lab 6

Create a service account.

Assign a role to that service account.

Generate a key for the service account.

Use the service account to authenticate and interact with Google Cloud resources.

Lab Steps:Step 1: Create a Service Account

First, we will create a service account in a specific project (openwriteup) using the gcloud CLI.

Command:

gcloud iam service-accounts create my-sa-account \

--description="My service account for lab" \

--display-name="My SA Account" \

--project=openwriteup

This will create a service account named my-sa-account in the project openwriteup.

Step 2: Assign a Role to the Service Account

Next, we will grant the service account the "Viewer" role, which allows it to view resources in the project.

Command:

gcloud projects add-iam-policy-binding openwriteup \

--member="serviceAccount:my-sa-account@openwriteup.iam.gserviceaccount.com" \

--role="roles/viewer"

This assigns the Viewer role to the my-sa-account service account.

Step 3: Generate a Key for the Service Account

To authenticate using the service account, we need to generate a key. This key will be used for authentication when performing tasks programmatically.

Command:

gcloud iam service-accounts keys create ~/my-sa-account-key.json \

--iam-account=my-sa-account@openwriteup.iam.gserviceaccount.com \

--project=openwriteup

This creates a private key for the service account and saves it to my-sa-account-key.json on your local machine.

Step 4: Set Up Authentication Using the Service Account Key

You can authenticate using the service account key you just created. Set the environment variable GOOGLE\_APPLICATION\_CREDENTIALS to the path of your key file.

Command:

export GOOGLE\_APPLICATION\_CREDENTIALS=~/my-sa-account-key.json

Now, your application or script will authenticate using this service account.

Step 5: Use the Service Account to List Resources

Now that you’ve set up authentication, let’s use the service account to perform actions. For example, listing the Google Cloud Storage buckets in the project openwriteup.

Command:

gcloud storage buckets list --project=openwriteup

This command should work using the my-sa-account service account since it has the Viewer role, which allows listing resources.

Step 6: Delete the Service Account Key

Once you're done using the key, it's best practice to delete it to prevent unauthorized access.

Command:

gcloud iam service-accounts keys delete <KEY\_ID> \

--iam-account=my-sa-account@openwriteup.iam.gserviceaccount.com \

--project=openwriteup

You can find the <KEY\_ID> by running:

gcloud iam service-accounts keys list --iam-account=my-sa-account@openwriteup.iam.gserviceaccount.com

Step 7: Clean Up by Deleting the Service Account

To remove the service account, use the following command:

Command:

gcloud iam service-accounts delete my-sa-account@openwriteup.iam.gserviceaccount.com --project provide project id