

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.

Item	Monthly estimate
2 vCPU + 7.5 GB memory	\$69.35
10 GB balanced persistent disk	\$1.00
Use discount	-\$20.80
Total	\$49.54

#### Task 2. Add Apache2 HTTP Server to your instance

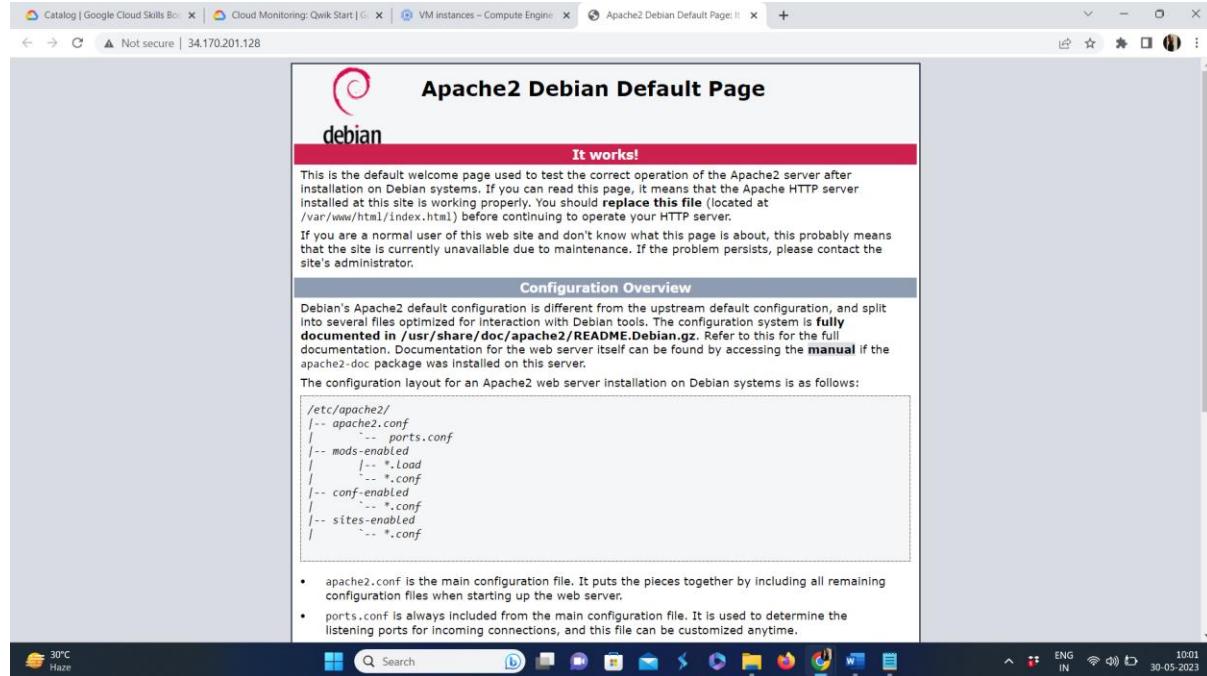
In the Console, click SSH in line with lamp-1-vm to open a terminal to your instance.

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:~$ 

```

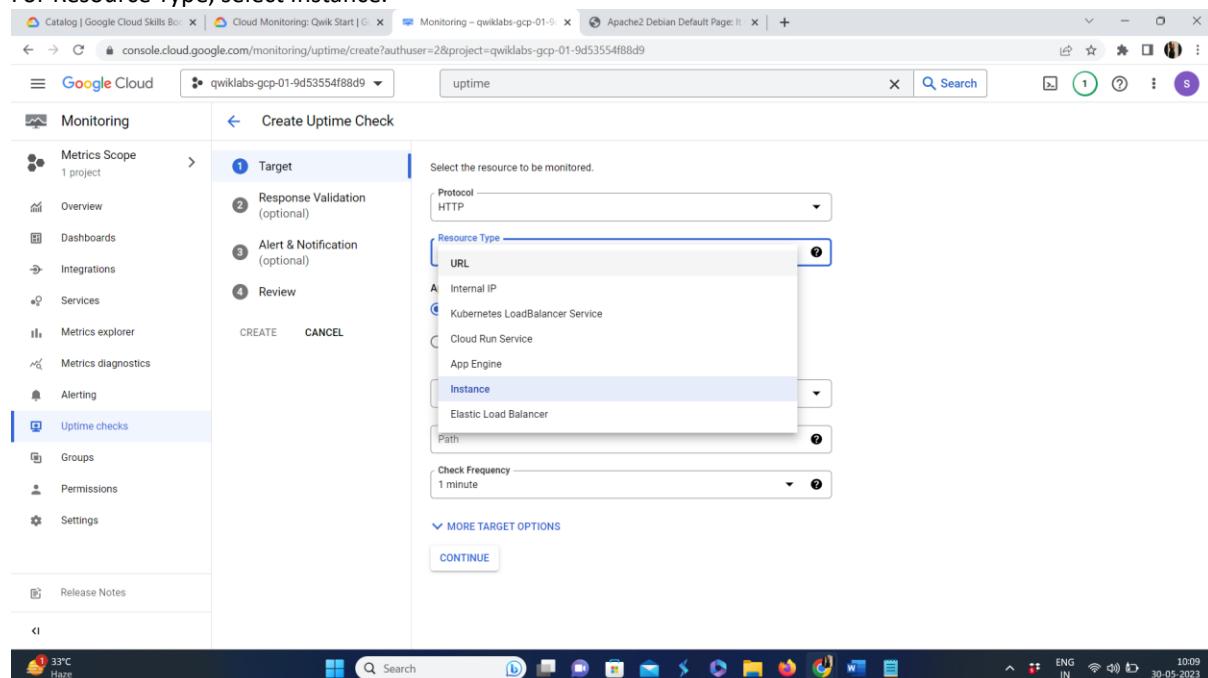
### Task 3. Create an uptime check

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.

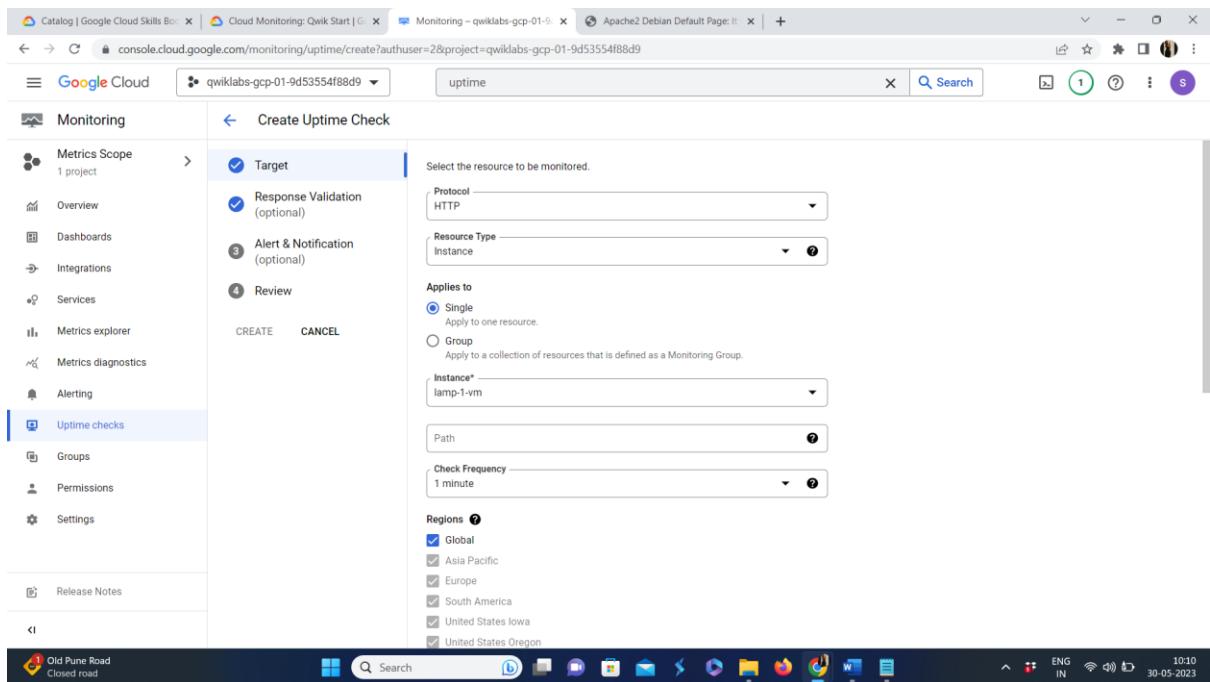
For Protocol, select HTTP.

For Resource Type, select Instance.



For Instance, select lamp-1-vm.

For Check Frequency, select 1 minute.



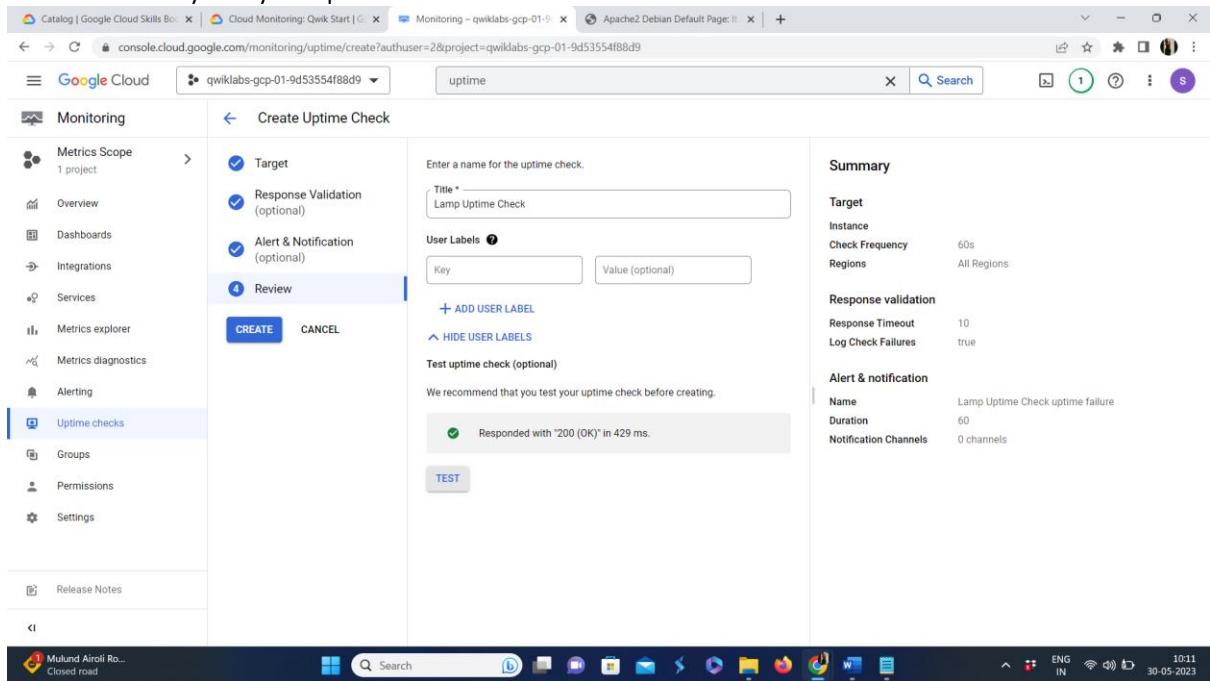
Click Continue.

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.

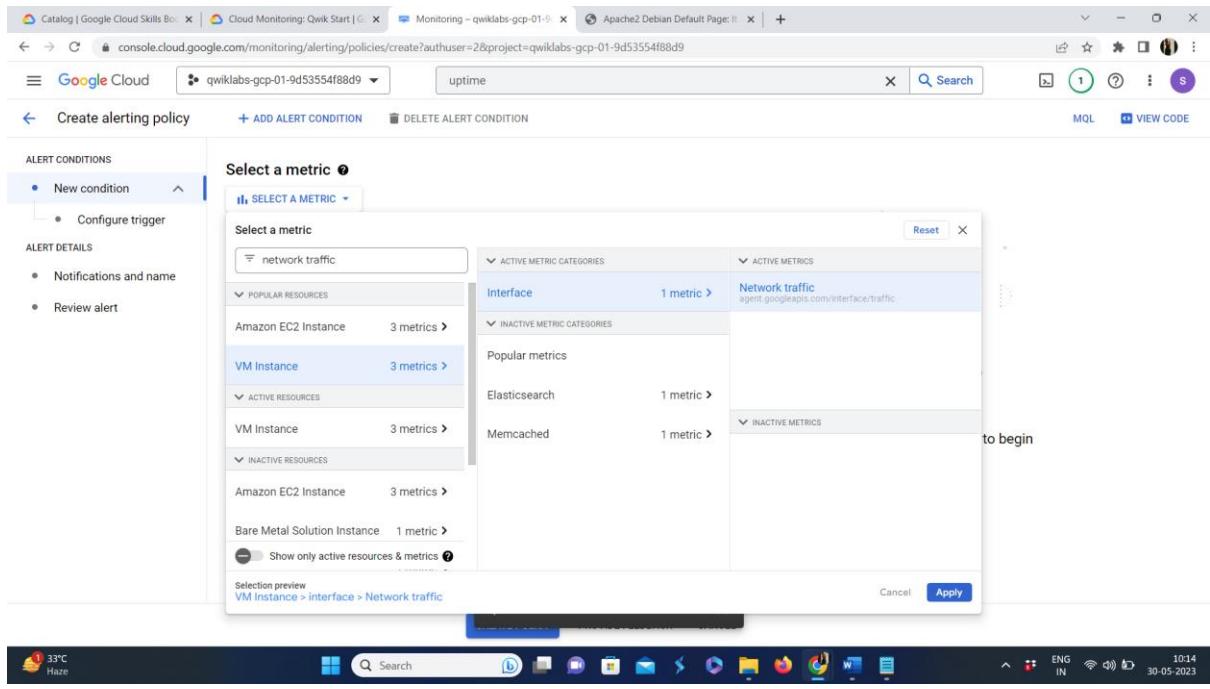
In the left menu, click Alerting, and then click +Create Policy.

The screenshot shows the Google Cloud Monitoring interface. On the left, there's a sidebar with various monitoring tools: Metrics Scope (1 project), Overview, Dashboards, Integrations, Services, Metrics explorer, Metrics diagnostics, Alerting (which is selected and highlighted in blue), Uptime checks, Groups, Permissions, Settings, and Release Notes. The main content area is titled 'Alerting' and shows a summary: 'Monitoring now supports both user-scoped and device-scoped Cloud Console Mobile notification channels'. It displays 'Incidents firing: 0', 'Incidents acknowledged: 0', and 'Alert policies: 1'. Below this is a 'Summary' card with sections for 'Incidents' and 'Snoozes'. A modal window at the bottom right says 'Uptime check and alert saved' with a close button. The status bar at the bottom shows it's 10:12 on 30-05-2023.

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

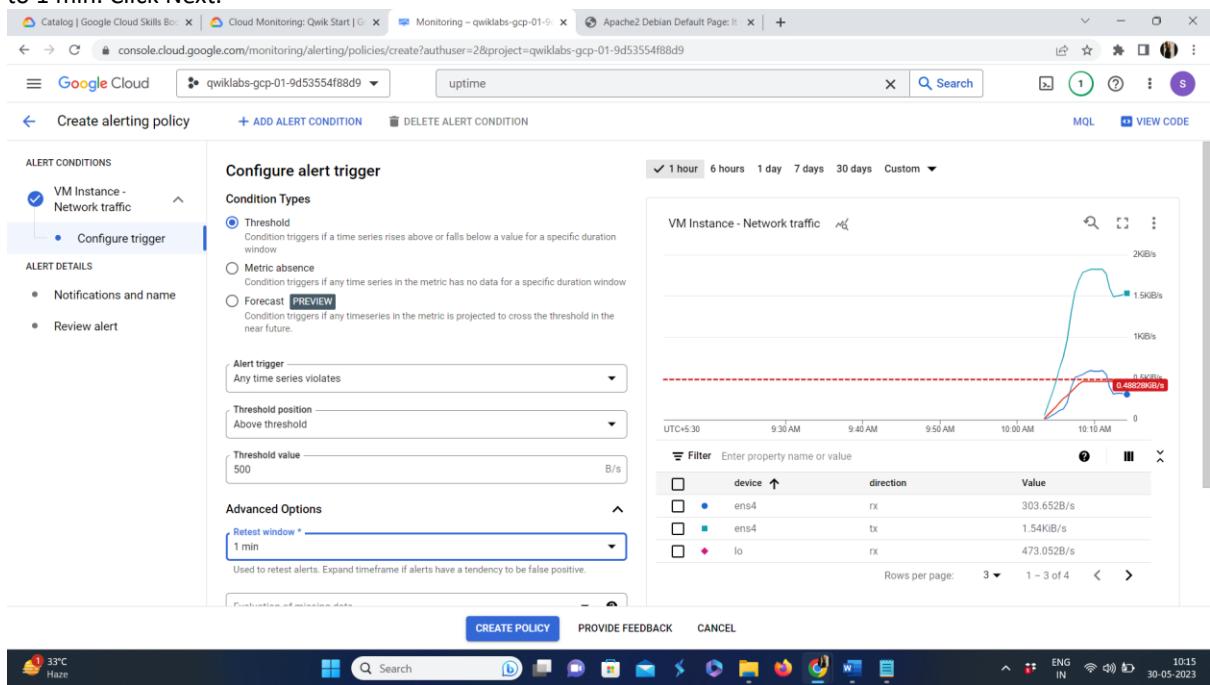
The screenshot shows the 'Create alerting policy' page. On the left, there are tabs for 'ALERT CONDITIONS' (New condition, Configure trigger), 'ALERT DETAILS' (Notifications and name, Review alert), and 'Review alert'. The 'ALERT CONDITIONS' tab is active. In the center, there's a 'Select a metric' dropdown with a sub-menu titled 'SELECT A METRIC'. This sub-menu has sections for 'POPULAR RESOURCES' (Amazon EC2 Instance, GAE Application, GKE Container, VM Instance) and 'ACTIVE RESOURCES' (Audited Resource). At the bottom of the dropdown, there's a checkbox labeled 'Show only active resources & metrics' with a help icon. A modal window at the bottom right says 'Uptime check and alert saved' with a close button. The status bar at the bottom shows it's 10:13 on 30-05-2023.

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.

The screenshot shows the Google Cloud Console interface for creating an alerting policy. The left sidebar has 'ALERT CONDITIONS' expanded, showing 'VM Instance - Network traffic' and 'Configure trigger'. The main area is titled 'Configure notifications and finalize alert'. Under 'Configure notifications', there's a note about recommended services like Cloud Mobile App, PagerDuty, Webhooks, and Slack. A modal window titled 'MANAGE NOTIFICATION CHANNELS' is displayed, indicating that no notification channels are available for the current workspace. Other options shown include 'Notify on incident closure' and 'Incident autoclose duration' set to 7 days. At the bottom, there are 'CREATE POLICY', 'PROVIDE FEEDBACK', and 'CANCEL' buttons.

Notification channels page will open in a new tab.

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

The screenshot shows the 'Notification channels' page in the Google Cloud Console. The left sidebar has 'Monitoring' selected. The main area lists various notification channels: 'Monitoring' (info message: 'Monitoring now supports both user-scoped and device-scoped Cloud Console Mobile notification channels'), 'PagerDuty Services' (info message: 'No PagerDuty services configured'), 'PagerDuty Sync' (info message: 'No PagerDuty Sync channels configured'), 'Slack' (info message: 'No Slack channels configured'), 'Webhooks' (info message: 'No webhook channels configured'), 'Email' (info message: 'No emails configured'), 'SMS' (info message: 'No SMS channels configured'), and 'Pub/Sub' (info message: 'No Pub/Sub channels configured'). Each channel entry includes an 'ADD NEW' button. The status bar at the bottom shows it's 10:16 on 30-05-2023.

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

Click on Save.

The screenshot shows the Google Cloud Monitoring - Notification channels interface. On the left sidebar, there are various monitoring and alerting options like Metrics Scope, Overview, Dashboards, Integrations, Services, Metrics explorer, Metrics diagnostics, Alerting, Uptime checks, Groups, Permissions, Settings, Release Notes, and Pub/Sub. The main area displays notification channels: PagerDuty Services, PagerDuty Sync (Beta), Slack, Webhooks, Email, SMS, and Pub/Sub. A modal window titled "Create Email Channel" is open, prompting for an "Email Address" (apnasapnayadav@gmail.com) and a "Display Name" (ALERT). Buttons for "CANCEL" and "SAVE" are at the bottom right of the modal.

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.

The screenshot shows the "Create alerting policy" page. The left sidebar lists "ALERT CONDITIONS" (VM Instance - Network traffic, Configure trigger) and "ALERT DETAILS" (Notifications and name, Review alert). The main area is titled "Configure notifications and finalize alert". It includes a "Configure notifications Recommended" section with a checked checkbox for "Use notification channel". Below it is a "Notification Channels" dropdown menu with "Email" selected and "ALERT" checked. There are also sections for "Policy user labels" and "CREATE POLICY", "PROVIDE FEEDBACK", and "CANCEL" buttons. At the bottom, there's a note about incident autoclose duration (7 days).

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.

The screenshot shows the Google Cloud Monitoring Dashboards Overview page. On the left, a sidebar menu includes options like Monitoring, Metrics Scope, Overview, Dashboards (which is selected), Integrations, Services, Metrics explorer, Metrics diagnostics, Alerting, Uptime checks, Groups, Permissions, Settings, and Release Notes. The main area displays a dashboard titled "Monitor your applications with Integrations!" with a brief description and a "VIEW AVAILABLE INTEGRATIONS" button. Below this is a "DASHBOARD LIST" section with a "SAMPLE LIBRARY" link. A table lists various dashboards categorized by type (Google Cloud Platform) and name. A modal at the bottom right says "Alert policy Inbound Traffic Alert saved". The system tray at the bottom shows the date as 30-05-2023.

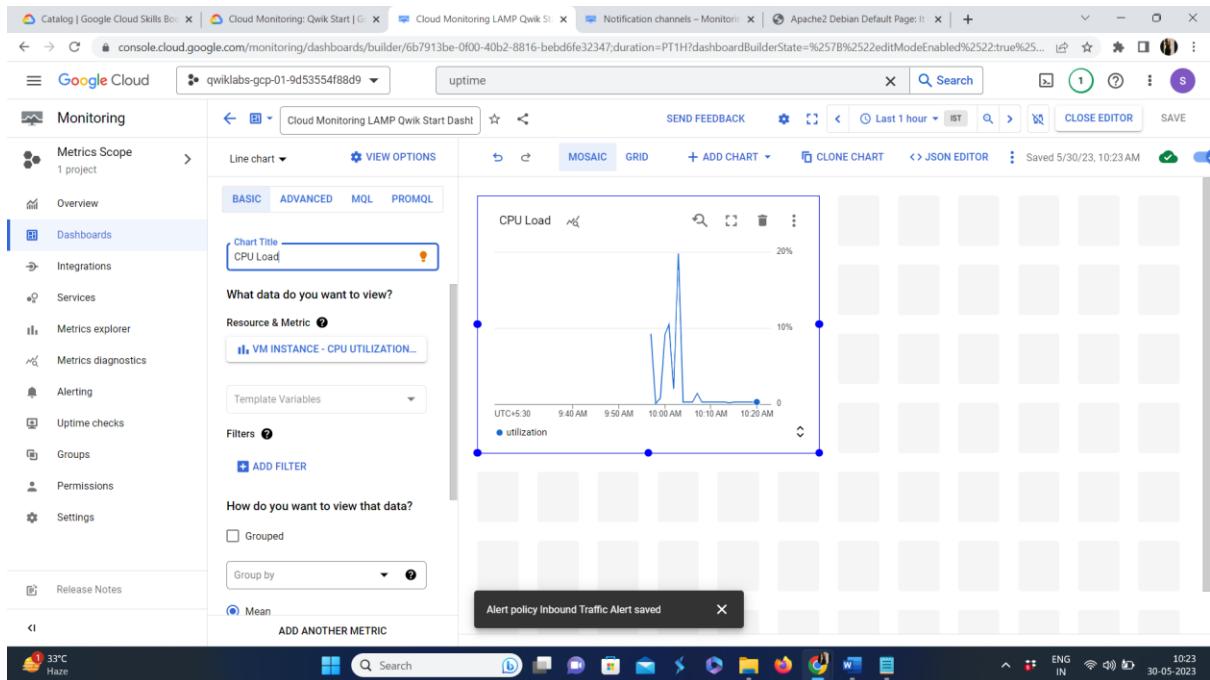
Name the dashboard Cloud Monitoring LAMP Qwik Start Dashboard.

Add the first chart

Click the Line option in the Chart library.

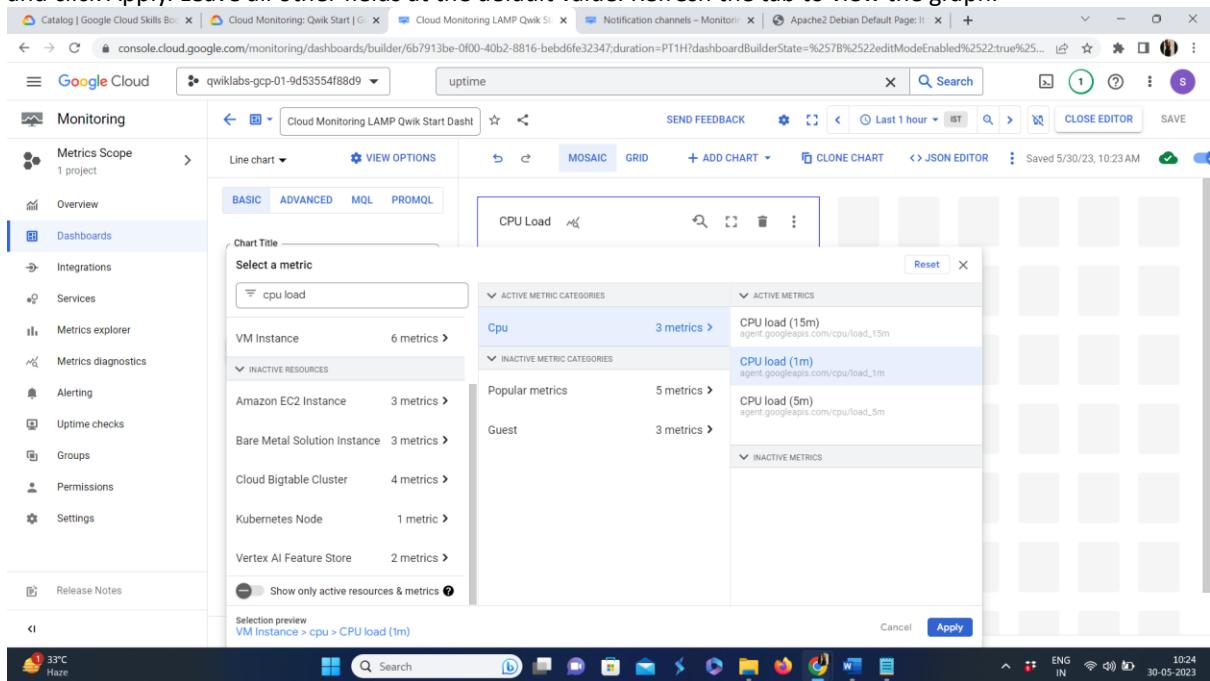
The screenshot shows the Google Cloud Monitoring Chart library. The sidebar is identical to the previous dashboard. The main area features a "Chart library" header with instructions: "Click or drag and drop to create a new chart. Select a chart on the canvas to display the properties panel." Below this are several chart types: Line, Stacked area, Stacked bar, Heatmap, Table, Top list, Gauge, Scorecard, Text, Alert chart, Logs panel, and Collapsible Grid. The "Line" icon is highlighted. A modal at the bottom right says "Alert policy Inbound Traffic Alert saved". The system tray at the bottom shows the date as 30-05-2023.

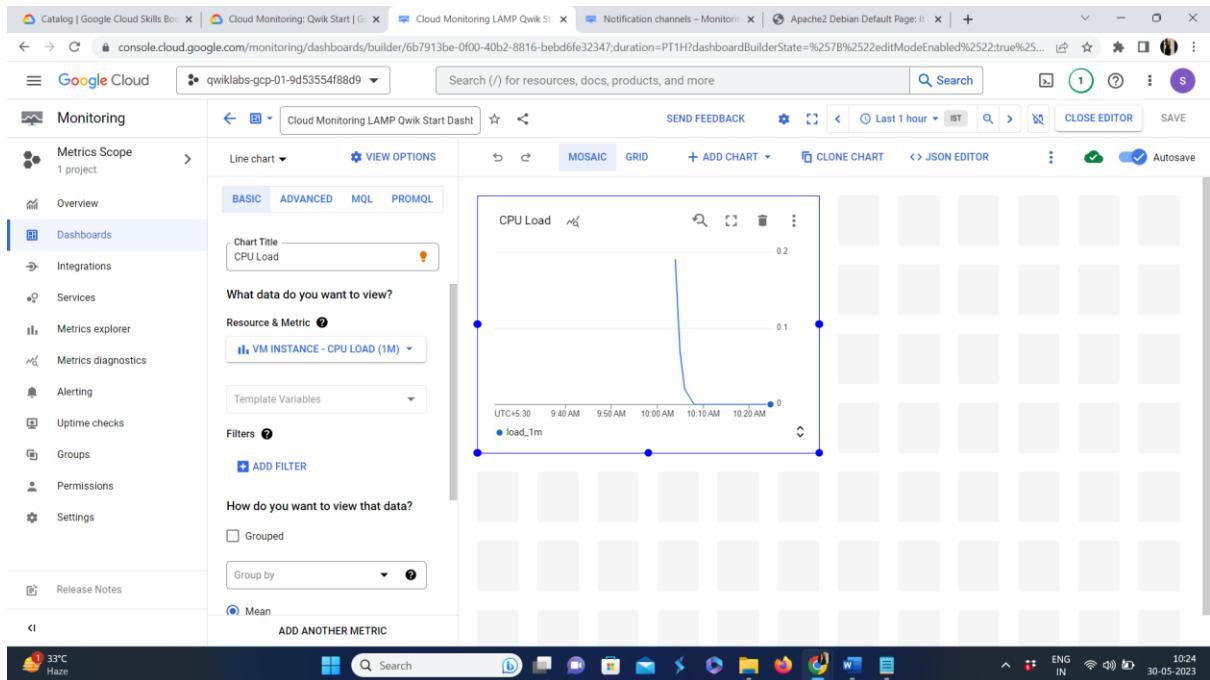
Name the chart title CPU Load.



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

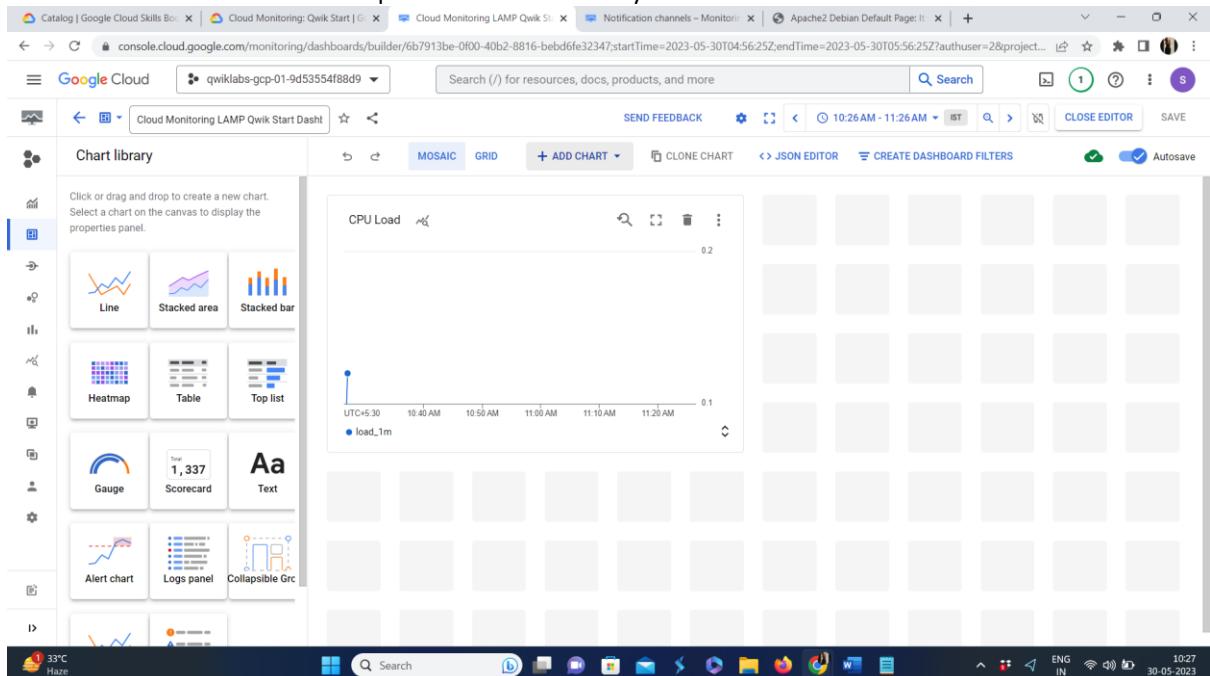
Type CPU load (1m) in filter by resource and metric name and click on VM instance > Cpu. Select CPU load (1m) and click Apply. Leave all other fields at the default value. Refresh the tab to view the graph.



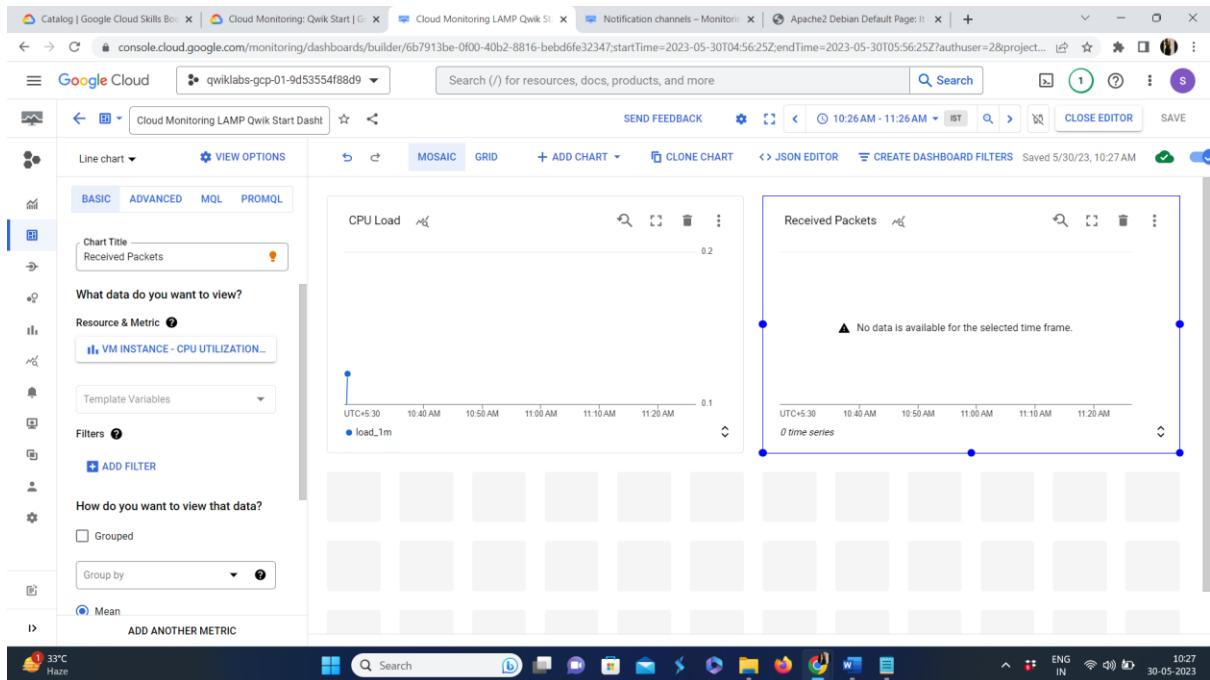


Add the second chart

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

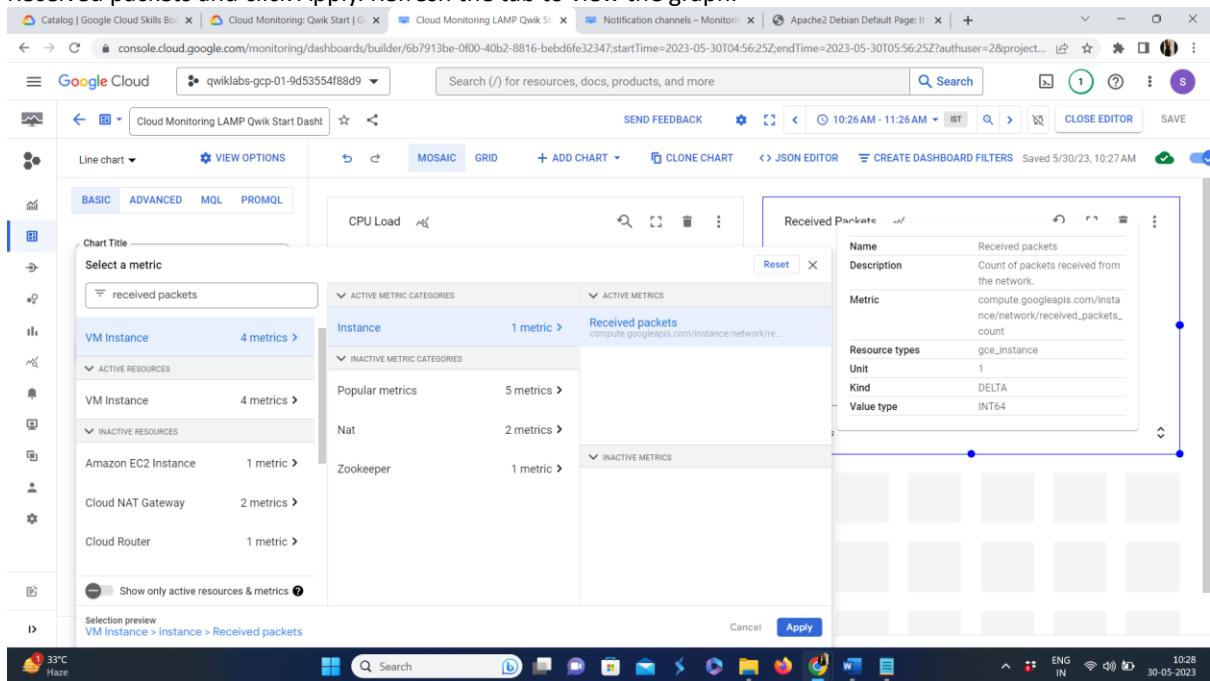


Name this chart Received Packets.



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.

VM Instance > lamp-1-vm > us-central1-a  
VM Instance > lamp-1-vm  
VM Instance > lamp-1-vm  
Audited Resource  
GCE Firewall Rule  
GCE Project  
GCP Location

Streaming logs...  
> 2023-05-30 10:27:36.255 IST lamp-1-vm May 30 04:57:36 lamp-1-vm systemd[1]: Starting GCE Workload Certificate refresh...  
> 2023-05-30 10:27:36.266 IST lamp-1-vm May 30 04:57:36 lamp-1-vm gce\_workload\_cert\_refresh[11040]: 2023/05/30 04:57:36: Error getting config status, workload certificates may not be configured: HTTP 404  
> 2023-05-30 10:27:36.266 IST lamp-1-vm May 30 04:57:36 lamp-1-vm gce\_workload\_cert\_refresh[11040]: 2023/05/30 04:57:36: Done  
> 2023-05-30 10:27:36.268 IST lamp-1-vm May 30 04:57:36 lamp-1-vm systemd[1]: gce-workload-cert-refresh.service: Succeeded.  
> 2023-05-30 10:27:36.268 IST lamp-1-vm May 30 04:57:36 lamp-1-vm systemd[1]: Started GCE Workload Certificate refresh.  
> 2023-05-30 10:27:42.000 IST lamp-1-vm May 30 04:58:25 lamp-1-vm dhclient[454]: XMT: Solicit on ens4, interval 124900ms.  
> 2023-05-30 10:28:25.229 IST lamp-1-vm May 30 04:58:25 lamp-1-vm dhclient[454]: XMT: Solicit on ens4, interval 124900ms.  
> 2023-05-30 10:30:30.186 IST lamp-1-vm May 30 05:00:38 lamp-1-vm dhclient[454]: XMT: Solicit on ens4, interval 121210ms.

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.

The screenshot shows the Google Cloud Logs Explorer interface. The top navigation bar includes tabs for Catalog, Google Cloud Skills Boost, Cloud Monitoring: Qwik Start, VM instances - Compute Engine, Apache2 Debian Default Page, and Logs Explorer - Logging - qwiklab. The main area is titled 'Logs' and shows a 'Logs Explorer' interface. It has sections for 'Logs' (selected), 'REFINE SCOPE' (set to 'Project'), 'Query' (Recent (3), Saved (0), Suggested (5), Library), and 'Run query'. Below this is a search bar and filter options for 'VM Instance +2', 'Log name', and 'Severity'. A 'Streaming' button is also present. The main content area displays 'Query results: 1,346 log entries'. The logs are sorted by 'TIMESTAMP' (descending). The first few log entries are as follows:

```
2023-05-30 10:26:32.372 IST lamp-1-vm May 30 04:56:32 lamp-1-vm dhclient[454]: XMT: Solicit on ens4, interval 112840ms.
2023-05-30 10:27:36.255 IST lamp-1-vm May 30 04:57:36 lamp-1-vm systemd[1]: Starting GCE Workload Certificate refresh...
2023-05-30 10:27:36.266 IST lamp-1-vm May 30 04:57:36 lamp-1-vm gce_workload_cert_refresh[11040]: 2023/05/30 04:57:36: Error getting config status, workload certificates may not be configured: HTTP 4...
2023-05-30 10:27:36.266 IST lamp-1-vm May 30 04:57:36 lamp-1-vm gce_workload_cert_refresh[11040]: 2023/05/30 04:57:36: Done
2023-05-30 10:27:36.268 IST lamp-1-vm May 30 04:57:36 lamp-1-vm systemd[1]: gce-workload-cert-refresh.service: Succeeded.
2023-05-30 10:27:36.268 IST lamp-1-vm May 30 04:57:36 lamp-1-vm systemd[1]: Started GCE Workload Certificate refresh.
2023-05-30 10:27:42.000 IST lamp-1-vm
2023-05-30 10:28:25.229 IST lamp-1-vm May 30 04:58:25 lamp-1-vm dhclient[454]: XMT: Solicit on ens4, interval 124900ms.
2023-05-30 10:30:30.184 IST lamp-1-vm May 30 05:00:30 lamp-1-vm dhclient[454]: XMT: Solicit on ens4, interval 121210ms.
2023-05-30 10:32:31.497 IST lamp-1-vm May 30 05:02:31 lamp-1-vm dhclient[454]: XMT: Solicit on ens4, interval 108670ms.
2023-05-30 10:34:20.229 IST lamp-1-vm May 30 05:04:20 lamp-1-vm dhclient[454]: XMT: Solicit on ens4, interval 111230ms.
2023-05-30 10:34:34.612 IST compute.googleapis.com v1.compute.instances.stop ... zones/us-central1-a/instances/lamp-1-vm student-00-f19bb2545ade@q... audit_log, method: "v1.compute.instances.stop", pr...
2023-05-30 10:34:39.570 IST lamp-1-vm {"@type": "type.googleapis.com/cloud_integrity.IntegrityEvent", "bootCounter": "1", "shutdownEvent": (...)}
2023-05-30 10:34:58.209 IST compute.googleapis.com v1.compute.instances.stop ... zones/us-central1-a/instances/lamp-1-vm student-00-f19bb2545ade@q... audit_log, method: "v1.compute.instances.stop", pr...
2023-05-30 10:35:09.381 IST lamp-1-vm {"google.monitoring.v3.UptimeCheckConfig": (...), "google.monitoring.v3.UptimeCheckResult": (...)}
2023-05-30 10:35:09.394 IST lamp-1-vm {"google.monitoring.v3.UptimeCheckConfig": (...), "google.monitoring.v3.UptimeCheckResult": (...)}
2023-05-30 10:35:21.287 IST lamp-1-vm {"google.monitoring.v3.UptimeCheckConfig": (...), "google.monitoring.v3.UptimeCheckResult": (...)}
```

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.

The screenshot shows the Google Cloud Logging interface. The search bar at the top contains the query: `resource.type="gce\_instance" AND resource.labels.instance\_id="163948736003228679" AND resource.labels.zone="us-central1-a" AND resource.labels.cursorTime > "2023-05-30T08:00:00Z"`. The results pane displays 1,346 log entries. The logs are timestamped from May 30, 2023, at 08:00:00 UTC to 10:36:00 UTC. Many entries are from the URL `compute.googleapis.com` and involve the method `v1.compute.instances.stop` or `v1.compute.instances.start` being called on the instance `lamp-1-vm` in the `us-central1-a` zone. Other logs show system events like `dhclient` and `audit\_log` entries.

### 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.

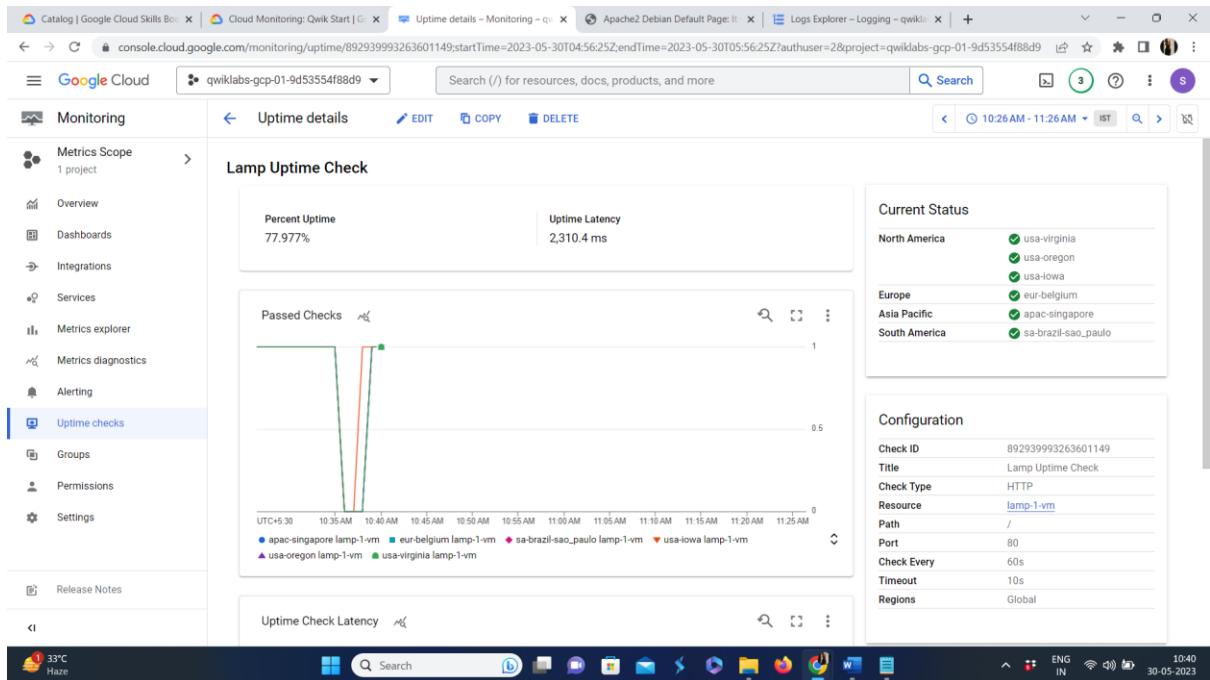
Click the name of the uptime check, Lamp Uptime Check.

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

The screenshot shows the Google Cloud Monitoring Uptime details page. The left sidebar is under the 'Monitoring' section and has 'Uptime checks' selected. The main area shows two charts: 'Uptime details' and 'Uptime Check Latency'. The 'Uptime details' chart shows a sharp peak at 10:35 AM UTC, with colors corresponding to regions: apac-singapore (blue), eur-belgium (green), sa-brazil-sao\_paulo (red), usa-iowa (orange), usa-oregon (purple), and usa-virginia (pink). The 'Uptime Check Latency' chart shows a similar sharp peak at the same time. On the right side, there is a 'Configuration' panel with the following details:

Check ID	892939993263601149
Title	Lamp Uptime Check
Check Type	HTTP
Resource	lamp-1-vm
Path	/
Port	80
Check Every	60s
Timeout	10s
Regions	Global

Below the configuration is an 'Alert Policies' section with a single entry: 'Lamp Uptime Check uptime failure'.



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.