Implementing Security in Dataplex

Overview

This project focused on implementing and testing security features in **Google Cloud Dataplex**, an intelligent data fabric that enables centralized management, monitoring, and governance of data across data lakes, warehouses, and marts.

We explored **Dataplex IAM-based access control** by assigning roles at different levels (lake, zone, asset) and verifying the access permissions through user simulation.

Objectives

- Create Dataplex resources (lake, zone, asset).
- Assign IAM roles for fine-grained security.
- Test read-only and write permissions using different user roles.
- Upload a file to a Dataplex-managed Cloud Storage bucket using an appropriately authorized user.

Task 1. Create a lake, zone, and asset in Dataplex

To apply and test user access to Dataplex resources, you first need to create some Dataplex resources.

In this task, you use the Google Cloud console to create a new Dataplex lake to store customer information, add a raw zone to the lake, and then attach a pre-created Cloud Storage bucket as a new asset in the zone.

To complete this task, **be sure you are logged in as User 1 (____)**, who is a Dataplex Administrator and can create new Dataplex resources in the project.

Create a lake

1. In the Google Cloud Console, in the **Navigation menu** (☰), navigate to **Analytics** > **Dataplex**.

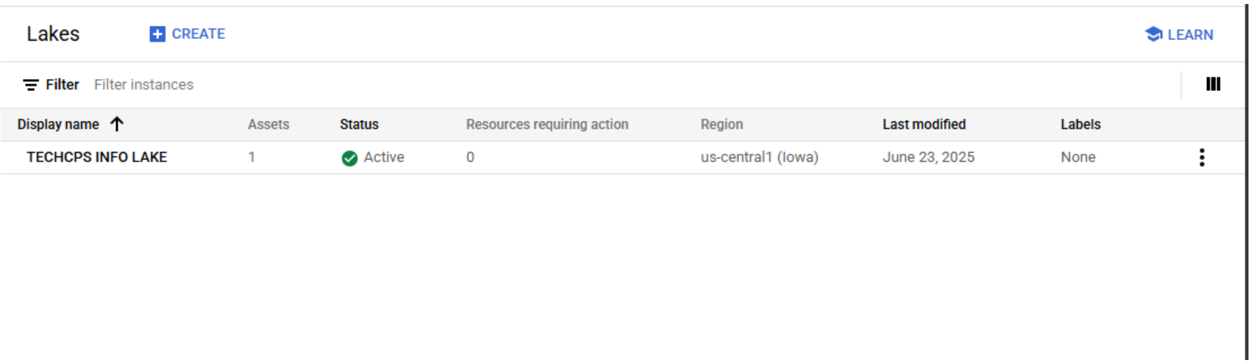
   If prompted Welcome to the new Dataplex experience, click **Close**.

2. Under **Manage lakes**, click **Manage**.
3. Click **Create lake**.
4. Enter the required information to create a new lake:

Property	**Value**
Display Name	Customer Info Lake
ID	Leave the default value.
Region	____

Leave the other default values.

5. Click **Create**.



Display name ↑	Assets	Status	Resources requiring action	Region	Last modified	Labels
TECHCPS INFO LAKE	1	✓ Active	0	us-central1 (Iowa)	June 23, 2025	None

Add a zone to the lake

1. On the **Manage** tab, click on the name of your lake.

2. Click **Add zone**.

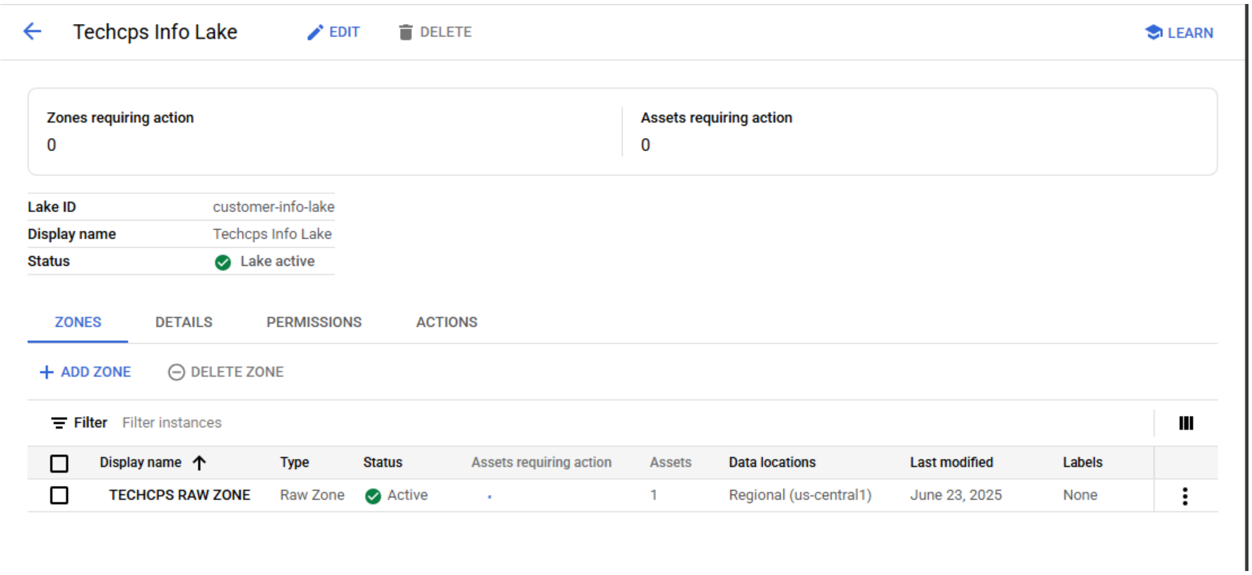
3. Enter the required information to create a new zone:

Property	**Value**
Display Name	Customer Raw Zone
ID	Leave the default value.
Type	**Raw zone**
Data locations	**Regional**

Leave the other default values.

For example, the option for **Enable metadata discovery** under **Discovery settings** is enabled by default and allows authorized users to discover the data in the zone.

4. Click **Create**.



Techcps Info Lake

Zones requiring action
0

Assets requiring action
0

Lake ID	customer-info-lake
Display name	Techcps Info Lake
Status	✓ Lake active

☐	Display name ↑	Type	Status	Assets requiring action	Assets	Data locations	Last modified	Labels
☐	TECHCPS RAW ZONE	Raw Zone	✓ Active	·	1	Regional (us-central1)	June 23, 2025	None

Attach an asset to a zone

1. On the **Zones** tab, click on the name of your zone.
2. On the **Assets** tab, click **Add assets**.
3. Click **Add an asset**.
4. Enter the required information to attach a new asset:

Property	**Value**
Type	**Storage bucket**
Display Name	Customer Online Sessions
ID	Leave the default value.
Bucket name	_____-bucket

Leave the other default values.

While the Cloud Storage bucket does not contain any files, you can attach it to the zone now, and newly added files will automatically be integrated into the zone.

5. Click **Done**.
6. Click **Continue**.
7. For **Discovery settings**, select **Inherit** to inherit the Discovery settings from the zone level, and then click **Continue**.
8. Click **Submit**.

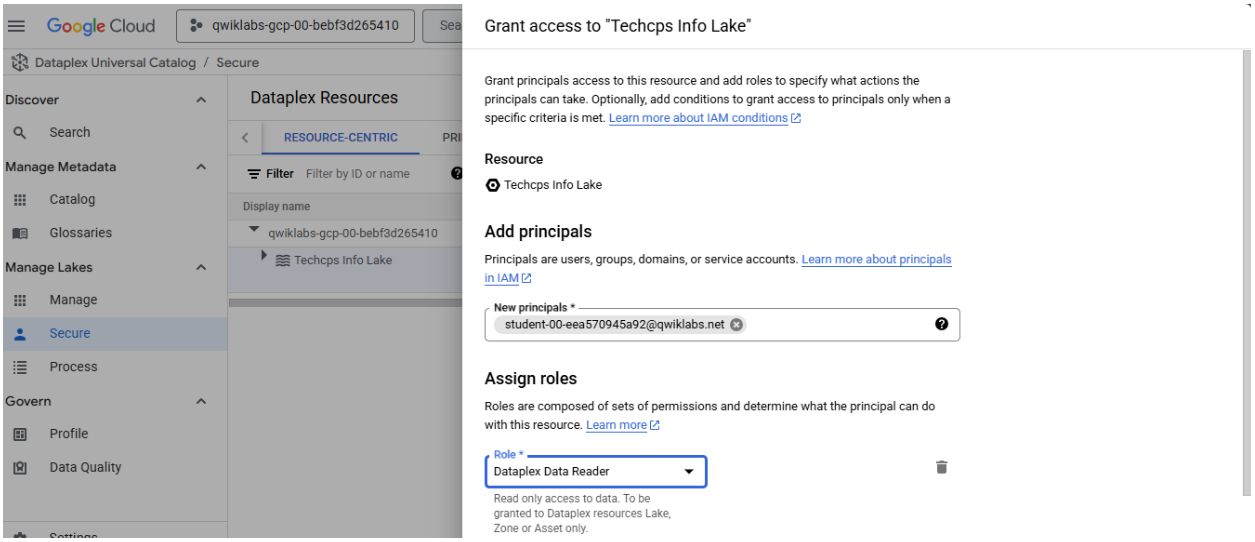
Task 2. Assign Dataplex Data Reader role to another user

Following the Google recommendation of least privilege, Dataplex allows Dataplex administrators to grant Dataplex IAM roles to users at the level of the project, lake, zone, and individual assets like a Cloud Storage bucket.

In this task, you use the Google Cloud console to assign the Dataplex Data Reader role to another user, so that they can have read access to the Cloud Storage bucket that is managed as a Dataplex resource.

To complete this task, **remain logged in as User 1 (____)**, who has the appropriate grant Dataplex IAM roles to other users.

1. In the Google Cloud Console, in the **Navigation menu** (☰), under **Analytics**, navigate to **Dataplex** > **Secure**.
2. In the **Dataplex resources** menu, expand the arrow next to the project ID (____).
3. Expand the arrow next to the name of your lake.
4. Expand the arrow next to the name of your zone.
5. Click on the asset name (Customer Online Sessions).
6. Click **Grant access**.
7. For **New principals**, enter the email for User 2: **User 2 ID**
8. For **Select a role**, select **Dataplex Data Reader** under **Cloud Dataplex**.
9. Click **Save**.



Grant access to "Techcps Info Lake"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions

Resource

Techcps Info Lake

Add principals

Principals are users, groups, domains, or service accounts. Learn more about principals in IAM

New principals *: student-00-eea570945a92@qwiklabs.net

Assign roles

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

Role *: Dataplex Data Reader

Read only access to data. To be granted to Dataplex resources Lake, Zone or Asset only.

Log out of the project as User 1

Log out of the project as User 1. In the next task, you log in to the project as User 2.

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

Task 3. Test access to Dataplex resources as a Dataplex Data Reader

Users who have been granted only the Dataplex Data Reader role on an asset have access to view the Dataplex asset but cannot modify it. For example, users with only the Dataplex Data Reader role on a Cloud Storage bucket cannot add new files to the bucket that is managed as a Dataplex asset.

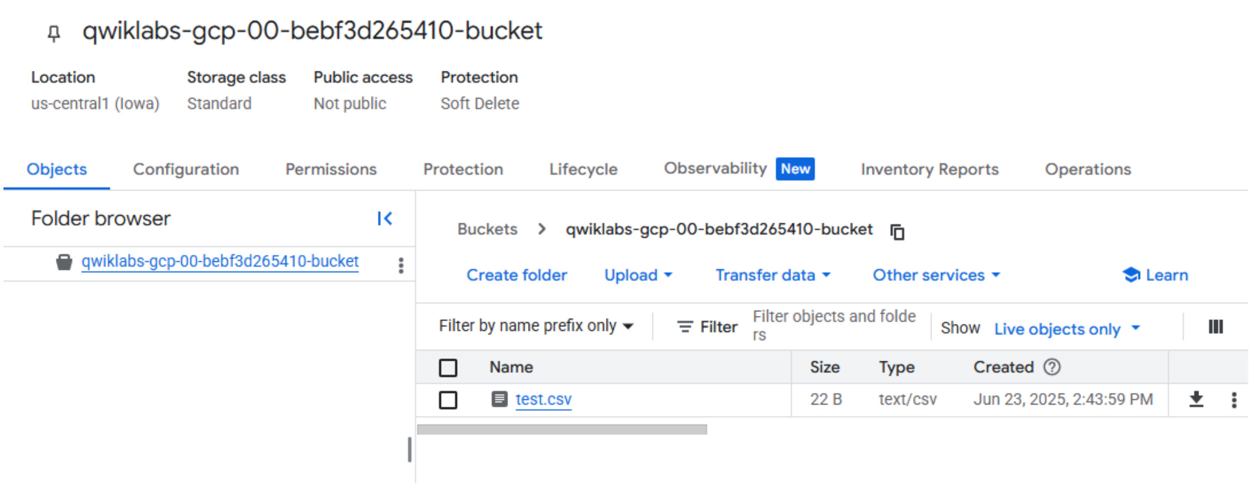
In this task, you use the Google Cloud console to test access for User 2 to Dataplex resources by attempting to add a new file to the pre-created Cloud Storage bucket.

To complete this task, **log in to the project as User 2 (____)**.

1. In the Google Cloud Console, in the **Navigation menu** (☰), navigate to **Cloud Storage** > **Buckets**.
2. Click on the bucket that has been precreated for you: ____-bucket
3. Click **Upload files**.
4. Select any file of your choice.

If you need a sample file, you can download the following test CSV file, and use it as the upload file.

5. Click **Open**.



qwiklabs-gcp-00-bebf3d265410-bucket

Location	Storage class	Public access	Protection
us-central1 (Iowa)	Standard	Not public	Soft Delete

☐	Name	Size	Type	Created
☐	test.csv	22 B	text/csv	Jun 23, 2025, 2:43:59 PM

Log out of the project as User 2

Log out of the project as User 2. In the next task, you log in to the project as User 1.

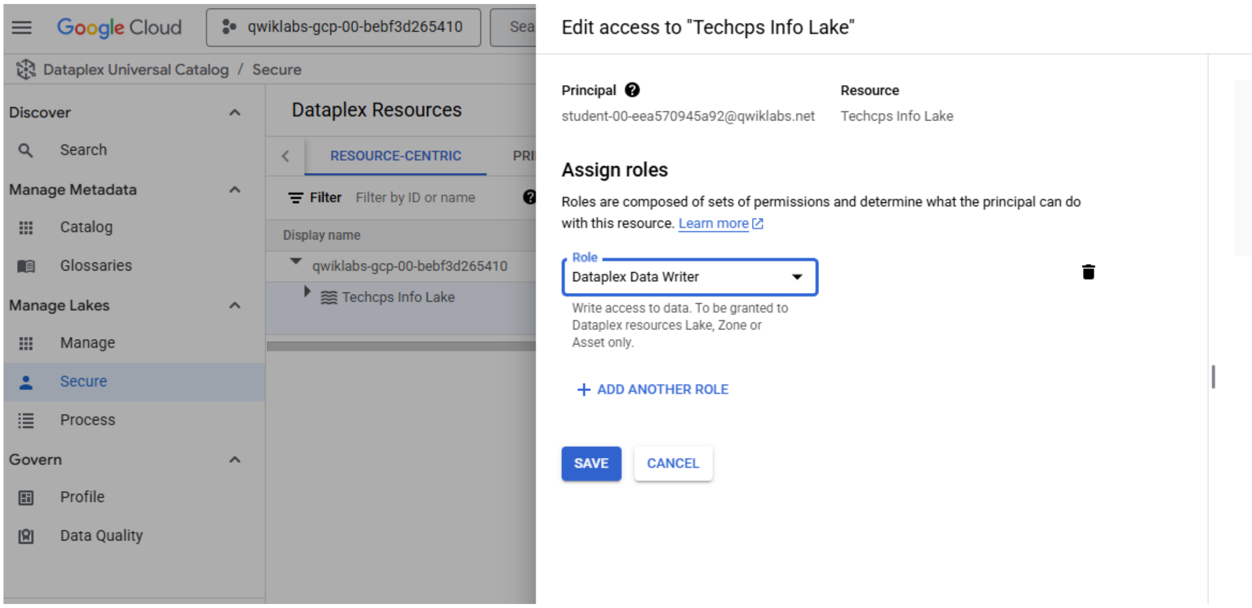
1. Click on the profile icon on the top right of the Google Cloud console.
2. Click **Sign out**.

Task 4. Assign Dataplex Writer role to another user

In this task, you use the Google Cloud console to assign the Dataplex Writer Role on the bucket to User 2, so that they can modify the bucket by adding new files.

To complete this task, **log in to the project as User 1 (____)**, who has the appropriate grant Dataplex IAM roles to other users.

1. In the Google Cloud Console, in the **Navigation menu** (☰), under **Analytics**, navigate to **Dataplex** > **Secure**.
2. In the **Dataplex resources** menu, expand the arrow next to the project ID (____).
3. Expand the arrow next to the name of your lake.
4. Expand the arrow next to the name of your zone.
5. Click on the asset name (Customer Online Sessions).
6. Click on **Edit principal** (pencil icon) next to the email for User 2: **User 2 ID**
7. For **Role**, select **Dataplex Data Writer** under **Cloud Dataplex**.



Edit access to "Techcps Info Lake"

Principal: student-00-eea570945a92@qwiklabs.net

Resource: Techcps Info Lake

Assign roles

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

Role: Dataplex Data Writer

Write access to data. To be granted to Dataplex resources Lake, Zone or Asset only.

Log out of the project as User 1

Log out of the project as User 1. In the next task, you log in to the project as User 2.

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

Task 5. Upload new file to Cloud Storage bucket as a Dataplex Data Writer

Users who have been granted the Dataplex Writer Reader role on an asset have access to modify the asset, including the ability to add new files to a Cloud Storage bucket that is managed as a Dataplex asset.

In this task, you use the Google Cloud console to test access again for User 2 to Dataplex resources by successfully adding a new file to the pre-created Cloud Storage bucket.

To complete this task, **log in to the project as User 2 (____)**.

1. In the Google Cloud Console, in the **Navigation menu** (☰), navigate to **Cloud Storage** > **Buckets**.
2. Click on the bucket that has been precreated for you: ____-bucket
3. Click **Upload files**.
4. Select any file of your choice.

If you need a sample file, you can download the following test CSV file, and use it as the upload file.

5. Click **Open**.

Key Concepts Demonstrated

- **Dataplex IAM Roles**:
  - *Dataplex Viewer*: View metadata only.
  - *Dataplex Data Reader*: Read data from assets.
  - *Dataplex Data Writer*: Modify assets (e.g., write to buckets).
- **Role Granularity**: Roles can be scoped to the entire lake, a zone, or individual assets.
- **Access Validation**: Attempting actions with insufficient roles correctly triggers permission errors.
- **Security Best Practices**: Follows the principle of least privilege by assigning minimum required access.

Conclusion

This lab effectively demonstrated how to implement security in Dataplex using IAM roles. The practical hands-on steps reinforced understanding of:

- Configuring Dataplex resources.
- Applying access controls at various levels.
- Verifying roles by simulating user actions.

By the end of the lab, we were able to securely manage access to data in Dataplex, ensuring that only authorized users could view or modify the data.