

Cloud IAM: Qwik Start

The screenshot shows the Google Cloud console dashboard for the project `qwiklabs-gcp-02-3a7a72dd2ef8`. The top navigation bar includes the Google Cloud logo, the project name, a search bar, and a notification bell with 5 alerts. The main dashboard is divided into three columns:

- Project info:** Displays the project name, number, and ID. It includes a link to "ADD PEOPLE TO THIS PROJECT" and a "Go to project settings" button.
- APIs:** A line chart showing "Requests (requests/sec)" over time. The current request rate is 0.054/s. A "Go to APIs overview" button is at the bottom.
- Google Cloud Platform status:** Indicates "All services normal" with a "Go to Cloud status dashboard" link.

Below the main dashboard, there are two more sections:

- Billing:** Shows "Estimated charges" for the billing period May 1 – 6, 2025, as USD \$0.00. It includes a "Take a tour of billing" link and a "View detailed charges" button.
- Monitoring:** Offers options to "Create my dashboard" and "Set up alerting policies".

This screenshot shows the same Google Cloud console dashboard as above, but with a left-hand navigation menu expanded. The menu includes:

- Cloud Hub**
- Cloud overview** (highlighted)
- Solutions**
- PINNED PRODUCTS**
- PRODUCTS**
- Billing**
- IAM & Admin**
- Marketplace**
- APIs & Services**
- Vertex AI**
- Compute Engine**

The main dashboard content remains the same, showing project information, API request rates, and status/billing/monitoring sections. The bottom of the screen shows a Windows taskbar with the date 06-05-2025 and time 17:48.

Task 1. Explore the IAM console and project level roles

1. Return to the **Username 1** Cloud Console page.

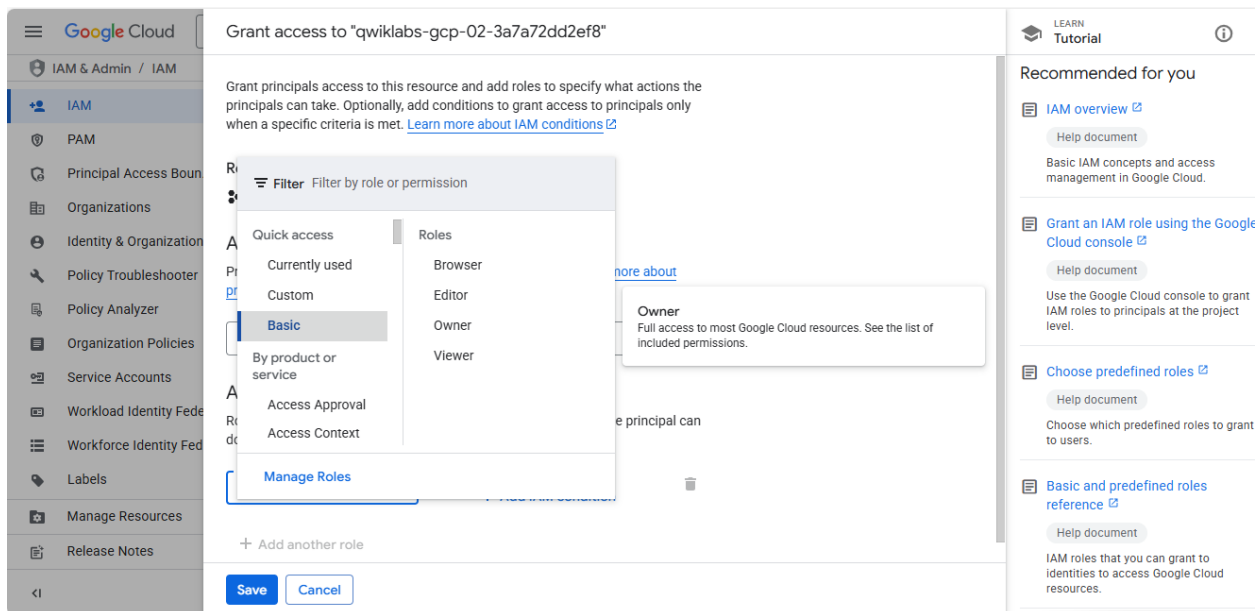
2. Select **Navigation menu > IAM & Admin > IAM**. You are now in the "IAM & Admin" console.
3. Click **+GRANT ACCESS** button at the top of the page.
4. Scroll down to **Basic** in Select a role section and mouse over.

There are three roles:

- Editor
- Owner
- Viewer

These are *primitive roles* in Google Cloud. Primitive roles set project-level permissions and unless otherwise specified, they control access and management to all Google Cloud services.

The following table pulls definitions from the Google Cloud IAM article, [Basic roles](#), which gives a brief overview of browser, viewer, editor, and owner role permissions:



Since you are able to manage roles and permissions for this project, Username 1 has Project owner permissions.

4. Click **CANCEL** to exit out of the "Add principal" panel.

Explore the editor role

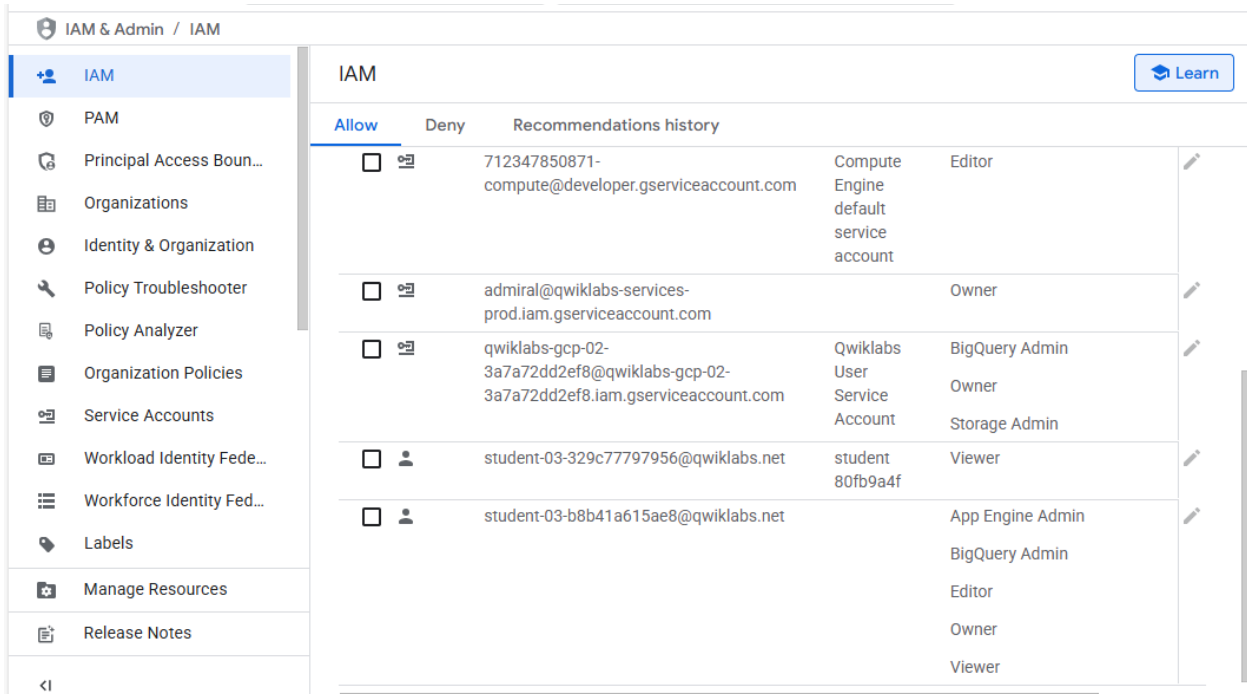
Now switch to the **Username 2** console.

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.



The screenshot shows the IAM & Admin console interface. On the left is a navigation menu with options like IAM, PAM, Organizations, and Service Accounts. The main area displays a table of IAM users. The table has columns for 'Allow', 'Deny', 'Recommendations history', and roles. The first user is '712347850871-compute@developer.gserviceaccount.com' with the role 'Compute Engine default service account' and 'Editor' permissions. The second user is 'admiral@qwiklabs-services-prod.iam.gserviceaccount.com' with the role 'Owner'. The third user is 'qwiklabs-gcp-02-3a7a72dd2ef8@qwiklabs-gcp-02-3a7a72dd2ef8.iam.gserviceaccount.com' with roles 'Qwiklabs User', 'Service Account', 'BigQuery Admin', 'Owner', and 'Storage Admin'. The fourth user is 'student-03-329c77797956@qwiklabs.net' with the role 'Viewer'. The fifth user is 'student-03-b8b41a615ae8@qwiklabs.net' with roles 'App Engine Admin', 'BigQuery Admin', 'Editor', 'Owner', and 'Viewer'.

Allow	Deny	Recommendations history	
<input type="checkbox"/>		712347850871-compute@developer.gserviceaccount.com	Compute Engine default service account Editor
<input type="checkbox"/>		admiral@qwiklabs-services-prod.iam.gserviceaccount.com	Owner
<input type="checkbox"/>		qwiklabs-gcp-02-3a7a72dd2ef8@qwiklabs-gcp-02-3a7a72dd2ef8.iam.gserviceaccount.com	Qwiklabs User Service Account BigQuery Admin Owner Storage Admin
<input type="checkbox"/>		student-03-329c77797956@qwiklabs.net	student 80fb9a4f Viewer
<input type="checkbox"/>		student-03-b8b41a615ae8@qwiklabs.net	App Engine Admin BigQuery Admin Editor Owner Viewer

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

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**.

Note: If you get a permissions error for bucket creation, sign out and then sign in back in with the Username 1 credentials.

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

Property	Value
Name:	<i>globally unique name (create it yourself!) and click CONTINUE.</i>
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**.

The screenshot displays the Google Cloud Storage 'Bucket details' page for a bucket named 'vinod-00'. The left sidebar shows navigation options like Overview, Buckets, Monitoring, Settings, and Storage Intelligence. The main content area shows bucket metadata: Location (us), Storage class (Standard), Public access (Not public), and Protection (Soft Delete). Below this is a tabbed interface with 'Objects' selected, showing a 'Folder browser' view with a single object 'vinod-00'. On the right, there are options to 'Create folder' and 'Upload', and a table header for object listing with columns: Name, Size, Type, Created, and Storage class. The table currently shows 'No rows to display'.

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**.

The screenshot shows the Google Cloud Storage 'Bucket details' page for a bucket named 'vinod-00'. The left sidebar contains navigation links: Overview, Buckets (selected), Monitoring, Settings, Storage Intelligence, Insights datasets, and Configuration. The main content area shows bucket metadata: Location (us), Storage class (Standard), Public access (Not public), and Protection (Soft Delete). Below this, the 'Objects' tab is active, displaying a 'Folder browser' with a sub-entry 'vinod-00'. On the right, there are buttons for 'Create folder' and 'Upload'. A table lists objects with columns for Name, Size, and Actions. One object is visible: 'Hosting a Web App on Google Clo...' with a size of 7 KB. A status bar at the bottom right shows 'Uploads and qwiklabs-gcp-02-3a7a... operations' with a completed upload of 'Hosting a Web App on Google Cloud Using Compute Engine.pdf'.

This screenshot shows the same Google Cloud Storage 'Bucket details' page for 'vinod-00', but with a 'Rename object' dialog box open in the foreground. The dialog box has a text input field labeled 'Object name *' containing the text 'sample.txt'. At the bottom of the dialog are 'Cancel' and 'Rename' buttons. The background interface is dimmed, showing the same bucket metadata and object list as the previous screenshot. The status bar at the bottom right remains the same, indicating a completed upload.

Verify project viewer access

1. Switch to the **Username 2** console.
2. From the Console, select **Navigation menu > Cloud Storage > Buckets**. Verify that this user can see the bucket.

Username 2 has the "Viewer" role prescribed which allows them read-only actions that do not affect state. This example illustrates this feature—they can view Cloud Storage buckets and files that are hosted in the Google Cloud project that they've been granted access to.

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**.

Note: You may have to widen the screen to see the pencil icon.

2. Remove Project Viewer access for **Username 2** by clicking the trashcan icon next to the role name. Then click **SAVE**.

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

Note: It can take up to 80 seconds for such a change to take effect as it propagates. Read more about Google Cloud IAM in the Google Cloud IAMResource Documentation, [Frequently asked questions](#).

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**.

You should see a permission error.

Note: As mentioned before, it can take up to 80 seconds for permissions to be revoked. If you haven't received a permission error, wait a 2 minutes and then try refreshing the console.

Cloud Storage

Overview

Buckets

Monitoring

Settings

Storage Intelligence

Insights datasets

Configuration

Marketplace

Release Notes

Buckets

Create Refresh

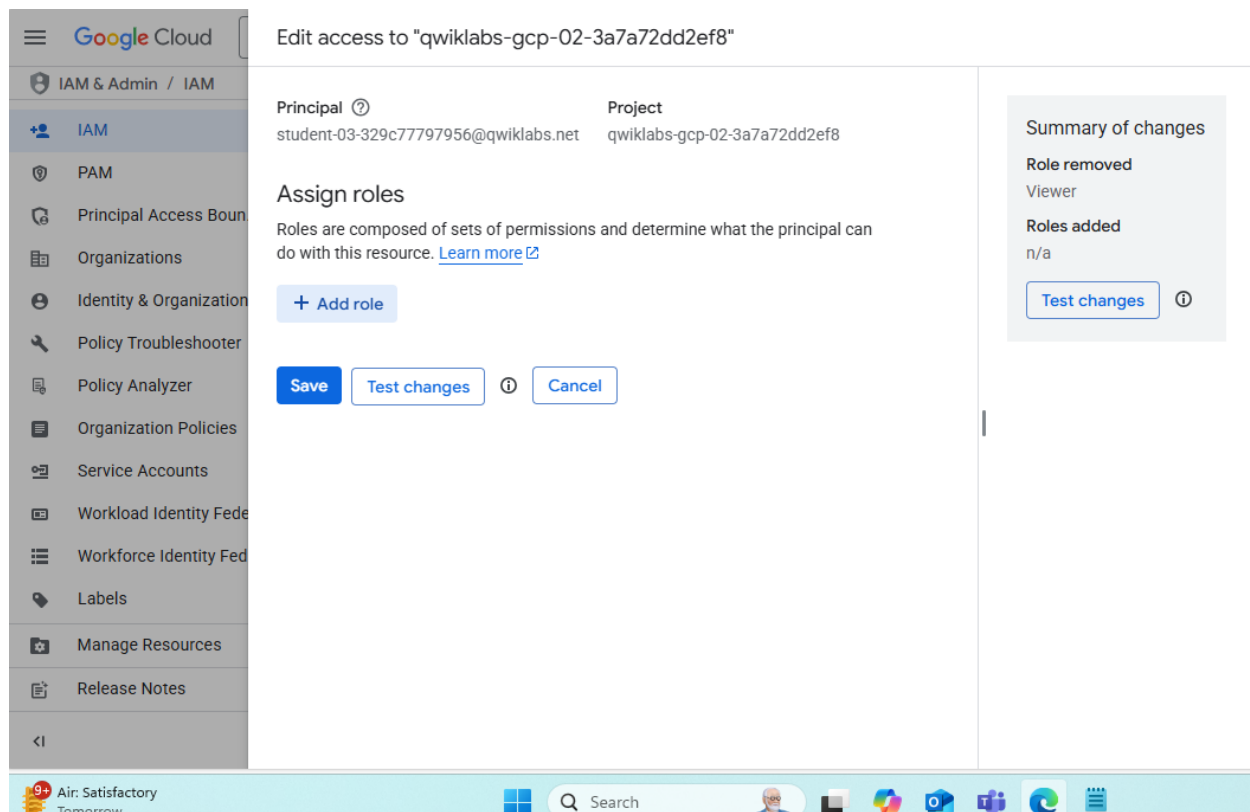
Go to path Learn

Filter Filter buckets

<input type="checkbox"/>	Name ↑	Created	Location type	Location	Default storage class ?	
<input type="checkbox"/>	vinod-00	May 6, 2025, 5:51:36 PM	Multi-region	us	Standard	

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]
```

Copied!

content_copy

You should receive a similar output:

```
gs://[YOUR_BUCKET_NAME]/sample.txt
```


Note: If you see `AccessDeniedException`, wait a minute and run the previous command again.

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

The screenshot displays the Google Cloud IAM & Admin console for the project "qwiklabs-gcp-02-3a7a72dd2ef8". The "Allow" tab is active, showing the "Permissions for project 'qwiklabs-gcp-02-3a7a72dd2ef8'". The table lists the following permissions:

Type	Principal	Name	Role	Sec
<input type="checkbox"/>	712347850871-compute@developer.gserviceaccount.com	Compute Engine	Editor	

A notification "Policy updated" is displayed. Below the console, the Cloud Shell terminal shows the command `gsutil ls gs://vinod-00` being executed, resulting in the output `gs://vinod-00/sample.txt`.