05.1 IAM-Service Accounts -KirkYagami👨‍💻🕵️

Step-01: Introduction

- Perform Service Account steps using Google Cloud Web console
  - Create VM Instance
  - Connect to Compute Instance and create Storage Bucket and it should fail with default service account associated to Compute Instance
  - Create a Service Account
  - Associate a Storage Admin Role to Service Account
  - Switch the Service Account to Compute Instance with new one
  - Connect to Compute Instance, create Storage Bucket and It should work
  - Delete VM Instance

Step-02: Create a VM Instance

```
# Set Project
gcloud config set project PROJECT-ID
gcloud config set project bigdata3844

# Create VM Instance
gcloud compute instances create vm901 \
  --zone=us-central1-a \
  --machine-type=e2-micro \
  --network-interface=subnet=default
```

Step-03: Connect to VM Instance and verify with default service account we have access to create Storage Buckets

```
# Connect to VM Instance
gcloud compute ssh --zone "us-central1-a" "vm901" --project "bigdata3844"

# Set Project config
gcloud config set project PROJECT-ID
gcloud config set project bigdata3844

# List Accounts or Service Accounts configured
gcloud auth list
```

```
# List Cloud Storage Buckets
gcloud storage buckets list

# Create Cloud Storage Bucket
gcloud storage buckets create gs://BUCKET_NAME
gcloud storage buckets create gs://mybucket1032

## Sample Output
kirkyagami@vm901:~$ gcloud storage buckets create gs://mybucket1032
Creating gs://mybucket1032/...
ERROR: (gcloud.storage.buckets.create) HTTPError 403: Access denied.
kirkyagami@vm901:~$
```

Step-04: Create IAM Service Account and Grant Storage Admin Role

- Goto -> IAM & Admin -> Service Accounts -> CREATE SERVICE ACCOUNT

Service Account Details

- **Service account name:** mysa901
- **Service account ID:** Auto-generated
- **Service account description:** Service Account for VM Instances with Storage Admin privileges
- Click on CREATE AND CONTINUE

Grant this service account access to project (optional)

- **Select Role:** Storage Admin
- Click on CONTINUE

Grant users access to this service account (optional)

- NOTHING
- Click on DONE

Step-05: Verify the Service Account

- Goto -> IAM & Admin -> Service Accounts -> mysa901@bigdata3844.iam.gserviceaccount.com

- DETAILS TAB
- PERMISSIONS TAB
- KEYS TAB
- METRICS TAB
- LOGS TAB

Step-06: Verify the Service Account via IAM Tab

- Goto -> IAM & Admin -> IAM -> mysa901@bigdata3844.iam.gserviceaccount.com
- Click on **EDIT**
- Click on **ASSIGN ROLES** (If we want to add more roles)

Step-07: Update VM Instance with new Service Account

Step-07-01: Stop VM Instance

- Go to Compute Engine -> VM Instances -> vm2 -> STOP

Step-07-02: Update VM Instance with new Service Account

- Go to Compute Engine -> VM Instances -> vm2 -> EDIT
- **Service accounts:** mysa901@bigdata3844.iam.gserviceaccount.com
- Click on **Save**

Step-07-03: Start VM Instance

- Go to Compute Engine -> VM Instances -> vm2 -> START

Step-08: Connect to VM Instance and verify with new service account we have access to create Storage Buckets

```
# Connect to VM Instance
gcloud compute ssh --zone "us-central1-a" "vm901" --project "bigdata3844"

# Set Project config
gcloud config set project PROJECT-ID
gcloud config set project bigdata3844

# List Accounts or Service Accounts configured
gcloud auth list
```

```
# List Cloud Storage Buckets
gcloud storage buckets list

# Create Cloud Storage Bucket
gcloud storage buckets create gs://BUCKET_NAME
gcloud storage buckets create gs://mybucket1032

Important Note: Bucket name should be unique across google cloud

## Sample Output
kirkyagami@vm901:~$ gcloud storage buckets create gs://mybucket1032
Creating gs://mybucket1032/...
kirkyagami@vm901:~$

# List Cloud Storage Buckets
gcloud storage buckets list

# Delete Cloud Storage Bucket
gcloud storage buckets delete gs://mybucket1032
```

Step-09: Delete VM Instance

```
# Delete VM instance
gcloud compute instances delete vm901 --zone us-central1-a
```

Step-10: Get IAM Policy and Verify the Service Account and Role

```
# Get IAM Policy for the Project
gcloud projects get-iam-policy bigdata3844

# Sample Output
- members:
  - serviceAccount:mysa901@bigdata3844.iam.gserviceaccount.com
  role: roles/storage.admin
```