

Cloud IAM: Qwik Start | Google Cloud Skills Boost

Qwiklabs : 11-14 minutes

GSP064



Google Cloud Self-Paced Labs

Overview

Google Cloud's Identity and Access Management (IAM) service lets you create and manage permissions for Google Cloud resources. Cloud IAM unifies access control for Google Cloud services into a single system and provides a consistent set of operations.

In this hands-on lab you learn how to assign a role to a second user and remove assigned roles associated with Cloud IAM. More specifically, you sign in with 2 different sets of credentials to experience how granting and revoking permissions works from Google Cloud Project Owner and Viewer roles.

Prerequisites

This is an **introductory level** lab. Little to no prior knowledge of Cloud IAM is expected. Experience with Cloud Storage is helpful to complete the tasks in this lab, but is not required. Make sure that you have a file in .txt or .html available. If you are looking for more advanced practice with Cloud IAM, be sure to check out the following Google Cloud Skills Boost lab, [IAM Custom Roles](#).


Once you're prepared, scroll down and follow the steps to get your lab environment set up.

Setup for two users

As mentioned earlier, this lab provides two sets of credentials to illustrate IAM policies and what permissions are available for specific roles.

In the **Lab Connection** panel on the left side of your lab, you see a list of credentials that resembles the following:

Student Resources

 **Manage Access Control with Google Cloud IAM**

[Open Google Console](#)

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. [Learn more.](#)

Username 1
google2727295_student@qwiklabs.net

Username 2
googleuser1632_student@qwiklabs.net

Password
xfmcRbn2Kvy

GCP Project ID
qwiklabs-gcp-e48562778bbebc76

[New to labs? View our introductory video!](#)

Notice that there are two usernames: Username 1 and Username 2. These represent identities in Cloud IAM, each with different access permissions allocated to them. These "roles" set constraints on what you can and cannot do with Google Cloud resources in the project you've been allocated.

Sign in to Cloud Console as the first user

1. Click on the **Open Google Console** button. This opens a new browser tab. If you are asked to **Choose an account**, click **Use another account**.
2. The Google Cloud sign in page opens. A Sign in page opens—copy and paste the **Username 1** credential that resembles `googlexxxxxx_student@qwiklabs.net` into the "Email or phone" field and then click **Next**.
3. Copy the password from the **Lab Connection** panel and paste into the Google Sign in password field.
4. Click **Next** and then **Accept** the terms of service. The Cloud Console opens. Agree to the terms of service and click **Agree and Continue**.

Sign in to Cloud Console as the second user

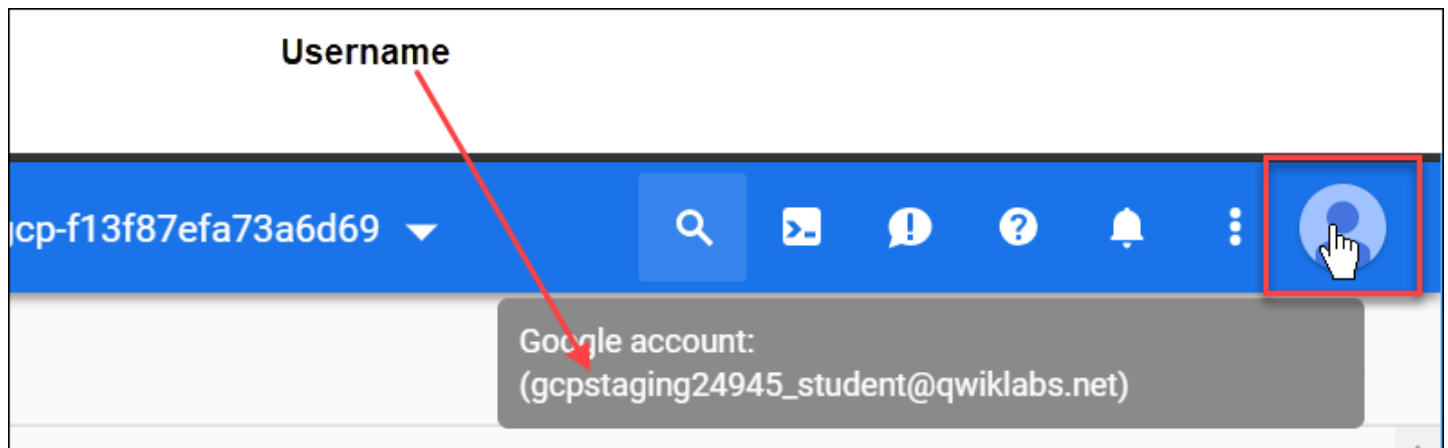
1. Click on the **Open Google Console** button again. A new browser tab opens, if you are asked to **Choose an account**, click **Use another account**.
2. The Google Cloud sign in page opens. Copy and paste the **Username 2** credential that resembles `googlexxxxxx_student@qwiklabs.net` into the **Email or phone** field and then click **Next**.
3. Copy the password from the **Lab Connection** panel and paste into the Google Sign in password field.
4. Click **Next** and then **Accept** the terms of service. The Cloud Console opens. Agree to the terms of service and click **Agree and Continue**.

You should now have two Cloud Console tabs open in your browser—one signed in with Username 1 and the other with Username 2.

View or reset the user in a browser tab

Occasionally, a user is overwritten in a browser tab or you may be confused about which user is signed into which browser tab.

To view which user is signed into a browser tab, hover over your Avatar to view your username in that browser tab.



To reset which user is signed into a browser tab:

1. Click your Avatar and click **Sign out** to sign out.
2. In the **Lab Connection** panel, click **Open Google Console** and sign in back using the appropriate Username and Password.

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** and mouse over.

There are four roles:

- Browser
- 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.

All editor permissions and permissions for the following actions:

roles/owner

- Manage roles and permissions for a project and all resources within the project.
- Set up billing for a project.

roles/browser Read access to browse the hierarchy for a project, including the folder, organization, and Cloud IAM policy. This role doesn't include permission to view resources in the 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 editor roles

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.

Prepare a resource 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**.

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**.

Click **Check my progress** to verify the objective.

Create a bucket and upload a sample file

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.

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 IAM Resource 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.

Click **Check my progress** to verify the objective.

Remove project access

Add 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]
```

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.

Click **Check my progress** to verify the objective.

Add Storage permissions

Congratulations!

In this lab you exercised granting and revoking Cloud IAM roles to a user.

Finish your Quest

This self-paced lab is part of the **Security & Identity Fundamentals**, **Baseline: Infrastructure**, and **Cloud Engineering** quests. A quest is a series of related labs that form a learning path. Completing this quest earns you a badge to recognize your achievement. You can make your badges public and link to them in your online resume or social media account. Enroll in a quest and get immediate completion credit if you've taken this lab. See the [Google Cloud Skills Boost catalog](#) for other available quests.

Next steps / Learn more

This lab is also part of a series of labs called Qwik Starts. These labs are designed to give you a little taste of the many features available with Google Cloud. Search for "Qwik Starts" in the [Google Cloud Skills Boost catalog](#) to find the next lab you'd like to take!

Google Cloud training and certification

...helps you make the most of Google Cloud technologies. [Our classes](#) include technical skills and best practices to help you get up to speed quickly and continue your learning journey. We offer fundamental to advanced level training, with on-demand, live, and virtual options to suit your busy schedule. [Certifications](#) help you validate and prove your skill and expertise in Google Cloud technologies.

Lab last tested October 3, 2022

Lab last tested October 3, 2022

Copyright 2023 Google LLC All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.