Lab1:

From Google Cloud Console

1. Go to the VM instances page by visiting:

<https://console.cloud.google.com/compute/instances>.

2. Click on each instance name to go to its VM instance details page.

3. Under the section API and identity management, ensure that the default

Compute Engine service account is not used. This account is named

[PROJECT\_NUMBER]-compute@developer.gserviceaccount.com.

From Google Cloud CLI

1. List the instances in your project and get details on each instance:

gcloud compute instances list --format=json | jq -r '. | "SA:

\(.[].serviceAccounts[].email) Name: \(.[].name)"'

Lab2:

From Google Cloud Console

1. Go to the VM instances page by visiting:

<https://console.cloud.google.com/compute/instances>.

2. Click on the instance name to go to its VM instance details page.

3. Click STOP and then click EDIT.

4. Under the section API and identity management, select a service account other

than the default Compute Engine service account. You may first need to create a new service account.

5. Click Save and then click START.

From Google Cloud CLI

1. Stop the instance:

gcloud compute instances stop <INSTANCE\_NAME>

2. Update the instance:

gcloud compute instances set-service-account <INSTANCE\_NAME> --serviceaccount=<SERVICE\_ACCOUNT>

3. Restart the instance:

gcloud compute instances start <INSTANCE\_NAME>

Lab3: Check the Api access for cloud instances

From Google Cloud Console

1. Go to the VM instances page by visiting:

<https://console.cloud.google.com/compute/instances>.

2. Click on each instance name to go to its VM instance details page

3. Under the API and identity management, ensure that Cloud API access scopes is not set to Allow full access to all Cloud APIs.

Lab 4:

From Google Cloud Console

1. Go to the VM instances page by visiting:

<https://console.cloud.google.com/compute/instances>.

2. Click on the impacted VM instance.

3. If the instance is not stopped, click the Stop button. Wait for the instance to be

stopped.

4. Next, click the Edit button.

5. Scroll down to the Service Account section.

6. Select a different service account or ensure that Allow full access to all

Cloud APIs is not selected.

7. Click the Save button to save your changes and then click START.