

# Exploring IAM

## Overview

In this lab, you learn how to use the Service Account User role and how to grant roles.

## Objectives

In this lab, you learn how to perform the following tasks:

- Use IAM to implement access control
- Restrict access to specific features or resources
- Use the Service Account User role

## Task 1. Setup for two users

Sign in to the Cloud Console as the first user

1. This lab provisions you with two user names available in the **Connection Details** dialog. Sign in to the Cloud Console in an Incognito window as usual with the **Username 1** provided in Qwiklabs. Note that both user names use the same single password.

## Sign in to the Cloud Console as the second user

1. Open another tab in your incognito window.
2. Browse to [console.cloud.google.com](https://console.cloud.google.com).
3. Click on the user icon in the top-right corner of the screen, and then click **Add account**.
4. Sign in to the Cloud Console with the **Username 2** provided in Qwiklabs.

**Note:** At some points in this lab, if you sign out of the **Username 1** account, the **Username 2** account is deleted by Qwiklabs. So remain signed in to **Username 1** until you are done using **Username 2**.

## Task 2. Explore the IAM console

Make sure you are on the **Username 1** Cloud Console tab.

Navigate to the IAM console and explore roles

1. On the **Navigation menu** (≡), click **IAM & admin > IAM**.
2. Click **Grant Access** and explore the roles in the drop-down menu. Note the various roles associated with each resource by navigating the **Roles** menu.
3. Click **CANCEL**.
4. Switch to the **Username 2** Cloud Console tab.
5. On the **Navigation menu** (≡), click **IAM & admin > IAM**. Browse the list for the lines with the names associated with **Username 1** and **Username 2** in the Qwiklabs **Connection Details** dialog.

**Note:** **Username 2** currently has access to the project, but does not have the Project Owner role, so it cannot edit any of the roles. Hover over the pencil icon for **Username 2** to verify this.

6. Switch back to the **Username 1** Cloud Console tab.
7. In the IAM console, for **Username 2**, click on the pencil icon. **Username 2** currently has the **Viewer** role. Do not change the Project Role.
8. Click **CANCEL**.

## Task 3. Prepare a resource for access testing

## Create a bucket and upload a sample file

1. Switch to the **Username 1** Cloud Console tab if you aren't already there.
2. On the **Navigation menu** (≡), click **Cloud Storage > Buckets**.
3. Click **+Create**.
4. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	Enter a globally unique name
Location type	Multi-region

**Note:** Record the bucket name: it will be used in a later step and referred to as [YOUR\_BUCKET\_NAME]

5. Click **CREATE**.

**Note:** If you see the prompt, **Public access will be prevented** and the option **Enforce public access prevention on this bucket** is checked, then click **Confirm**.

6. Click **UPLOAD FILES**.
7. Upload any sample file from your local machine.
8. When the file has been uploaded, click on the three dots at the end of the line containing the file, and click **Rename**.
9. Rename the file to **sample.txt**, and click **RENAME**.

## Verify project viewer access

1. Switch to the **Username 2** Cloud Console tab.
2. In the Console, navigate to **Navigation menu > Cloud Storage > Buckets**.
3. Verify that **Username 2** can see the bucket.

## Task 4. Remove project access

### Remove Project Viewer role for Username 2

1. Switch to the **Username 1** Cloud Console tab.
2. On the **Navigation menu** (≡), click **IAM & admin > IAM**.
3. Select **Username 2** and click **Remove Access**.

**Note:** Verify that you're removing access for **Username 2**. If you accidentally remove access for **Username 1** you will have to restart this lab!

4. Confirm by clicking **CONFIRM**.


Notice that the user has disappeared from the list! The user has no access now.

### Verify that Username 2 has lost access

1. Switch to the **Username 2** Cloud Console tab.
2. On the **Navigation menu** (≡), click **Cloud overview > Dashboard**.
3. On the **Navigation menu** (≡), click **Cloud Storage > Buckets**. An error will be displayed. If not, refresh the page. **Username 2** still has a Google Cloud account, but has no access to the project.

## Task 5. Add storage access


### Add storage permissions

1. Copy the value of **Username 2** from the Qwiklabs **Connection Details** dialog.
2. Switch to the **Username 1** Cloud Console tab.
3. On the **Navigation menu** () , click **IAM & admin > IAM**.
4. Click **Grant Access** to add the user.
5. For **New principals**, paste the **Username 2** value you copied from the Qwiklabs **Connection Details** dialog.
6. For **Select a role**, select **Cloud Storage > Storage Object Viewer**.
7. Click **SAVE**.

### Verify that Username 2 has storage access

1. Switch to the **Username 2** Cloud Console tab.

**Note:** **Username 2** doesn't have Project Viewer roles, so that user can't see the project or any of its resources in the Console. However, the user has specific access to Cloud Storage.

2. To start Cloud Shell, click **Activate Cloud Shell** (). If prompted, click **Continue**.
3. To view the contents of the bucket you created earlier, run the following command, replacing `[YOUR_BUCKET_NAME]` with the unique name of the Cloud Storage bucket you created:

```
gcloud storage ls gs://[YOUR_BUCKET_NAME]
```


As you can see, **Username 2** has limited access to Cloud Storage.

4. Close the **Username 2** Cloud Console tab. The rest of the lab is performed on the **Username 1** Cloud Console tab.
5. Switch to the **Username 1** Cloud Console tab.

## Task 6. Set up the Service Account User

In this part of the lab, you assign narrow permissions to service accounts and learn how to use the Service Account User role.

### Create a service account

1. On the **Navigation menu** () , click **IAM & Admin > Service Accounts**.
2. Click **+ CREATE SERVICE ACCOUNT**.
3. Specify the **Service account name** as **read-bucket-objects** .
4. Click **CREATE AND CONTINUE**.
5. For **Select a role**, select **Cloud Storage > Storage Object Viewer** .
6. Click **CONTINUE**.
7. Click **DONE**.

### Add the user to the service account

1. Select the **read-bucket-objects** service account.
2. Click on the three dots to the right of the service account name. Then click on **Manage permissions**

**Note:** You will grant the user the role of Service Account User, which allows that person to use a service account on a VM, if they have access to the VM. You could perform this activity for a specific user, group, or domain. For training purposes, you will grant the Service Account User role to everyone at a company called Altostrat.com. Altostrat.com is a fake company used for demonstration and training.

3. Click on the **GRANT ACCESS** button. Specify the following, and leave the remaining settings as their defaults:


Property	Value (type value or select option as specified)
New principals	altostrat.com
Role	Service Accounts > Service Account User

- 4.

Click **SAVE**.

## Grant Compute Engine access

You now give the entire organization at Altostrat the Compute Engine Admin role.

1. On the **Navigation menu** () , click **IAM & admin > IAM**.
2. Click **Grant Access**.
3. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
New principals	altostrat.com




Select a role	Compute Engine > Compute Instance Admin (v1)
---------------	--

4. Click **SAVE**.

**Note:** This step is a rehearsal of the activity you would perform for a specific user. This action gives the user limited abilities with a VM instance. The user will be able to connect via SSH to a VM and perform some administration tasks.

## Create a VM with the Service Account User

1. On the **Navigation menu** () , click **Compute Engine > VM instances**.
2. Click **CREATE INSTANCE**.
3. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	demoiam
Region	us-east5
Zone	us-east5-a
Series	E2
Machine Type	e2-micro (2 vCPU, 1 GB memory)
Boot disk	Debian GNU/Linux 11 (bullseye)

Service account	read-bucket-objects
-----------------	---------------------

4. Click **Create**.

## Task 7. Explore the Service Account User role

At this point, you might have the user test access by connecting via SSH to the VM and performing the next actions. As the owner of the project, you already possess the Service Account User role. So you can simulate what the user would experience by just using SSH to access the VM from the Cloud Console.

The actions you perform and results will be the same as if you were the target user.

### Use the Service Account User

1. For **demoiam**, click **SSH** to launch a terminal and connect.
2. Run the following command:

```
gcloud compute instances list
```

Result (**example output**):

```
ERROR: (gcloud.compute.instances.list) Some requests did not succeed:  
- Required 'compute.zones.list' permission for 'projects/qwiklabs-gcp'
```

What happened? Why?

3. Copy the sample.txt file from the bucket you created earlier. Note that the trailing period is part of the command below. It means copy to "this location":

```
gcloud storage cp gs://[YOUR_BUCKET_NAME]/sample.txt .
```

Result (**example output**):

```
Copying gs://train-test-iam/sample.txt...  
/ [1 files][ 28.0 B/ 28.0 B]  
Operation completed over 1 objects/28.0 B.
```

4. To rename the file you copied, run the following command:

```
mv sample.txt sample2.txt
```

5. To copy the renamed file back to the bucket, run the following command:

```
gcloud storage cp sample2.txt gs://[YOUR_BUCKET_NAME]
```

Copied!


content\_copy

Result (**example output**):

```
AccessDeniedException: 403 Caller does not have storage.objects.create  
access to bucket train-test-iam.
```

**Note:** What happened? Because you connected via SSH to the instance, you can act as the service account essentially assuming the same permissions. The service account the instance was started with had the Storage Viewer role, which permits downloading objects from GCS buckets in the project. To list instances in a project, you need to grant the compute.instance.list permission. Because the service account did not have this permission, you could not list instances running in the project. Because the service account *did* have permission to download objects, it

could download an object from the bucket. It did not have permission to write objects, so you got an 403 access denied message.

6. On the **Navigation menu** () , click **IAM & admin > IAM**.
7. Browse the list for the lines with **read-bucket-objects**, click on the pencil icon.  
**read-bucket-objects** currently has the **Storage Object Viewer** role. Alter the **Role** to **Cloud Storage > Storage Object Creator** .
8. Click **Save**
9. Return to the SSH window for **demoiam**
10. To copy the renamed file back to the bucket, run the following command:

```
gcloud storage cp sample2.txt gs://[YOUR_BUCKET_NAME]
```

Copied!

content\_copy

This time the command succeeds as the service account has the correct permissions.

## Task 8. Review

In this lab you exercised granting and revoking IAM roles, first to a user, **Username 2**, and then to a Service Account User. You could allocate Service Account User credentials and "bake" them into a VM to create specific-purpose authorized bastion hosts.