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.

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:

Role Name	**Permissions**
roles/viewer	Permissions for read-only actions that do not affect state, such as viewing (but not modifying) existing resources or data.
roles/editor	All viewer permissions, plus permissions for actions that modify state, such as changing existing resources.
roles/owner	All editor permissions and permissions for the following actions: Manage roles and permissions for a project and all resources within the project. Set up billing for a project.

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.

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:	*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**.

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

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**.

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.

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.