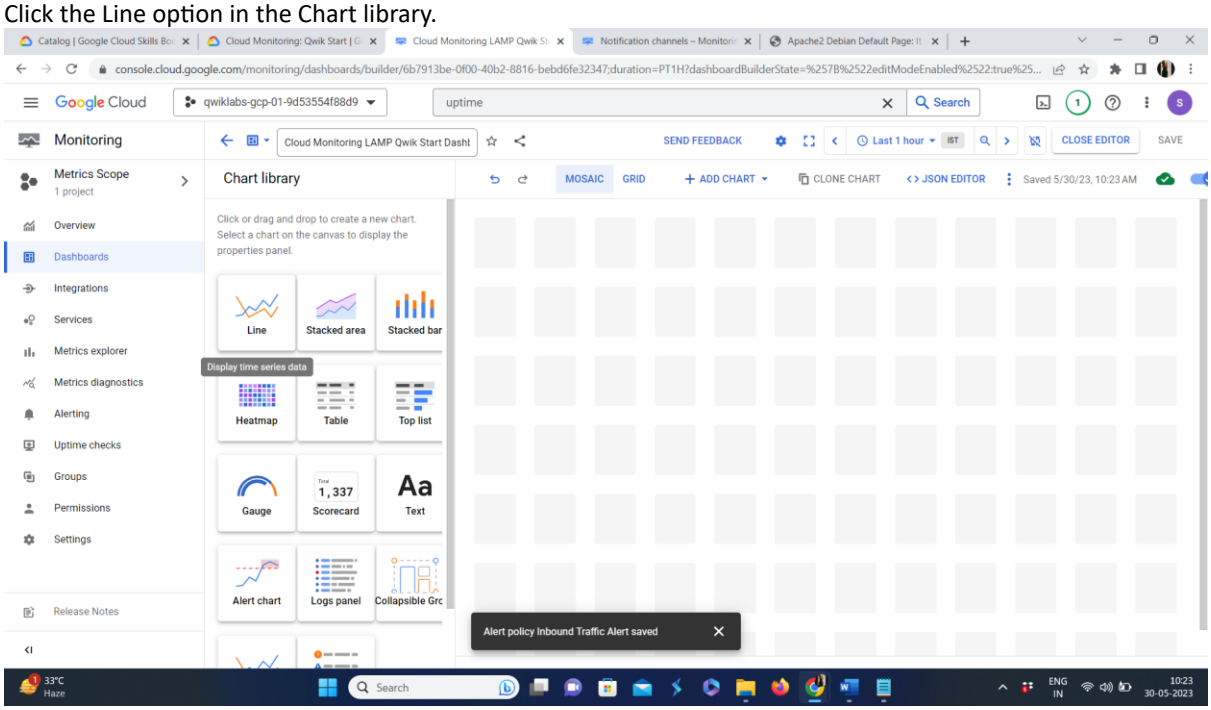
In the left menu select Dashboards, and then +Create Dashboard.



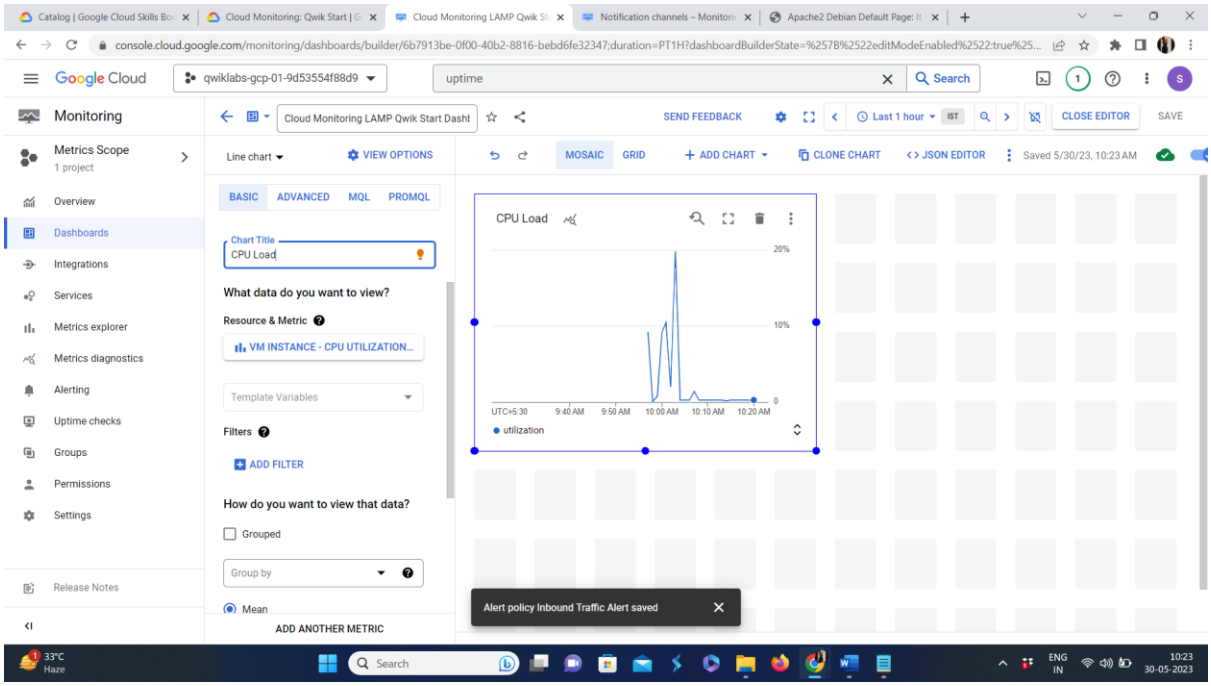
Name the dashboard Cloud Monitoring LAMP Qwik Start Dashboard.

Add the first chart

Click the Line option in the Chart library.

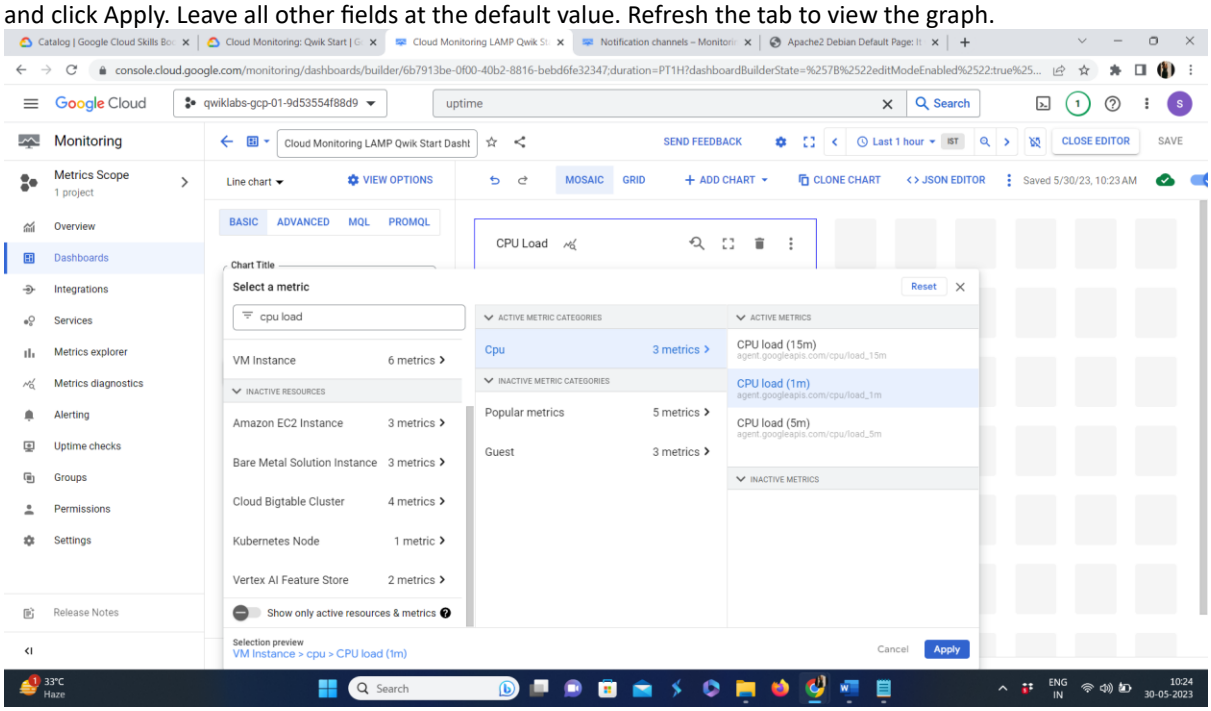


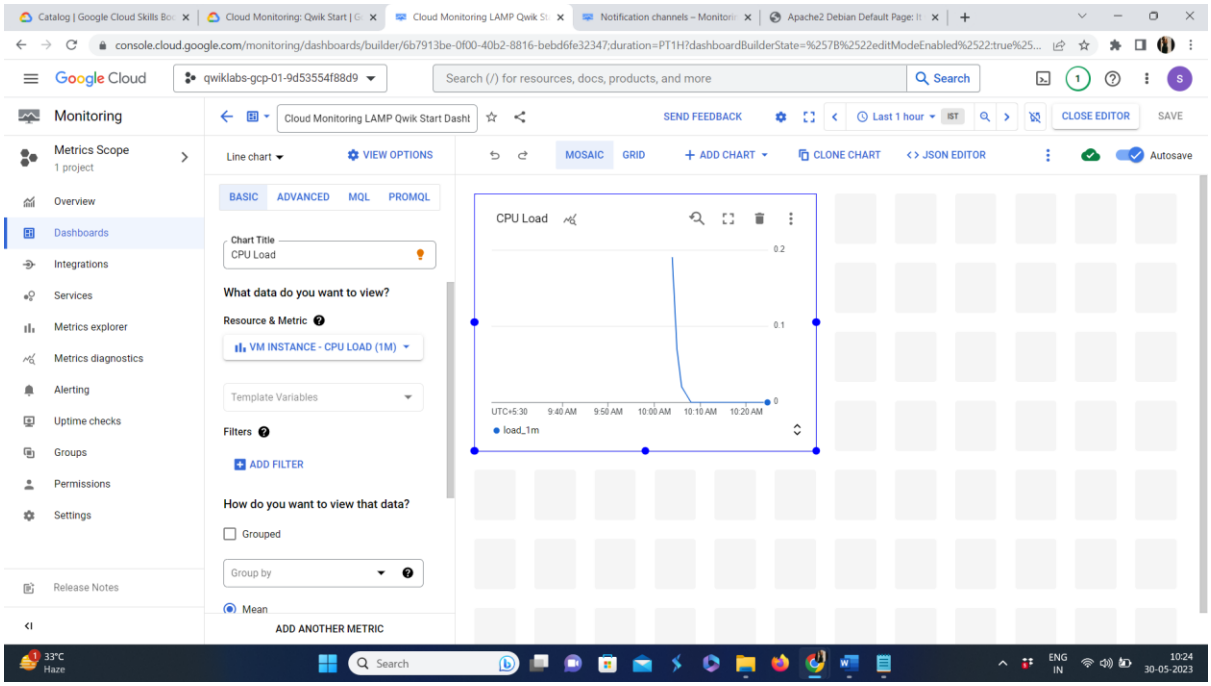
Name the chart title CPU Load.



Click on Resource & Metric dropdown. Disable the Show only active resources & metrics.

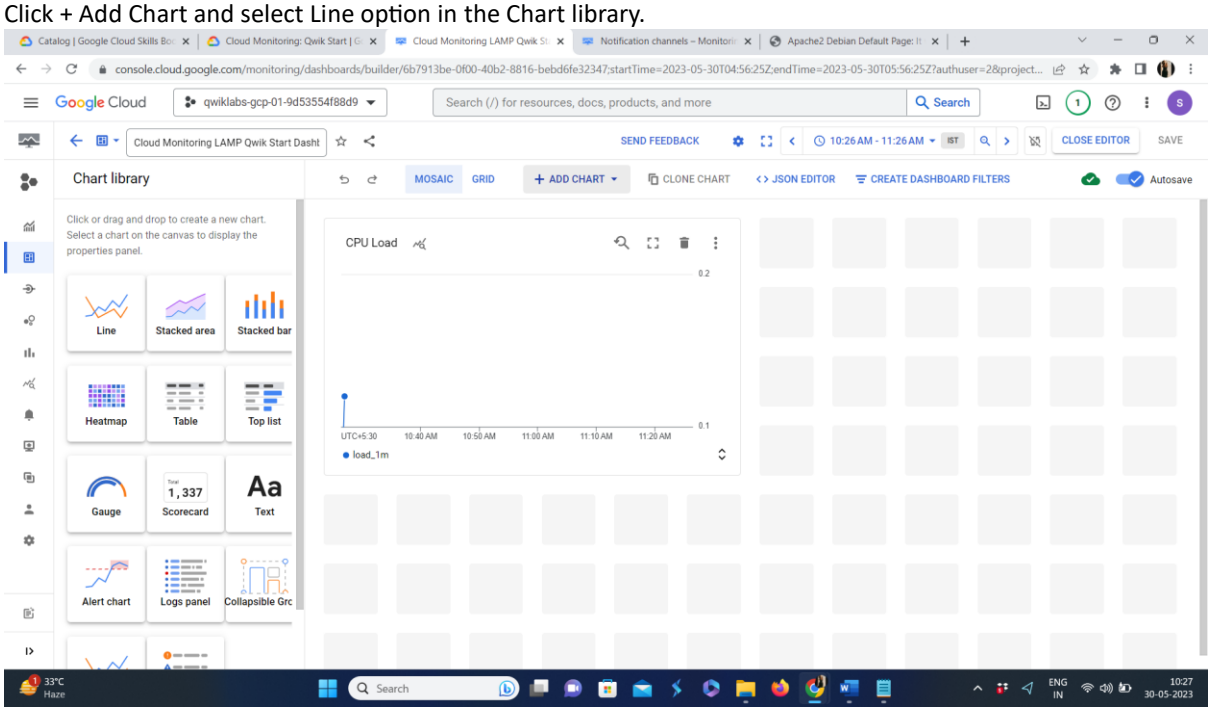
Type CPU load (1m) in filter by resource and metric name and click on VM instance > Cpu. Select CPU load (1m) and click Apply. Leave all other fields at the default value. Refresh the tab to view the graph.



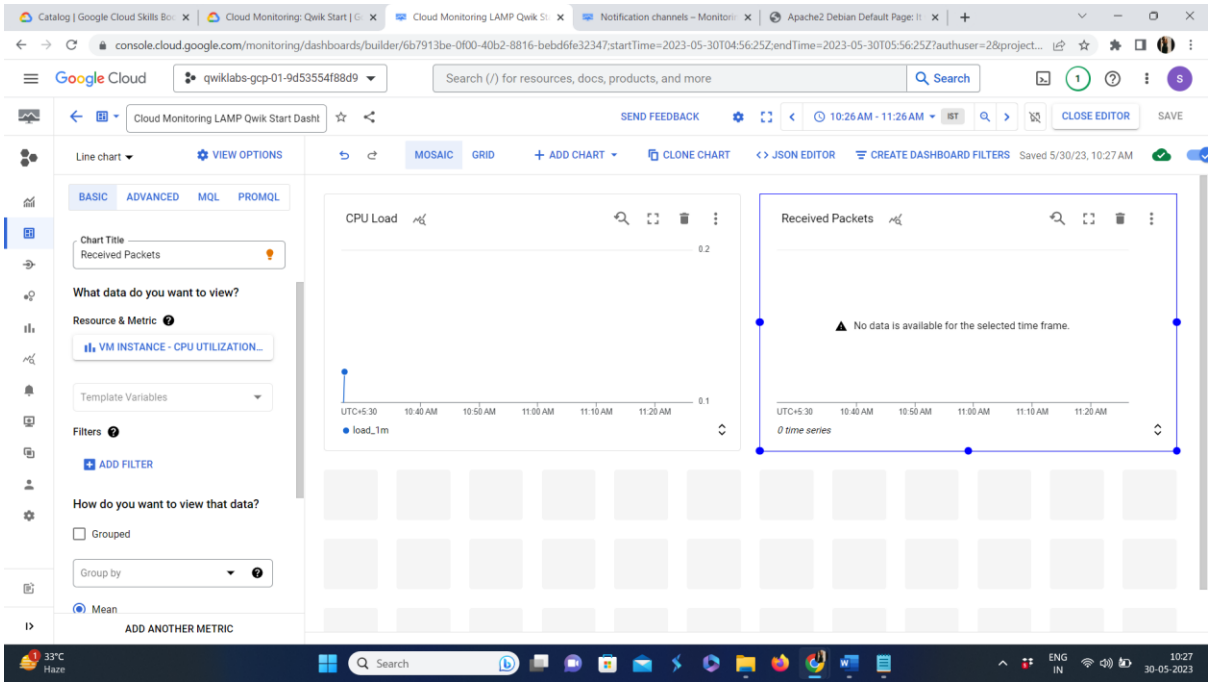


Add the second chart

Click + Add Chart and select Line option in the Chart library.

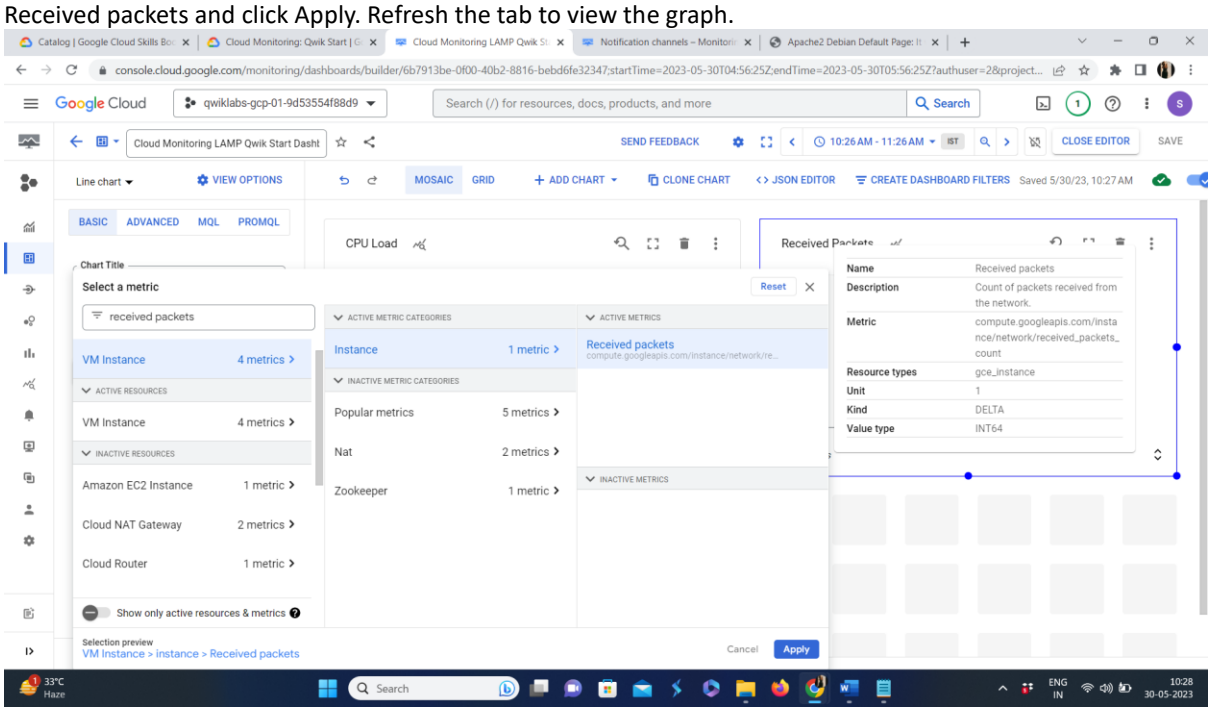


Name this chart Received Packets.



Click on Resource & Metric dropdown. Disable the Show only active resources & metrics.

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.

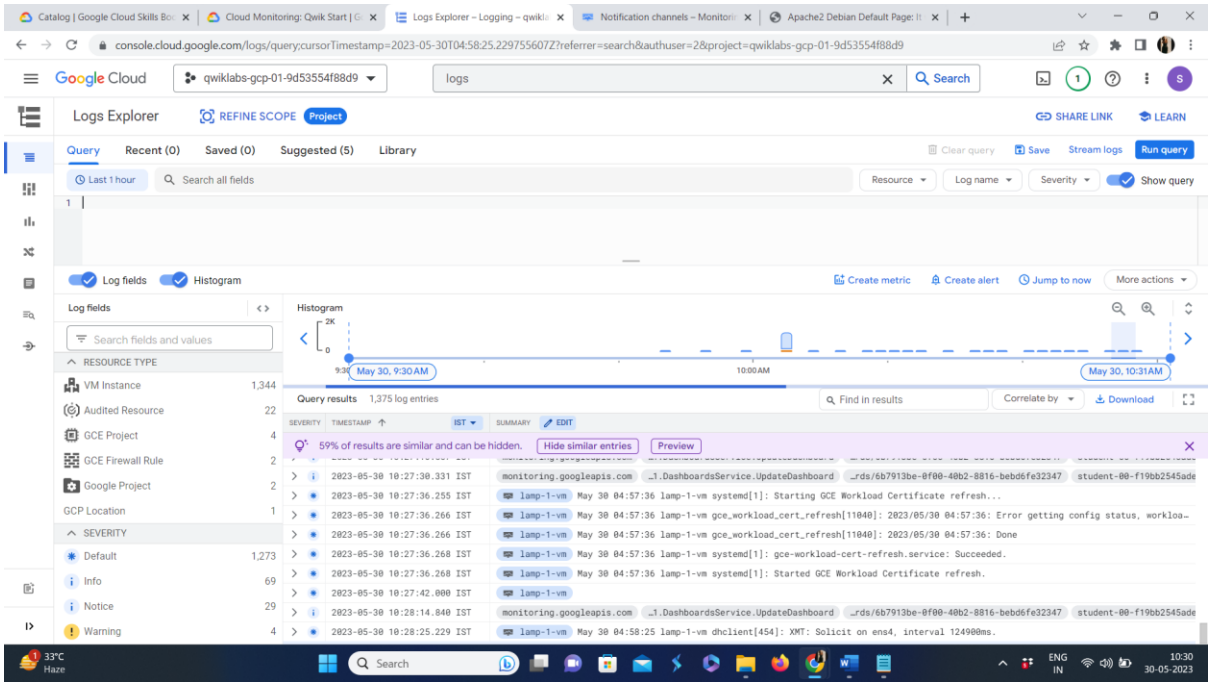


Leave the other fields at their default values. You see the chart data.

Task 6. View your logs

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

Select Navigation menu > Logging > Logs Explorer.



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 Resource.

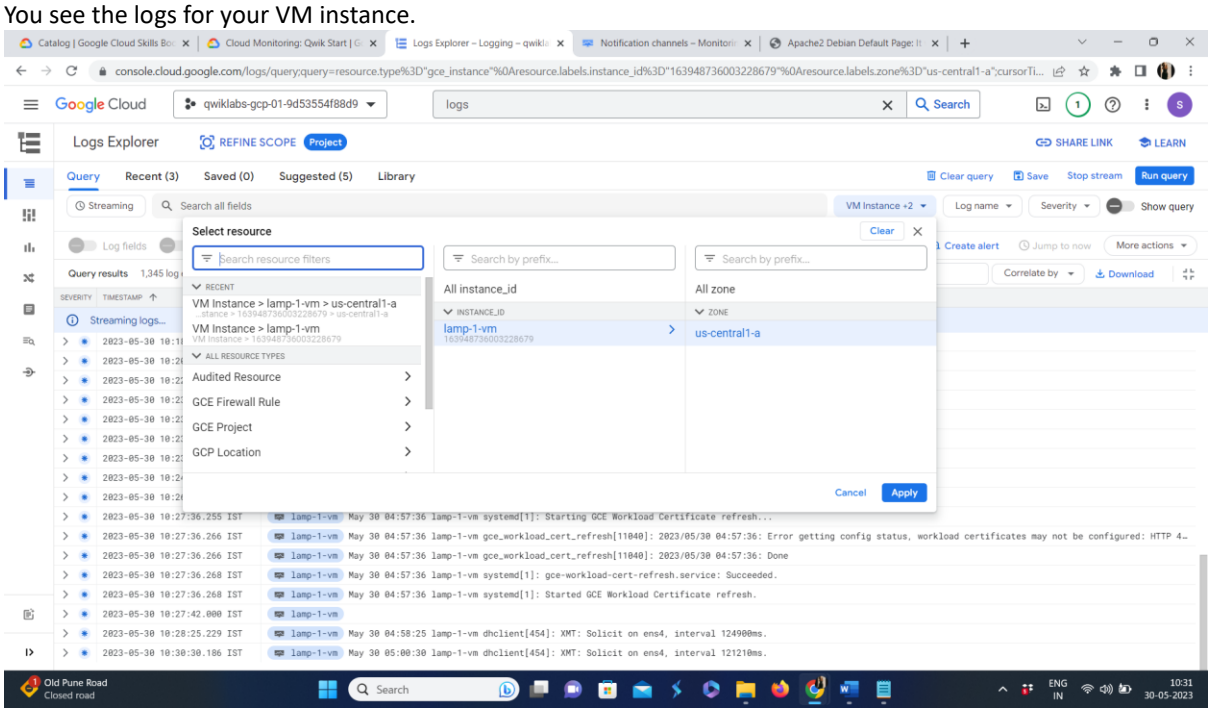
Select VM Instance > lamp-1-vm in the Resource drop-down menu.

Click Apply.

Leave the other fields with their default values.

Click the Stream logs.

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.

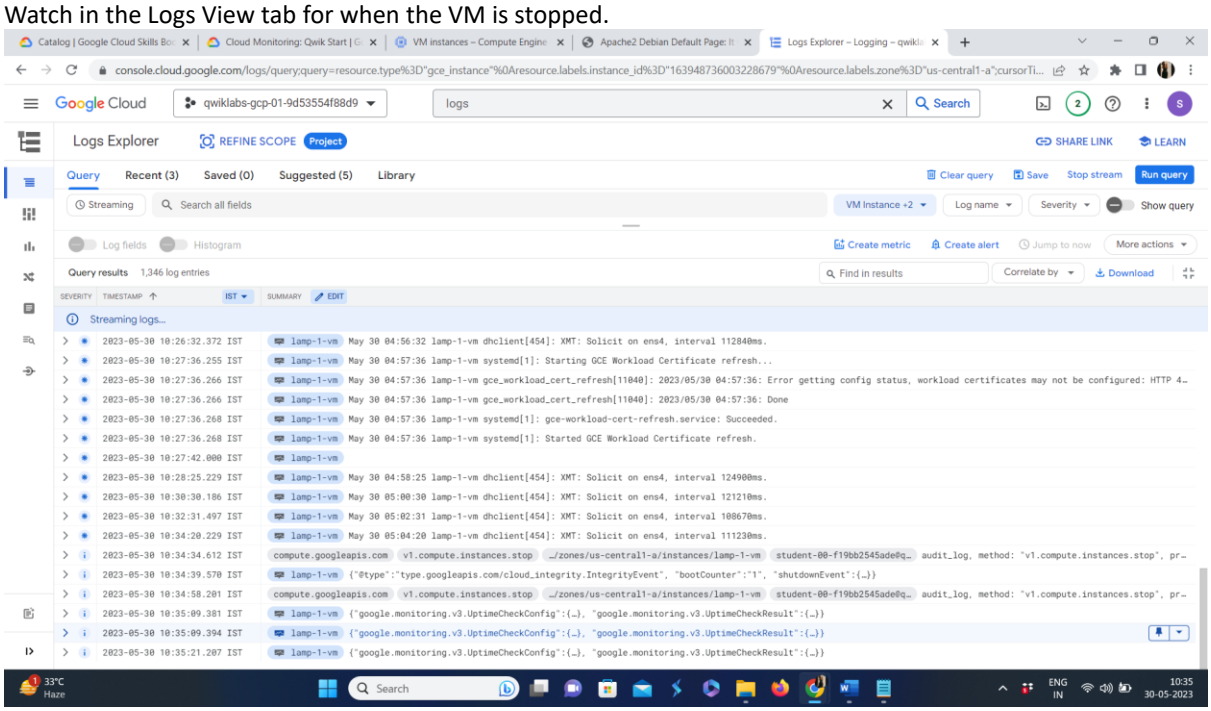
Open the Compute Engine window in a new browser window. Select Navigation menu > Compute Engine, right-click VM instances > Open link in new window.

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

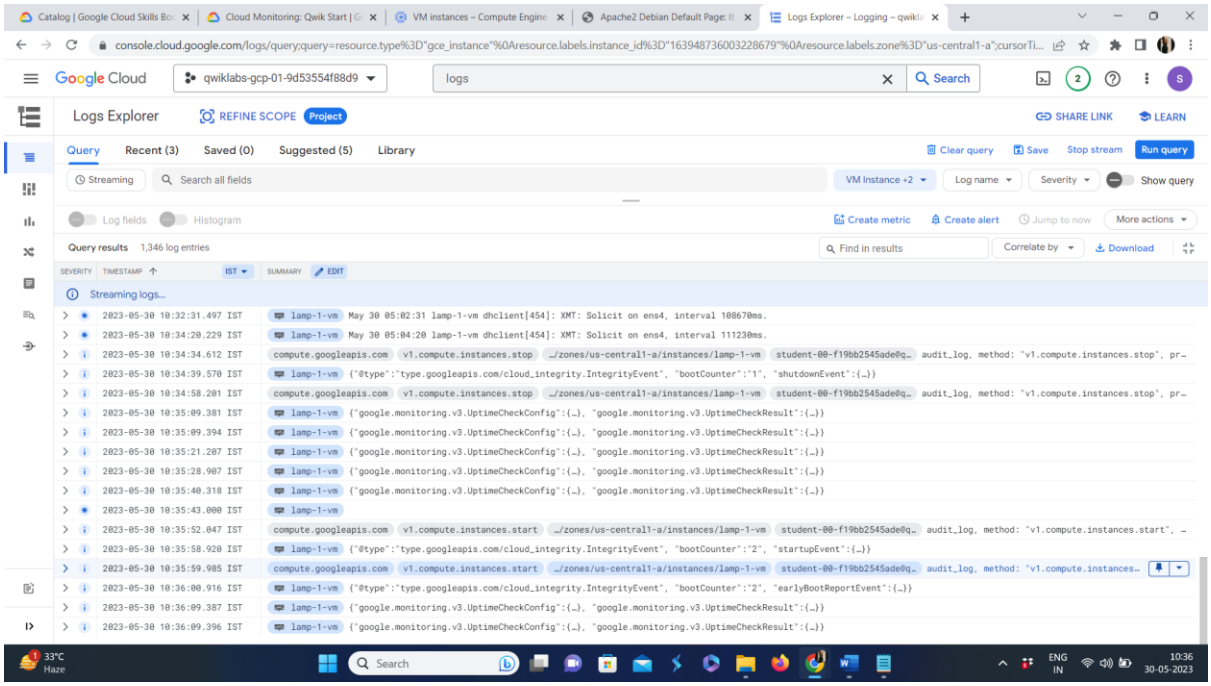
In the Compute Engine window, select the lamp-1-vm instance, click the three vertical dots at the right of the screen and then click Stop, and then confirm to stop the instance.

It takes a few minutes for the instance to stop.

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



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.

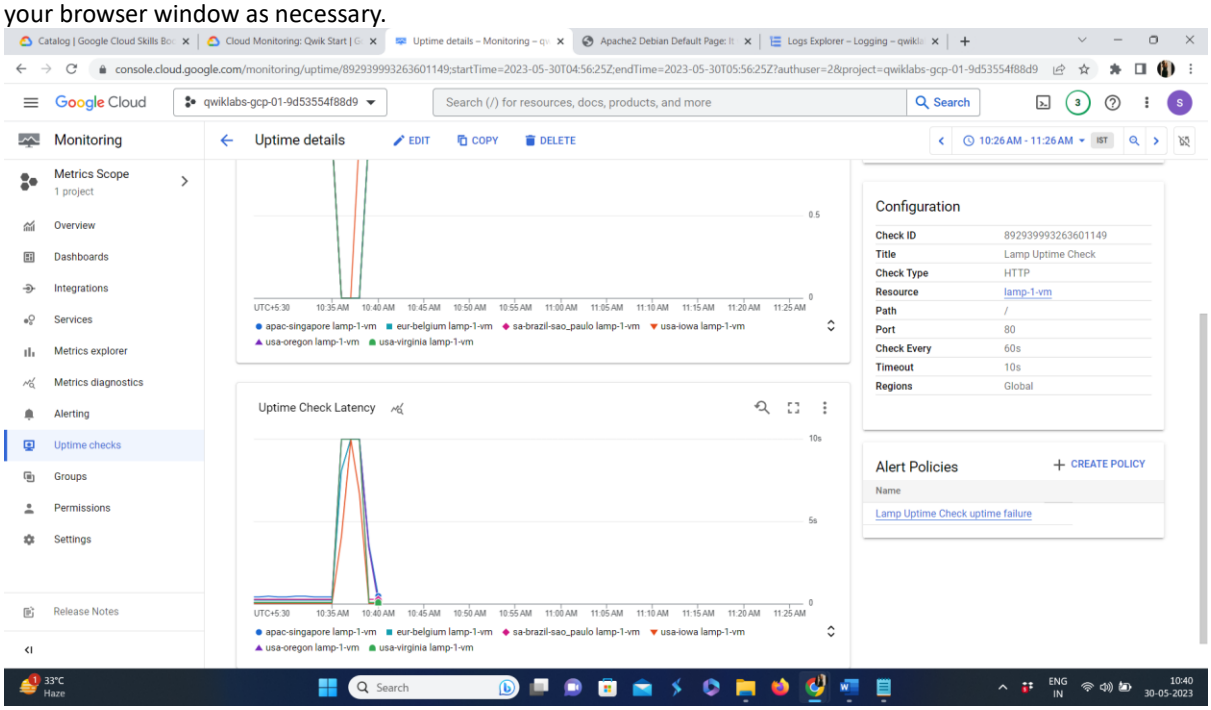


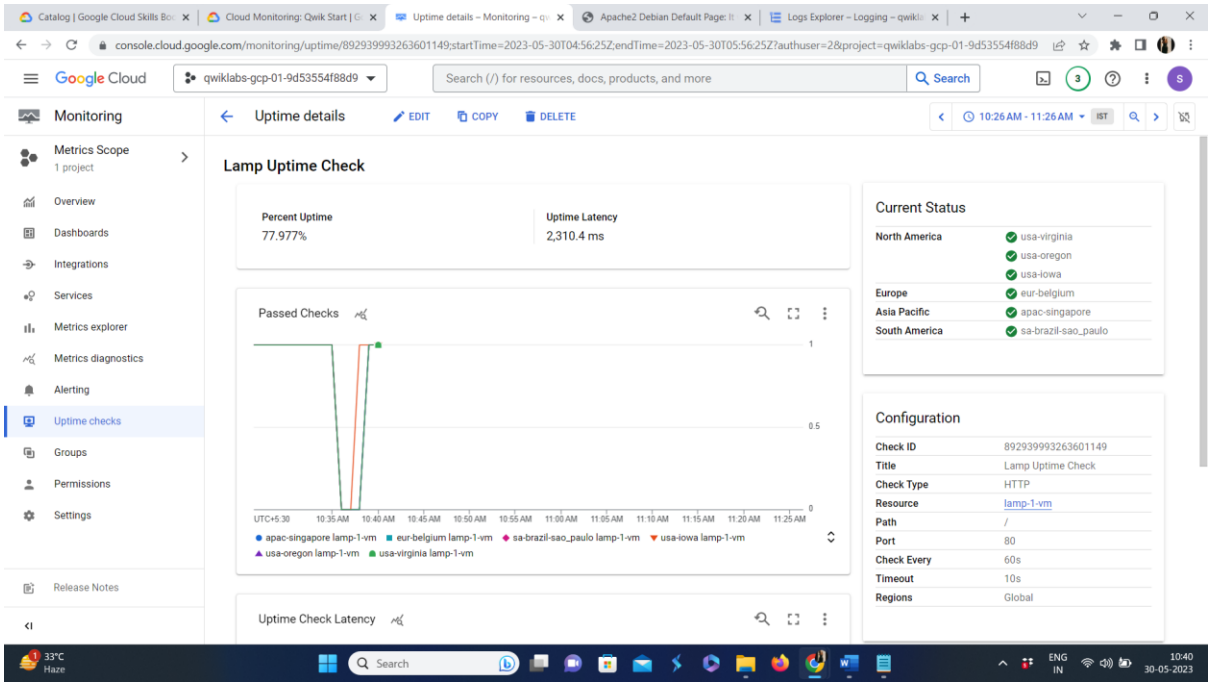
Task 7. Check the uptime check results and triggered alerts
In the Cloud Logging window, select Navigation menu > Monitoring > Uptime checks. This view provides a list of all active uptime checks, and the status of each in different locations.

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.

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
In the left menu, click Alerting.

You see incidents and events listed in the Alerting window.

Check your email account. You should see Cloud Monitoring Alerts.

You have successfully set up and monitored a VM with Cloud Monitoring.