Lab:

From Google Cloud Console

Delete any external (user-managed) Service Account Key older than 90 days:

1. Go to APIs & Services\Credentials using

<https://console.cloud.google.com/apis/credentials>

2. In the Section Service Account Keys, for every external (user-managed) service

account key where creation date is greater than or equal to the past 90 days, click Delete Bin Icon to Delete Service Account key

Create a new external (user-managed) Service Account Key for a Service Account:

1. Go to APIs & Services\Credentials using

<https://console.cloud.google.com/apis/credentials>

2. Click Create Credentials and Select Service Account Key.

3. Choose the service account in the drop-down list for which an External (usermanaged) Service Account key needs to be created.

4. Select the desired key type format among JSON or P12.

5. Click Create. It will download the private key. Keep it safe.

6. Click Close if prompted.

7. The site will redirect to the APIs & Services\Credentials page. Make a note of the new ID displayed in the Service account keys section.

**Using Gcloud cli**

1) list the keys

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

2) script to rotate keys, create bash script , chmod

#!/bin/bash

# Define variables

PROJECT\_ID="openwriteup"

SERVICE\_ACCOUNT\_EMAIL="my-sa-account@openwriteup.iam.gserviceaccount.com"

KEY\_OUTPUT\_PATH="$HOME/keys"

ROTATION\_THRESHOLD\_DAYS=90 # Rotate keys older than this

# Ensure key output path exists

mkdir -p "$KEY\_OUTPUT\_PATH"

# Generate a new key

echo "Generating new key for $SERVICE\_ACCOUNT\_EMAIL..."

gcloud iam service-accounts keys create "$KEY\_OUTPUT\_PATH/new-key.json" \

--iam-account="$SERVICE\_ACCOUNT\_EMAIL" \

--project="$PROJECT\_ID"

# Get current date in seconds since epoch

current\_date=$(date +%s)

# List all existing keys for the service account

echo "Checking for old keys to delete..."

for key\_info in $(gcloud iam service-accounts keys list \

--iam-account="$SERVICE\_ACCOUNT\_EMAIL" \

--format="value(name,validAfterTime)" \

| sed 's/ /\_/g'); do

# Split key info into ID and creation date

key\_id=$(echo "$key\_info" | cut -d'\_' -f1)

key\_creation\_date=$(echo "$key\_info" | cut -d'\_' -f2)

# Convert key creation date to seconds since epoch

key\_creation\_epoch=$(date -d "$key\_creation\_date" +%s)

# Calculate age of the key in days

key\_age\_days=$(( (current\_date - key\_creation\_epoch) / (60\*60\*24) ))

# Delete the key if it is older than the threshold

if [[ "$key\_age\_days" -ge "$ROTATION\_THRESHOLD\_DAYS" ]]; then

echo "Attempting to delete old key with ID $key\_id (age: $key\_age\_days days)"

gcloud iam service-accounts keys delete "$key\_id" \

--iam-account="$SERVICE\_ACCOUNT\_EMAIL" --quiet || {

echo "Failed to delete key with ID $key\_id due to FAILED\_PRECONDITION or other error."

}

else

echo "Key with ID $key\_id is $key\_age\_days days old, keeping it."

fi

done

echo "Key rotation complete."