www.cloudskillsboost.google /course_sessions/3777998/labs/375043

Securing and Sharing BigQuery Datasets and Tables | Google Cloud Skills Boost

Qwiklabs : 12-16 minutes

Overview

In Google Cloud, permissions are not assigned directly to users, groups, or service accounts. Instead, users, groups, or service accounts are granted access to basic, predefined, or custom Identity and Access Management (IAM) roles to give them permissions to perform actions on specific Google Cloud resources such as BigQuery. There are many predefined IAM roles for BigQuery that can be granted at various levels of the resource hierarchy including at the Google Cloud project level and the BigQuery dataset level.

A predefined IAM role can provide different permissions depending on which level of the Google Cloud hierarchy it is applied. For example, when applied at the BigQuery dataset level, the role of BigQuery data editor provides the ability to create, update, and delete the tables in the dataset. When the same role is applied at the Google Cloud project level, it provides the ability to create new BigQuery datasets in the project. Depending on your organization's needs and requirements, you can choose which roles to apply at which level of the Google Cloud hierarchy for any individual user, group, or service account to control access to BigQuery resources.

In this lab, you work in a simulated enterprise environment that has two Google Cloud projects and two users: one user with full access (project owner) on Project 1 and another user with limited access (project viewer) in Project 2. Using the two Google Cloud projects, you explore and test access to the Google Cloud projects and grant access to specific BigQuery datasets using predefined IAM roles.

Objectives

In this lab, you learn how to:

- Explore and test user access to Google Cloud projects and BigQuery data.
- Create a BigQuery dataset and table.
- Share a BigQuery dataset using predefined IAM roles.

Setup and requirements

Note: It can take 3 - 5 minutes for the lab environment to auto-generate two Google Cloud Projects and two user accounts.

Note: Once started, the lab cannot be paused, and ending the lab will delete all student projects that are running.

For each lab, you get a new Google Cloud project and set of resources for a fixed time at no cost.

1. Sign in to Qwiklabs using an **incognito window**.

2. Note the lab's access time (for example, `1:15:00`), and make sure you can finish within that time.
   There is no pause feature. You can restart if needed, but you have to start at the beginning.

3. When ready, click **Start lab**.

4. Note your lab credentials (**Username** and **Password**). You will use them to sign in to the Google Cloud Console.

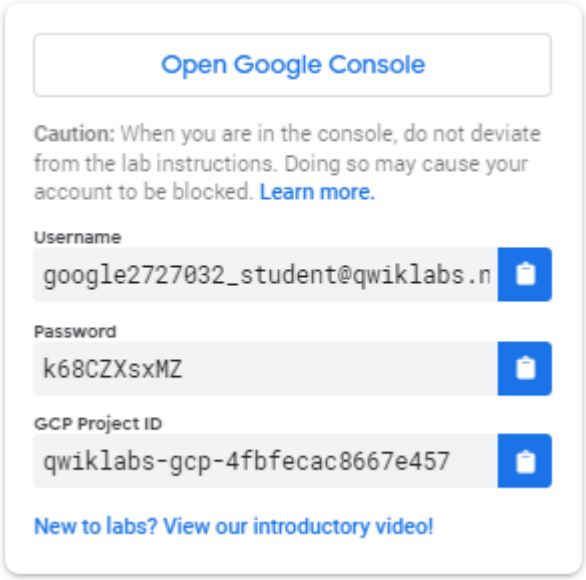
5. Click **Open Google Console**.

6. Click **Use another account** and copy/paste credentials for **this** lab into the prompts.
   If you use other credentials, you'll receive errors or **incur charges**.

7. Accept the terms and skip the recovery resource page.

How to start your lab and sign in to the Console

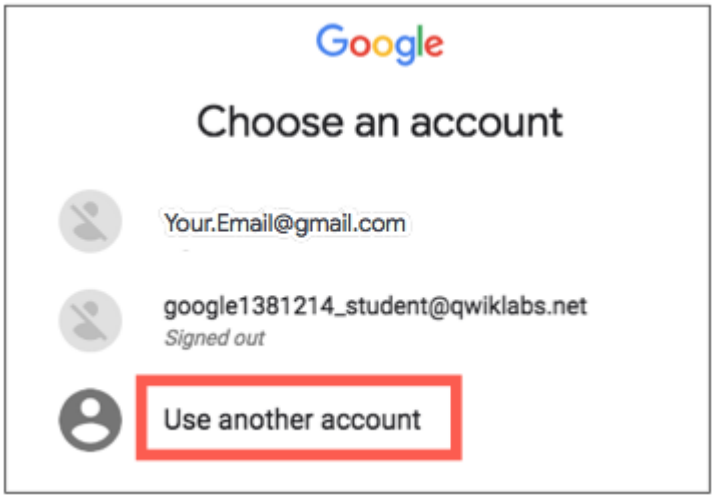
1. Click the **Start Lab** button. If you need to pay for the lab, a pop-up opens for you to select your payment method. On the left is a panel populated with the temporary credentials that you must use for this lab.



2. Copy the username, and then click **Open Google Console**. The lab spins up resources, and then opens another tab that shows the **Choose an account** page.

   Note: Open the tabs in separate windows, side-by-side.

3. On the Choose an account page, click **Use Another Account**. The Sign in page opens.



4. Paste the username that you copied from the Connection Details panel. Then copy and paste the password.

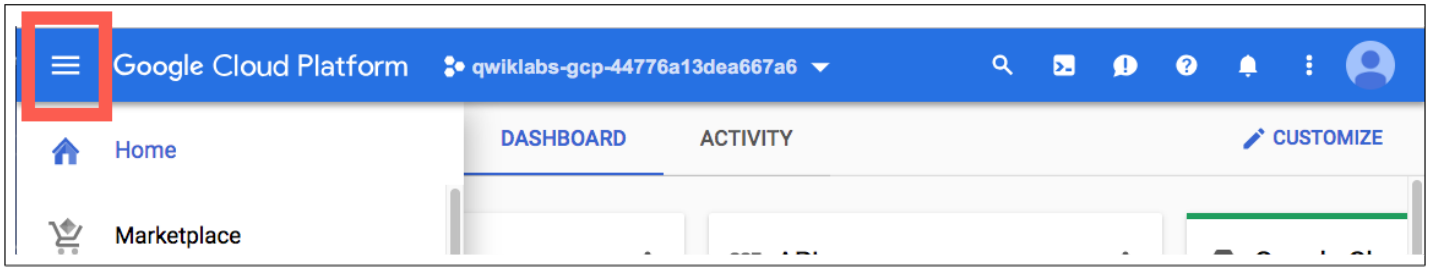
Note: You must use the credentials from the Connection Details panel. Do not use your Google Cloud Skills Boost credentials. If you have your own Google Cloud account, do not use it for this lab (avoids incurring charges).

5. Click through the subsequent pages:

- Accept the terms and conditions.
- Do not add recovery options or two-factor authentication (because this is a temporary account).
- Do not sign up for free trials.

After a few moments, the Cloud console opens in this tab.

Note: You can view the menu with a list of Google Cloud Products and Services by clicking the **Navigation menu** at the top-left.

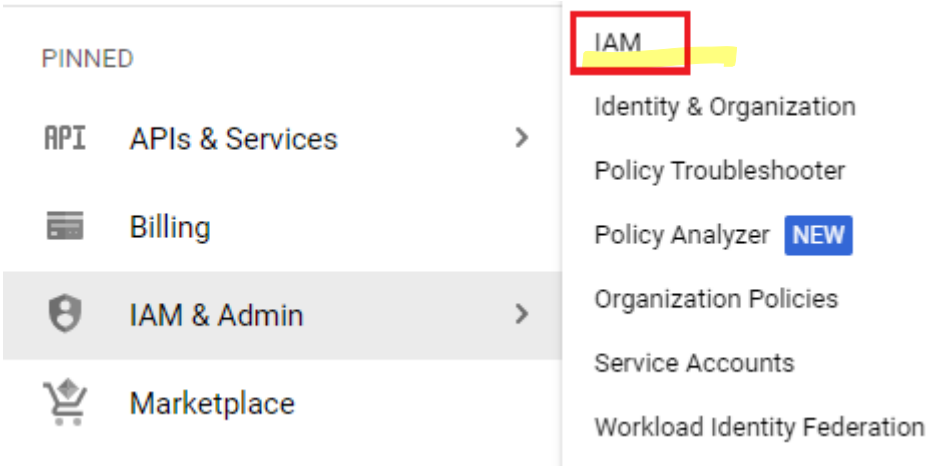


Task 1. Confirm User 1 access to the Project 1

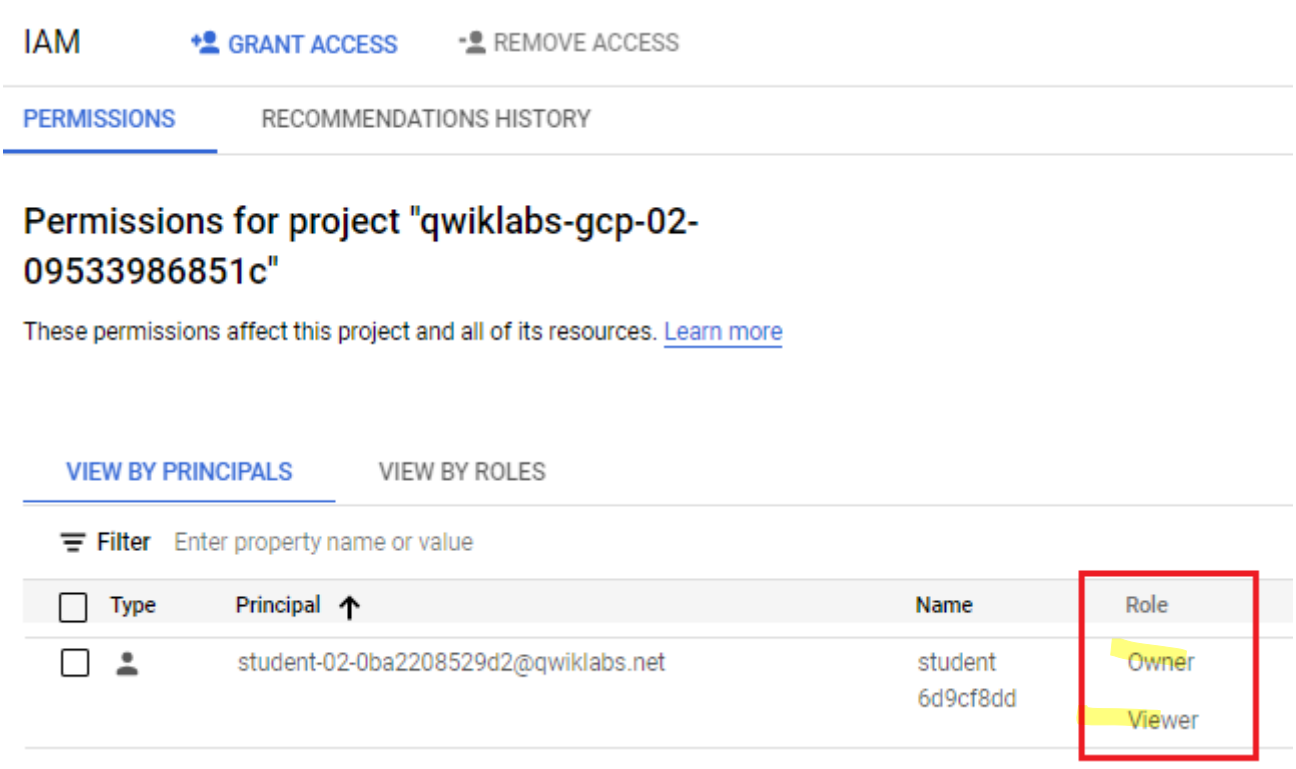
In this task, you work in Project 1 () to explore the permissions of User 1 in Project 1. Be sure that you log in to this project using the credentials for User 1 ().

1. In a new Incognito window, click **Open Google Console** for Project 1 (), and log in using the credentials for User 1 ().

2. In the Google Cloud console, in the **Navigation menu** (☰), click **IAM & Admin** > **IAM**.

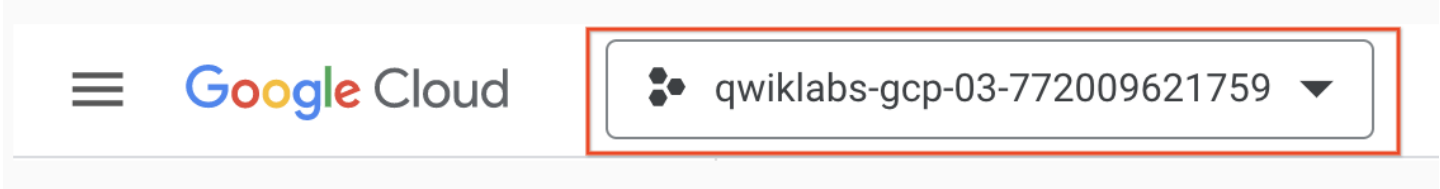


The IAM page displays permissions at the project level for all principals (users). As a project owner, User 1 can access and modify IAM permissions in Project 1.



Note: As User 1, you are a project owner of Project 1. Check that you see the Owner role.

3. At the top of the Google Cloud console, click on the **Select a Project** dropdown menu to see a list of projects that User 1 is logged into.



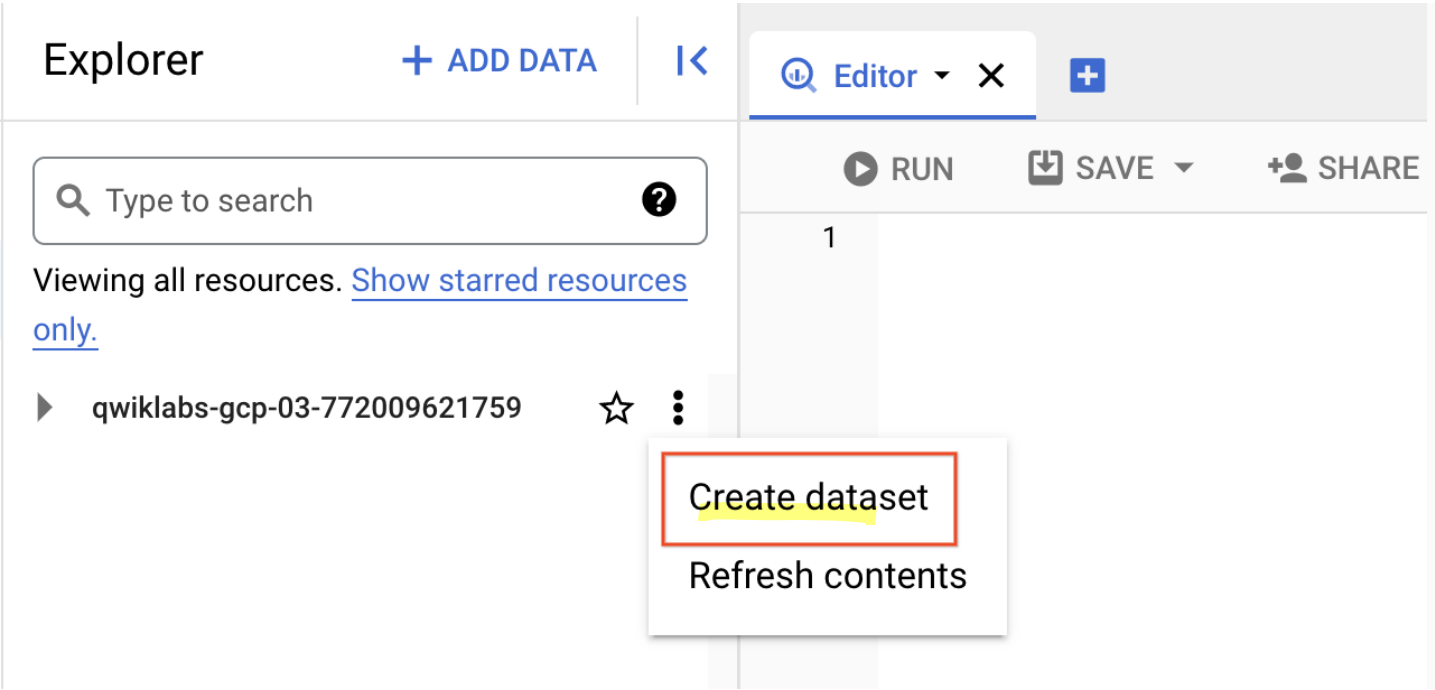
The drop-down menu will show the project ID for Project 1 in the drop-down menu: .

Task 2. Create a BigQuery dataset and table in Project 1

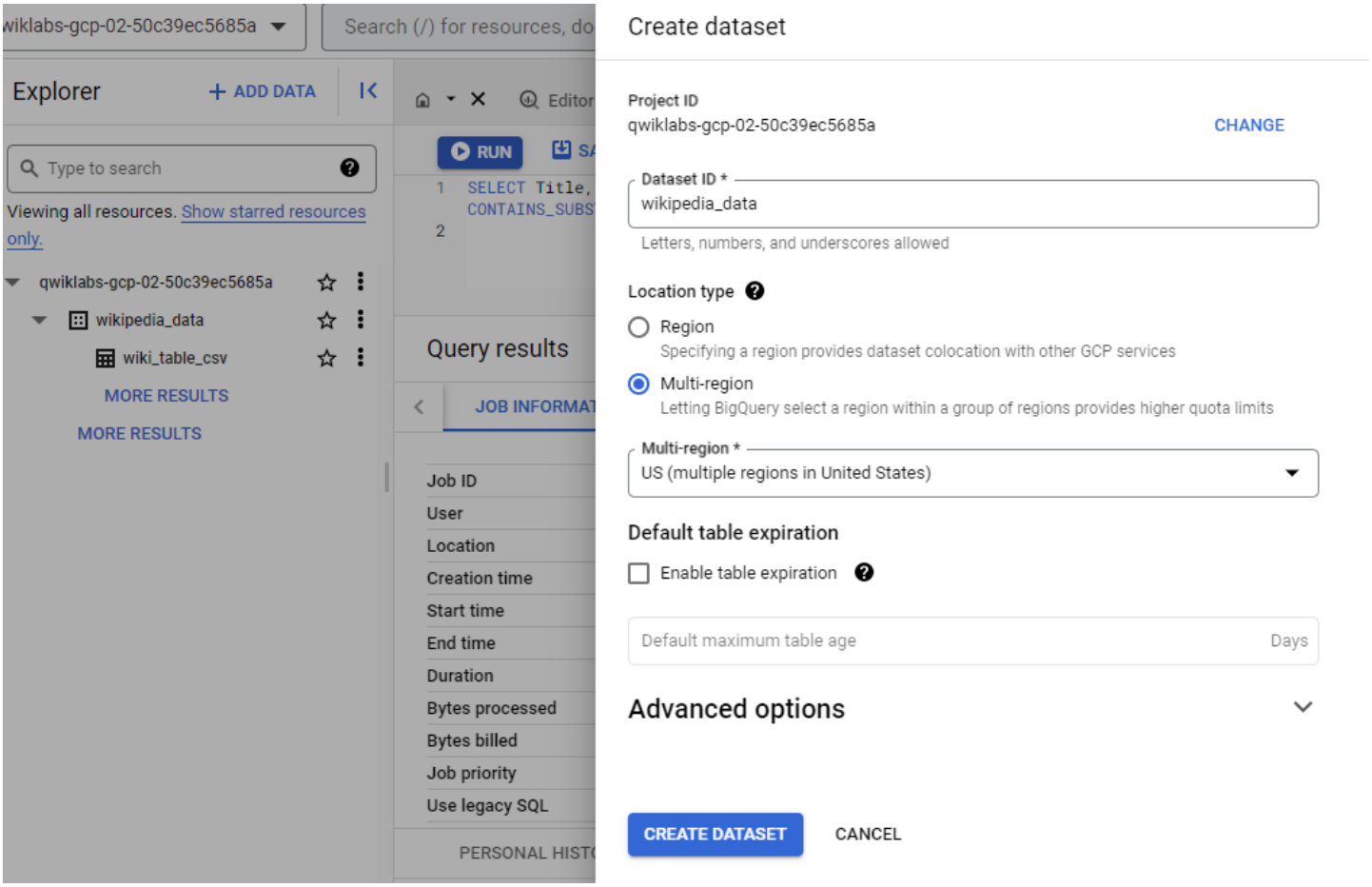
In this task, you continue to work in Project 1 () as User 1 to create a new BigQuery dataset and table. Be sure that you remain logged into this project using the credentials for User 1 ().

Create a dataset

1. In the Google Cloud console, in the **Navigation menu** (☰), under Analytics, click **BigQuery**. When prompted click **Done**.
2. In the Explorer pane (left side pane), click **View Action** (three vertical dots) next to your Project ID, and select **Create dataset**.



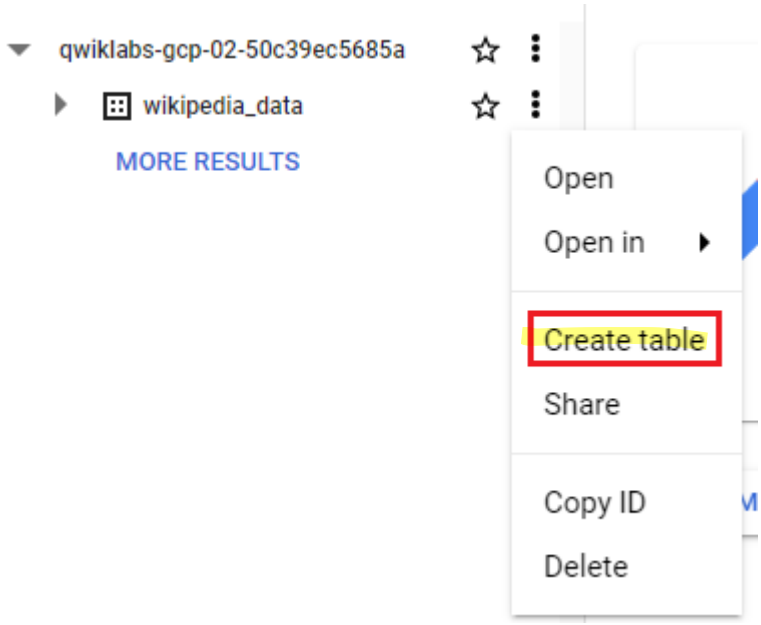
3. For **Dataset ID**, type: **wikipedia_data**
4. For **Location type**, select **Multi-region** and **US (multiple regions in United States)**.



5. Click **Create dataset**.

Create a table

1. In the Explorer pane, click **View Action** (three vertical dots) next to **wikipedia_data**, and select **Create table**.



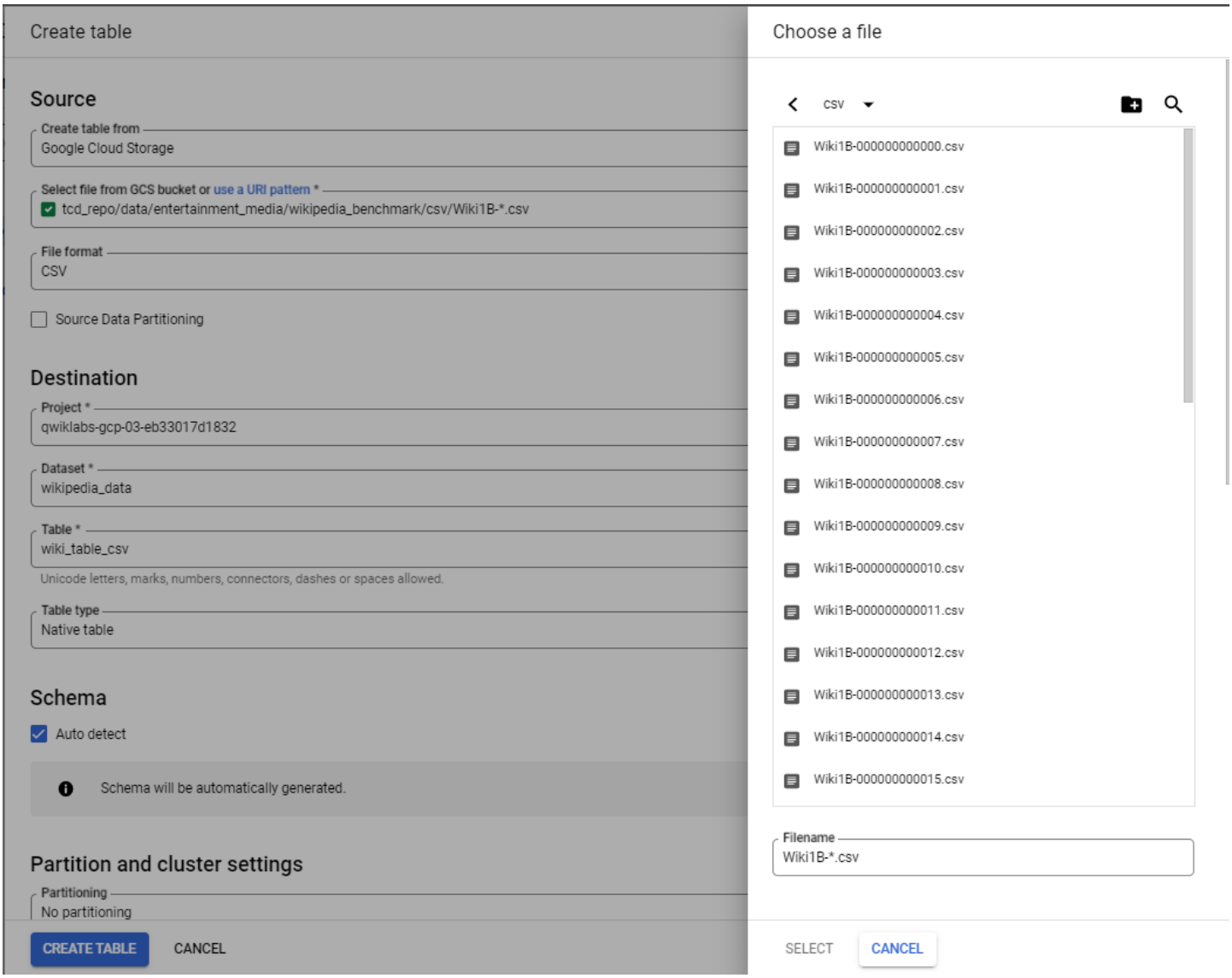
2. For **Create table from**, select **Google Cloud Storage**.

3. For **Select file from GCS bucket**, type: **tcd_repo/data/entertainment_media/wikipedia_benchmark/csv/Wiki1B-*.csv**

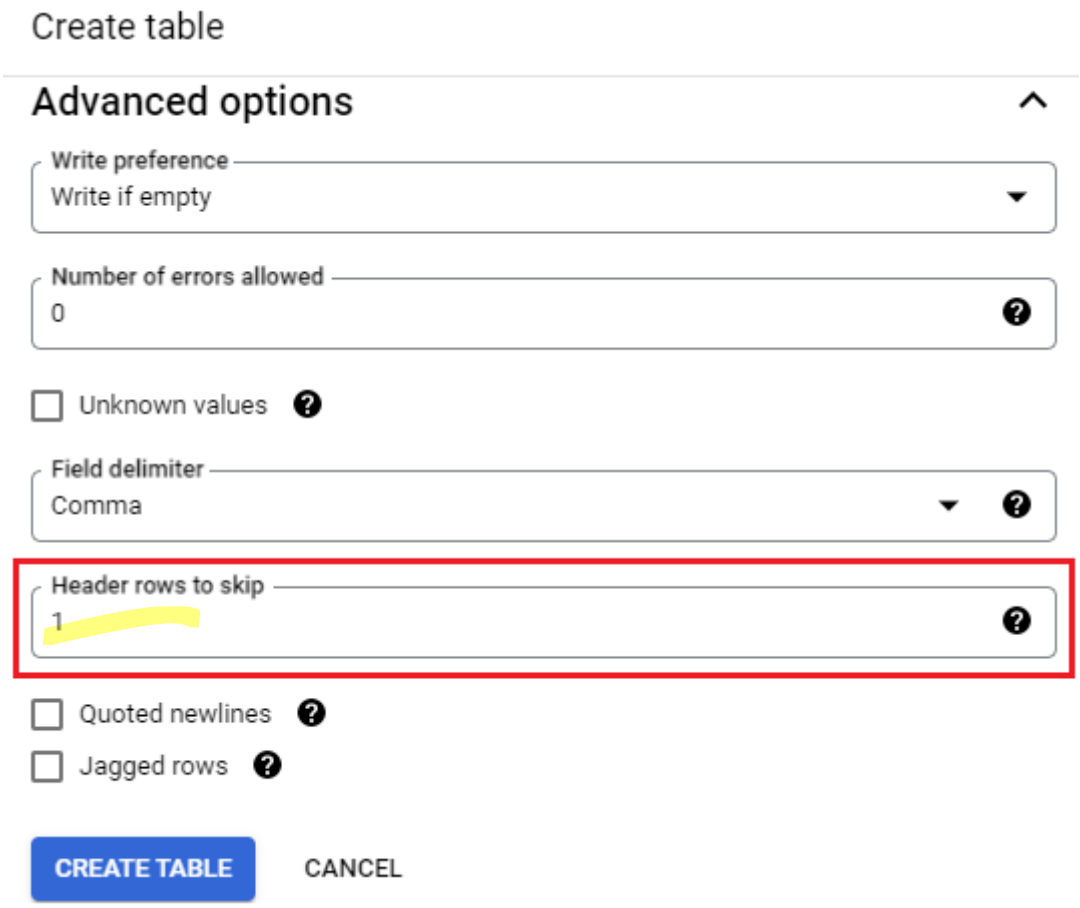
The file format will update to CSV.

Note: Notice the asterisk (`*`) in the file pattern. There is approximately a gigabyte (GB) of data that will be imported from multiple CSV files into the new table.

4. For **Project**, leave the default value ().
5. For **Dataset**, leave the default value (**wikipedia_data**).
6. For **Table**, type: **wiki_table_csv**
7. For **Table type**, leave the default value (**Native table**).
8. In the Schema section, enable the **Auto detect** checkbox.



9. Expand the **Advanced options** section.
10. For **Header rows to skip**, type **1**



11. Click **Create Table**.

Run a query on the loaded data

1. In the query editor, copy and paste the following query, and click **Run**.

```
SELECT Title, COUNT(views) AS views FROM wikipedia_data.wiki_table_csv WHERE CONTAINS_SUBSTR(title, 'GOOGLE') GROUP BY Title ORDER BY views DESC LIMIT 100;
```

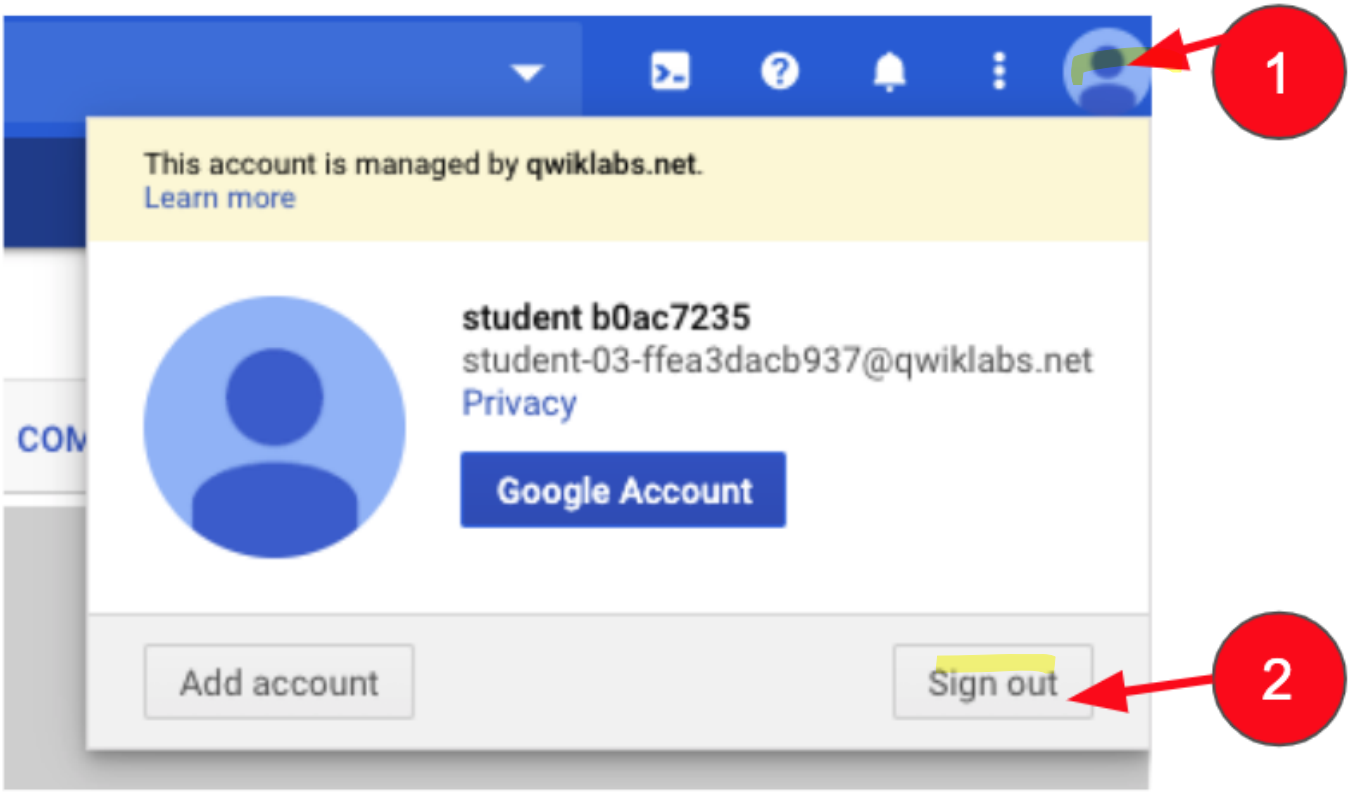
Using the newly populated data, this query counts the number of views for Wikipedia articles with "GOOGLE" in the title.

Click **Check my progress** to verify the objective. Create BigQuery dataset and table

Sign out of Project 1

1. Click on the profile icon on the top right of the Google Cloud console.
2. Click **Sign out**.

If asked to confirm, click **Leave**.



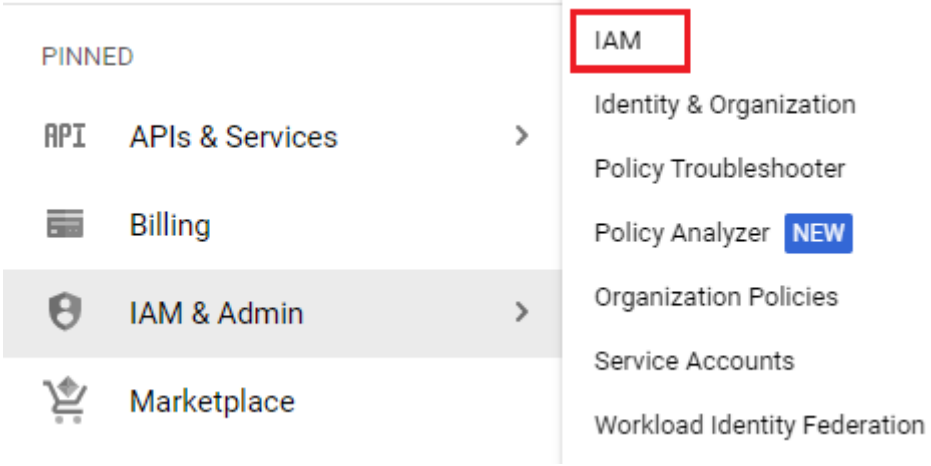
Task 3. Log into Project 2 as User 2 to confirm restricted project access

In this task, you work in Project 2 () to explore the permissions for User 2 in Project 2. Be sure that you log in to this project using the credentials for User 2 ().

1. In a new Incognito window, click **Open Google Console** for Project 2 (), and log in using the credentials for User 2 ().
2. At the top of the Google Cloud console, click on the **Select a Project** dropdown menu to see a list of projects that User 2 is logged into.

The drop-down menu will show the project ID for Project 2 in the drop-down menu: .

3. In the Google Cloud console, in the **Navigation menu** (☰), click **IAM & Admin** > **IAM**.



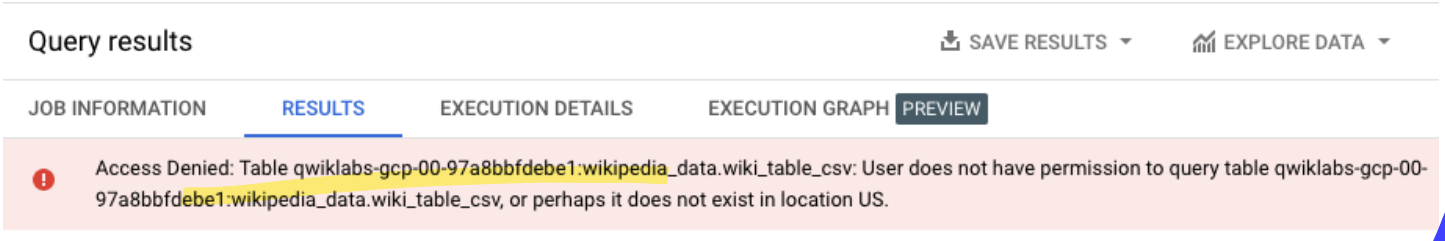
User 2 () is a project viewer in Project 2. As a project viewer in Project 2, User 2 can run query jobs on BigQuery data stored in Project 2 or in any other project as long as the user has been given access to the data in the other project.

Task 4. Run a query in Project 2 to confirm restricted data access

In this task, you continue to work in Project 2 () as User 2 () to test your access to the BigQuery data in Project 1. Be sure that you remain logged into this project using the credentials for User 2 ().

1. In the Google Cloud console, in the **Navigation menu** (☰), under Analytics, click **BigQuery**. When prompted click **Done**.
2. In the query editor, run the following query, replacing `ProjectID` with the Project 1 ID () to specify the project that hosts the data:

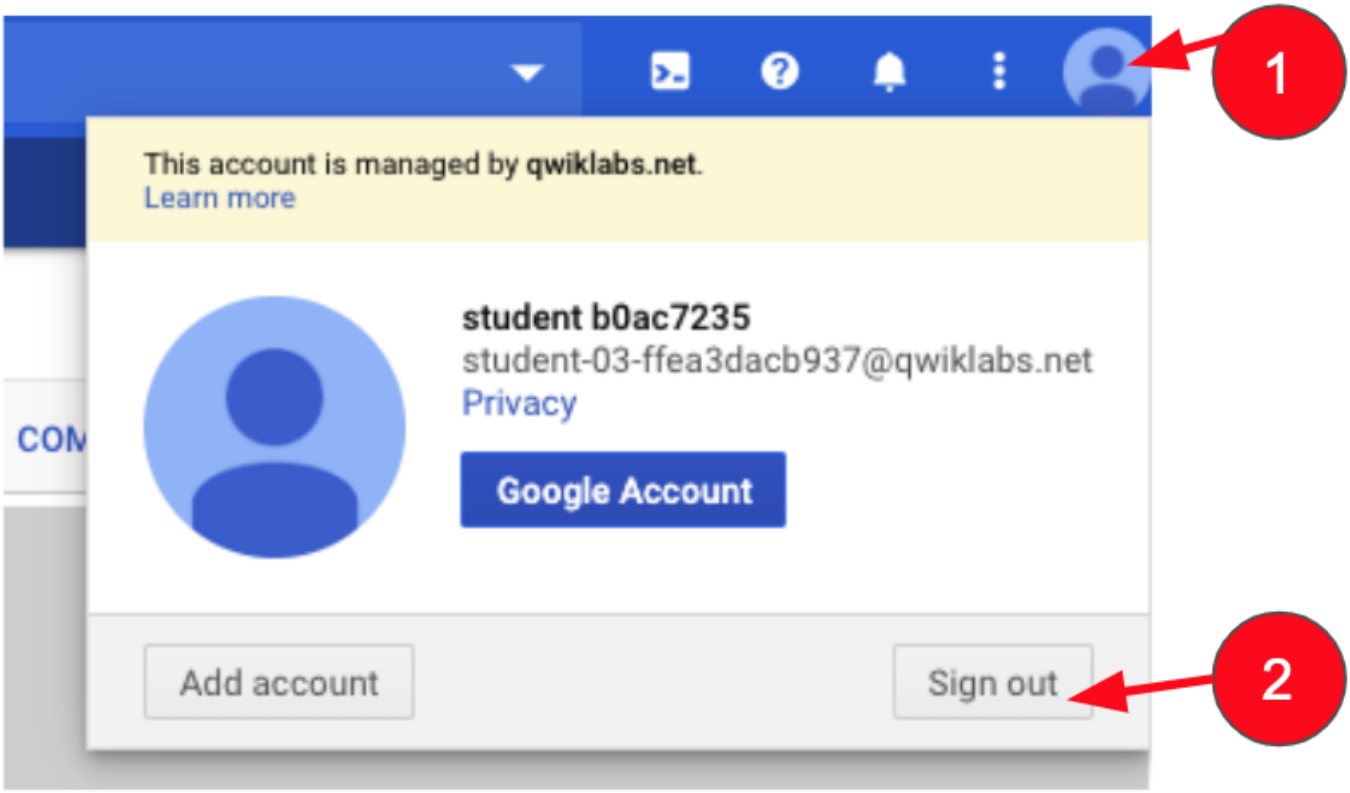
SELECT Title, COUNT(views) AS views FROM `ProjectID.wikipedia_data.wiki_table_csv` WHERE CONTAINS_SUBSTR(title, 'GOOGLE') GROUP BY Title ORDER BY views DESC LIMIT 100; **Note:** In BigQuery, even if a project is not pinned or visible in your Explorer pane, you can still query BigQuery data if you have been granted access to that data. In this case, User 2 is not able to query the data created by User 1 in Project 1 because User 2 has not been granted access to the data. The error message states that access to the data is denied.



Sign out of project 2

1. Click on the profile icon on the top right of the Google Cloud console.
2. Click **Sign out**.

If asked to confirm, click **Leave**.



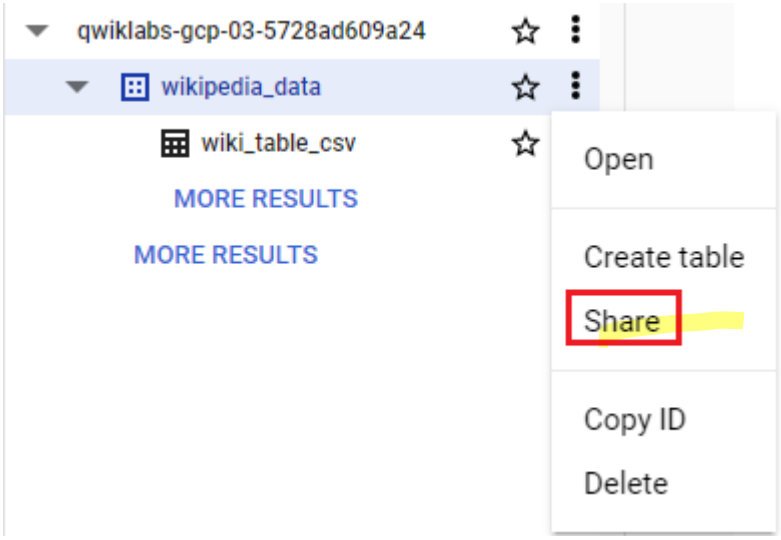
Task 5. Grant access to User 2 on the Project 1 data

You can assign BigQuery roles to users that do not have access to the Google Cloud project that hosts the data. This flexibility makes it easy to control and customize the level of access provided to any user, group, or service account because users can run queries in their own projects on only the specific data that they have been granted access to, even if that is hosted in other Google Cloud projects.

In this task, you return to work in Project 1 () to grant access to User 2 on the Project 1 dataset. Be sure that you log in to this project using the credentials for User 1 ().

Using the Google Cloud console, you assign the BigQuery data editor role on the dataset named **wikipedia_data** in Project 1 to User 2.

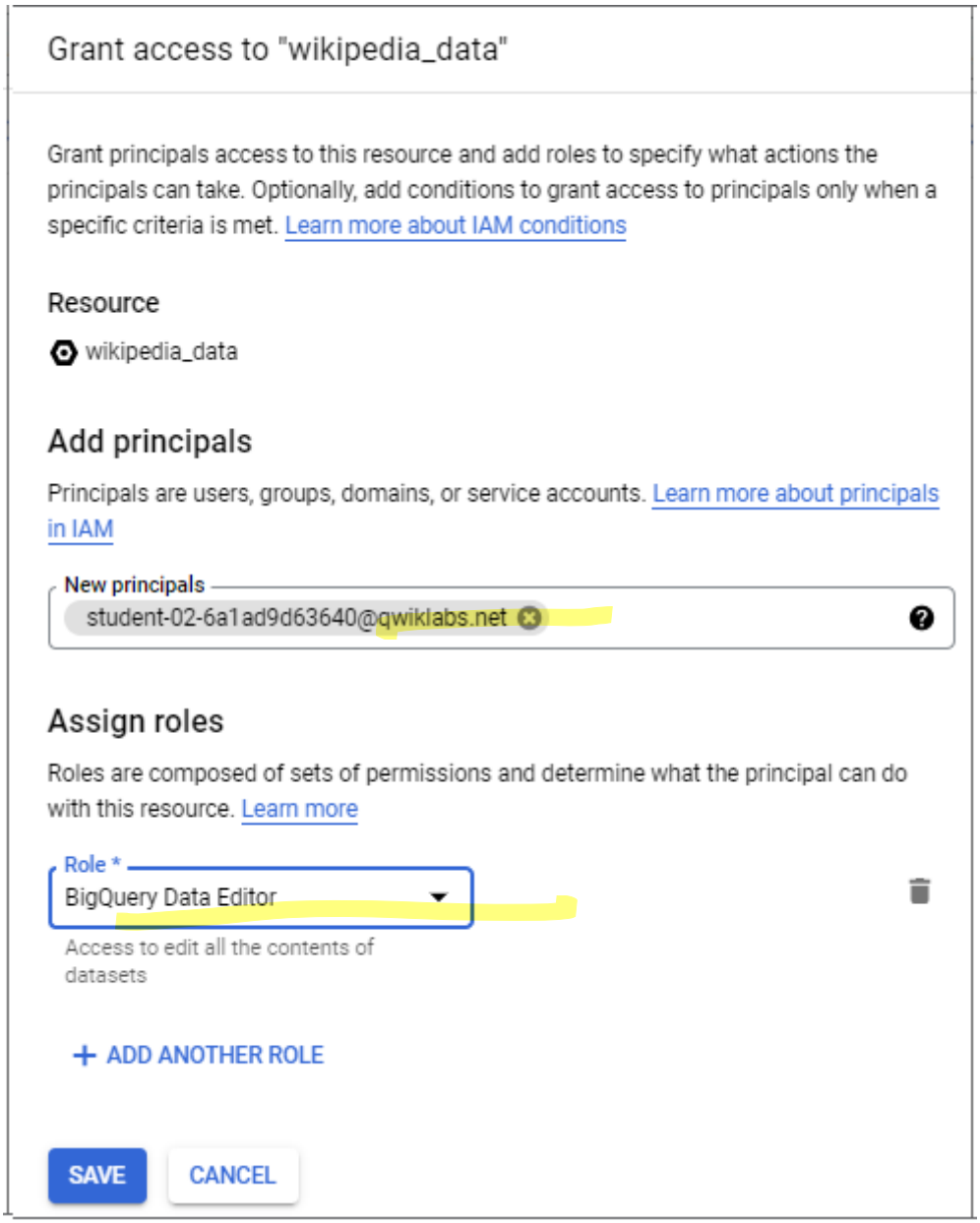
1. In a new Incognito window, click **Open Google Console** for Project 1 (), and log in using the credentials for User 1 ().
2. In the Google Cloud console, in the **Navigation menu** (☰), under Analytics, click **BigQuery**.
3. In the Explorer pane, click **View Action** (three vertical dots) next to **wikipedia_data**, and select **Share**.



4. Click **Add principal**.

5. For **New principals**, enter the email for User 2:

6. For **Select a role**, select **BigQuery Data Editor** under **BigQuery**.



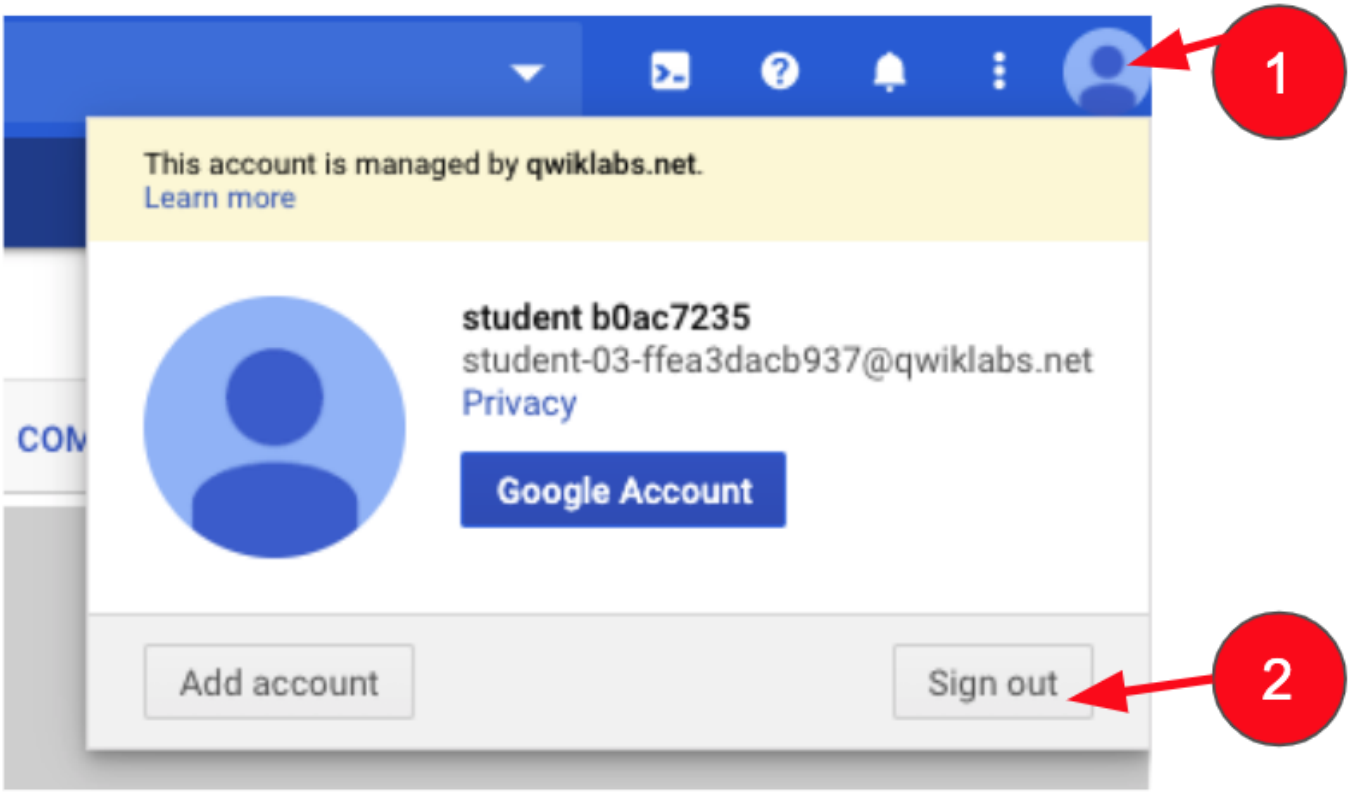
7. Click **Save**.

Click **Check my progress** to verify the objective. Assign BigQuery data editor role to User 2

Sign out of project 1

1. Click on the profile icon on the top right of the Google Cloud console.
2. Click **Sign out**.

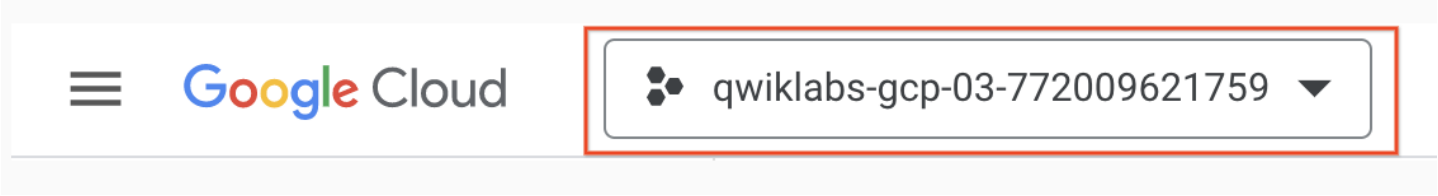
If asked to confirm, click **Leave**.



Task 6. Run query as User 2 in Project 2 to confirm access

For this task, you return to work in Project 2 () to test the data access that was granted to User 2. Be sure that you log in to this project using the credentials for User 2 ().

1. In a new Incognito window, click **Open Google Console** for Project 2 (), and log in using the credentials for User 2 ().
2. At the top of the Google Cloud console, click on the **Select a Project** dropdown menu to see a list of projects that User 2 is logged into.



Notice that as User 2, you can still only see Project 2 because you were not granted access to Project 1. User 2 was only granted access to the BigQuery dataset in Project 1, not the actual project.

3. In the query editor, run the following query, replacing `ProjectID` with the Project 1 ID () to specify the project that hosts the data:

```
SELECT Title, COUNT(views) AS views FROM `ProjectID.wikipedia_data.wiki_table_csv` WHERE CONTAINS_SUBSTR(title, 'GOOGLE') GROUP BY Title ORDER BY views DESC LIMIT 100;
```

As User 2, you can now successfully run the query on the BigQuery dataset in Project 1. Assigning the role of BigQuery data editor on the BigQuery dataset allows User 2 to run queries on the tables in the BigQuery dataset (and more actions including creating, modifying, and deleting tables), even though User 2 does not have direct access to Project 1.

Click **Check my progress** to verify the objective. Run query on Project 1 data as User 2 in Project 2

End your lab

When you have completed your lab, click **End Lab**. Google Cloud Skills Boost removes the resources you've used and cleans the account for you.

You will be given an opportunity to rate the lab experience. Select the applicable number of stars, type a comment, and then click **Submit**.

The number of stars indicates the following:

- 1 star = Very dissatisfied
- 2 stars = Dissatisfied
- 3 stars = Neutral
- 4 stars = Satisfied
- 5 stars = Very satisfied

You can close the dialog box if you don't want to provide feedback.

For feedback, suggestions, or corrections, please use the **Support** tab.