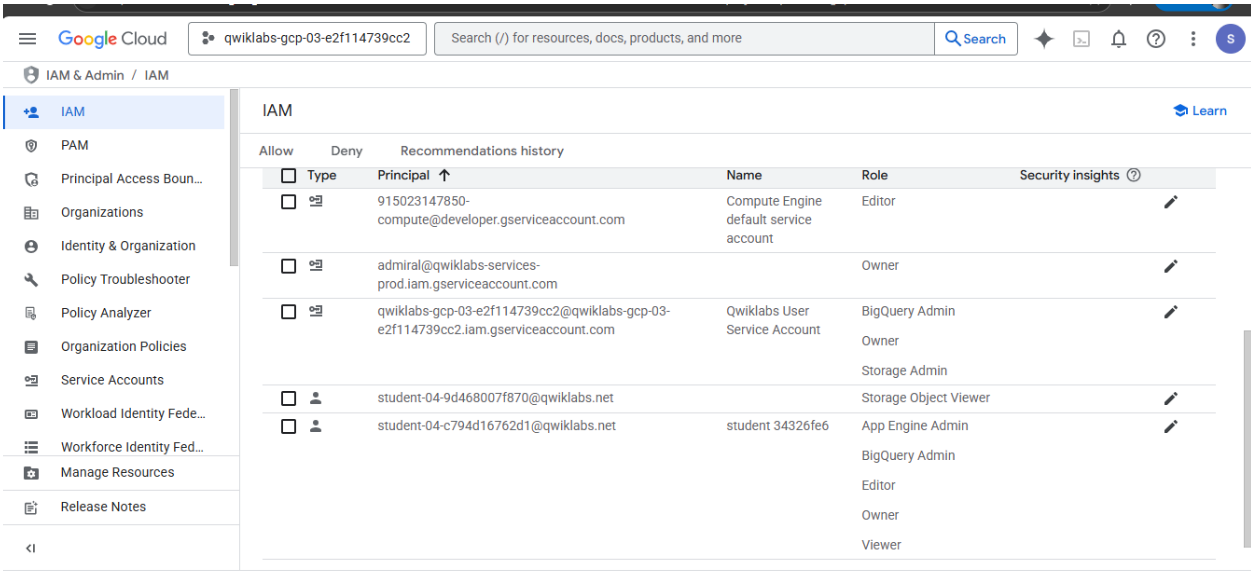
Cloud IAM: Qwik Start

Task 1. Explore the IAM console and project level roles

1. Return to the **Username 1** Cloud Console page.
2. Select **Navigation menu** > **IAM & Admin** > **IAM**. You are now in the "IAM & Admin" console.
3. Click **+GRANT ACCESS** button at the top of the page.
4. Scroll down to **Basic** in Select a role section and mouse over.
5. Click **CANCEL** to exit out of the "Add principal" panel.



☐ Type	Principal ↑	Name	Role	Security insights
☐	915023147850-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	
☐	admiral@qwiklabs-services-prod.iam.gserviceaccount.com		Owner	
☐	qwiklabs-gcp-03-e2f114739cc2@qwiklabs-gcp-03-e2f114739cc2.iam.gserviceaccount.com	Qwiklabs User Service Account	BigQuery Admin Owner Storage Admin	
☐	student-04-9d468007f870@qwiklabs.net		Storage Object Viewer	
☐	student-04-c794d16762d1@qwiklabs.net	student 34326fe6	App Engine Admin BigQuery Admin Editor Owner Viewer	

Explore the editor role

Now switch to the **Username 2** console.

1. Navigate to the IAM & Admin console, select **Navigation menu** > **IAM & Admin** > **IAM**.
2. Search through the table to find Username 1 and Username 2 and examine the roles they are granted. The Username 1 and Username 2 roles are listed inline and to the right of each user.

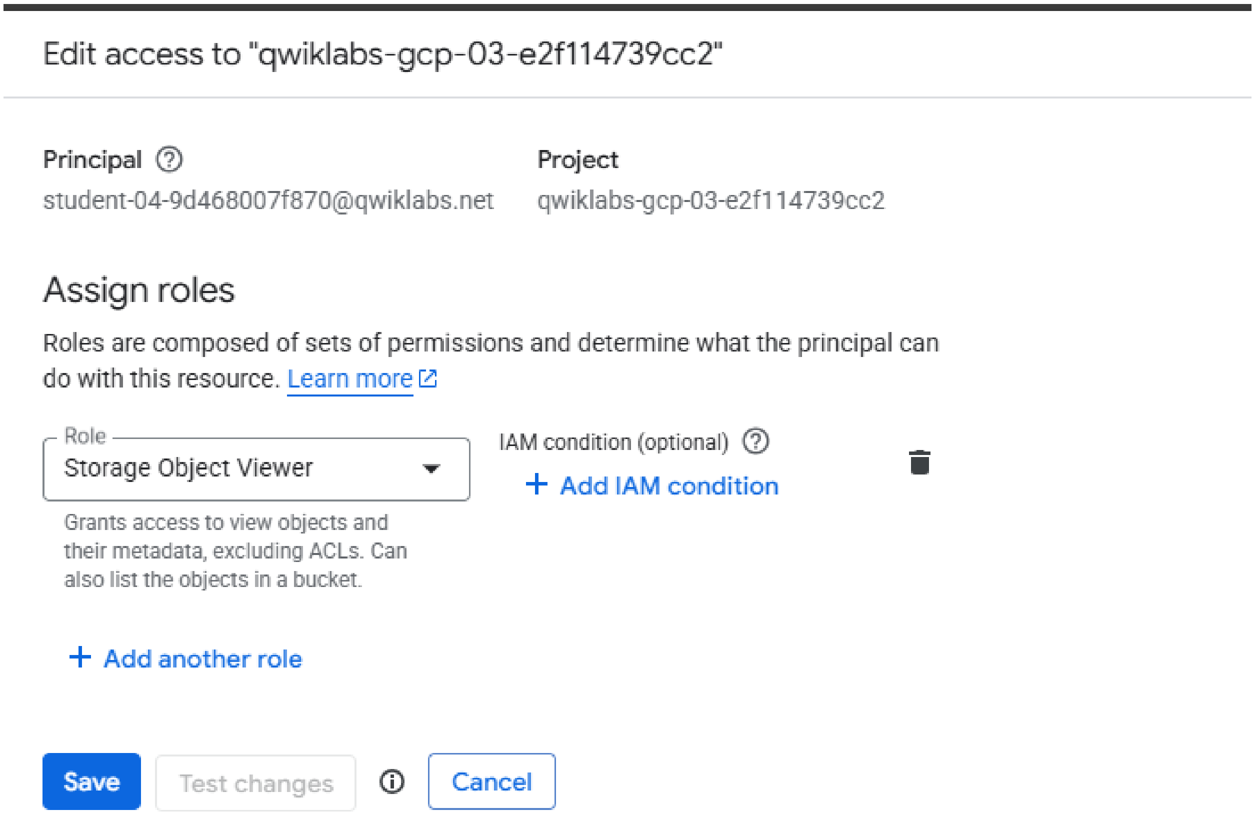
You should see:

- Username 2 has the "Viewer" role granted to it.

- The **+GRANT ACCESS** button at the top is grayed out—if you try to click on it you get the message, "You need permissions for this action. Required permission(s): resource manager.projects.setIamPolicy".

This is one example of how IAM roles affect what you can and cannot do in Google Cloud.

3. Switch back to the **Username 1** console for the next step.



Edit access to "qwiklabs-gcp-03-e2f114739cc2"

Principal
student-04-9d468007f870@qwiklabs.net

Project
qwiklabs-gcp-03-e2f114739cc2

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more

Role: Storage Object Viewer

Grants access to view objects and their metadata, excluding ACLs. Can also list the objects in a bucket.

IAM condition (optional)

Task 2. Prepare a Cloud Storage bucket for access testing

Ensure that you are in the **Username 1** Cloud Console.

Create a bucket

1. Create a Cloud Storage bucket with a unique name. From the Cloud Console, select **Navigation menu** > **Cloud Storage** > **Buckets**.

2. Click **+CREATE**.

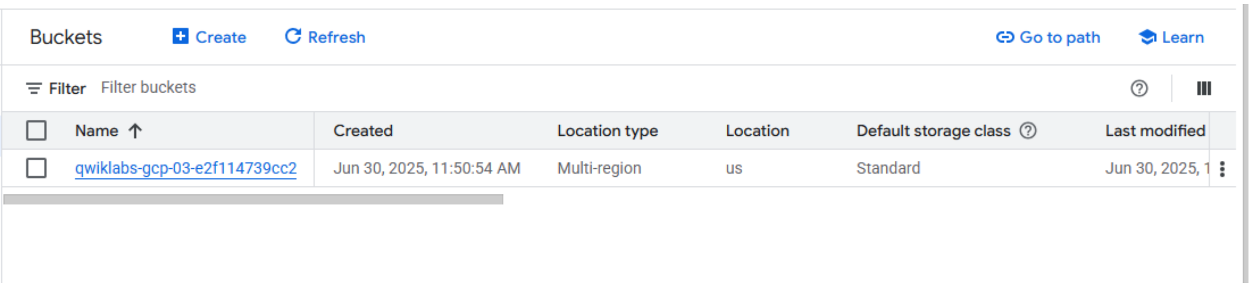
3. Update the following fields, leave all others at their default values:

Property	**Value**
Name:	*globally unique name (create it yourself!) and click* ***CONTINUE***.
Location Type:	Multi-Region

Note the bucket name. You will use it in a later step.

4. Click **CREATE**.

5. If prompted, Public access will be prevented, click **Confirm**.



□	Name ↑	Created	Location type	Location	Default storage class	Last modified
□	qwiklabs-gcp-03-e2f114739cc2	Jun 30, 2025, 11:50:54 AM	Multi-region	us	Standard	Jun 30, 2025, 1

Upload a sample file

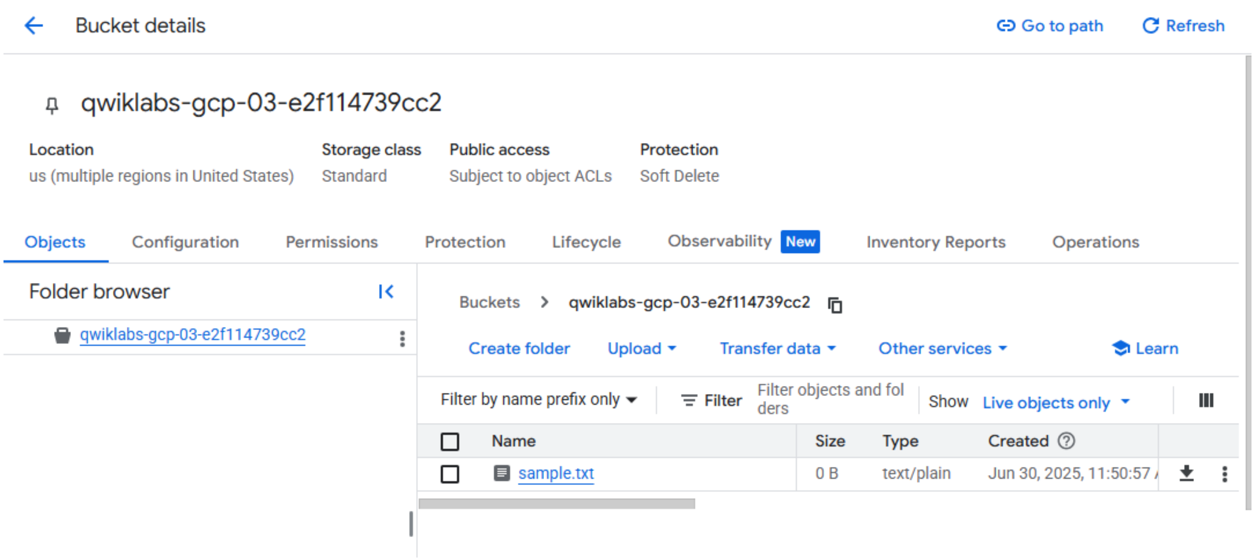
1. On the Bucket Details page click **UPLOAD FILES**.

2. Browse your computer to find a file to use. Any text or html file will do.

3. Click on the three dots at the end of the line containing the file and click **Rename**.

4. Rename the file ‘sample.txt'.

5. Click **RENAME**.



qwiklabs-gcp-03-e2f114739cc2

Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Subject to object ACLs	Soft Delete

Buckets > qwiklabs-gcp-03-e2f114739cc2

Name	Size	Type	Created
sample.txt	0 B	text/plain	Jun 30, 2025, 11:50:57

Task 3. Remove project access

Switch to the **Username 1** console.

Remove Project Viewer for Username 2

1. Select **Navigation menu** > **IAM & Admin** > **IAM**. Then click the pencil icon inline and to the right of **Username 2**.
2. Remove Project Viewer access for **Username 2** by clicking the trashcan icon next to the role name. Then click **SAVE**.

Verify that Username 2 has lost access

1. Switch to **Username 2** Cloud Console. Ensure that you are still signed in with Username 2's credentials and that you haven't been signed out of the project after permissions were revoked. If signed out, sign in back with the proper credentials.
2. Navigate back to Cloud Storage by selecting **Navigation menu** > **Cloud Storage** > **Buckets**.

Task 4. Add Cloud Storage permissions

1. Copy **Username 2** name from the **Lab Connection** panel.
2. Switch to **Username 1** console. Ensure that you are still signed in with Username 1's credentials. If you are signed out, sign in back with the proper credentials.
3. In the Console, select **Navigation menu** > **IAM & Admin** > **IAM**.

4. Click **+GRANT ACCESS** button and paste the **Username 2** name into the **New principals** field.

5. In the **Select a role** field, select **Cloud Storage** > **Storage Object Viewer** from the drop-down menu.

6. Click **SAVE**.

Verify access

1. Switch to the **Username 2** console. You'll still be on the Storage page.

Username 2 doesn't have the Project Viewer role, so that user can't see the project or any of its resources in the Console. However, this user has specific access to Cloud Storage, the Storage Object Viewer role - check it out now.

2. Click **Activate Cloud Shell** >_ to open the Cloud Shell command line. If prompted click **Continue**.

3. Open up a Cloud Shell session and then enter in the following command, replace [YOUR_BUCKET_NAME] with the name of the bucket you created earlier:

```
gsutil ls gs://[YOUR_BUCKET_NAME]
```

u can see, you gave **Username 2** view access to the Cloud Storage bucket.