**Cloud Audit Logs**

experimentLabschedule1 houruniversal\_currency\_alt5 Creditsshow\_chartIntermediate

infoThis lab may incorporate AI tools to support your learning.

**Overview**

In this lab, you investigate Google Cloud Audit Logs. Cloud Audit Logging maintains multiple audit logs for each project, folder, and organization, all of which help answer the question, "Who did what, when, and where?"

Objectives

In this lab, you learn how to:

* Enable data access logs on Cloud Storage.
* Generate admin and data access activity.
* View Audit logs.

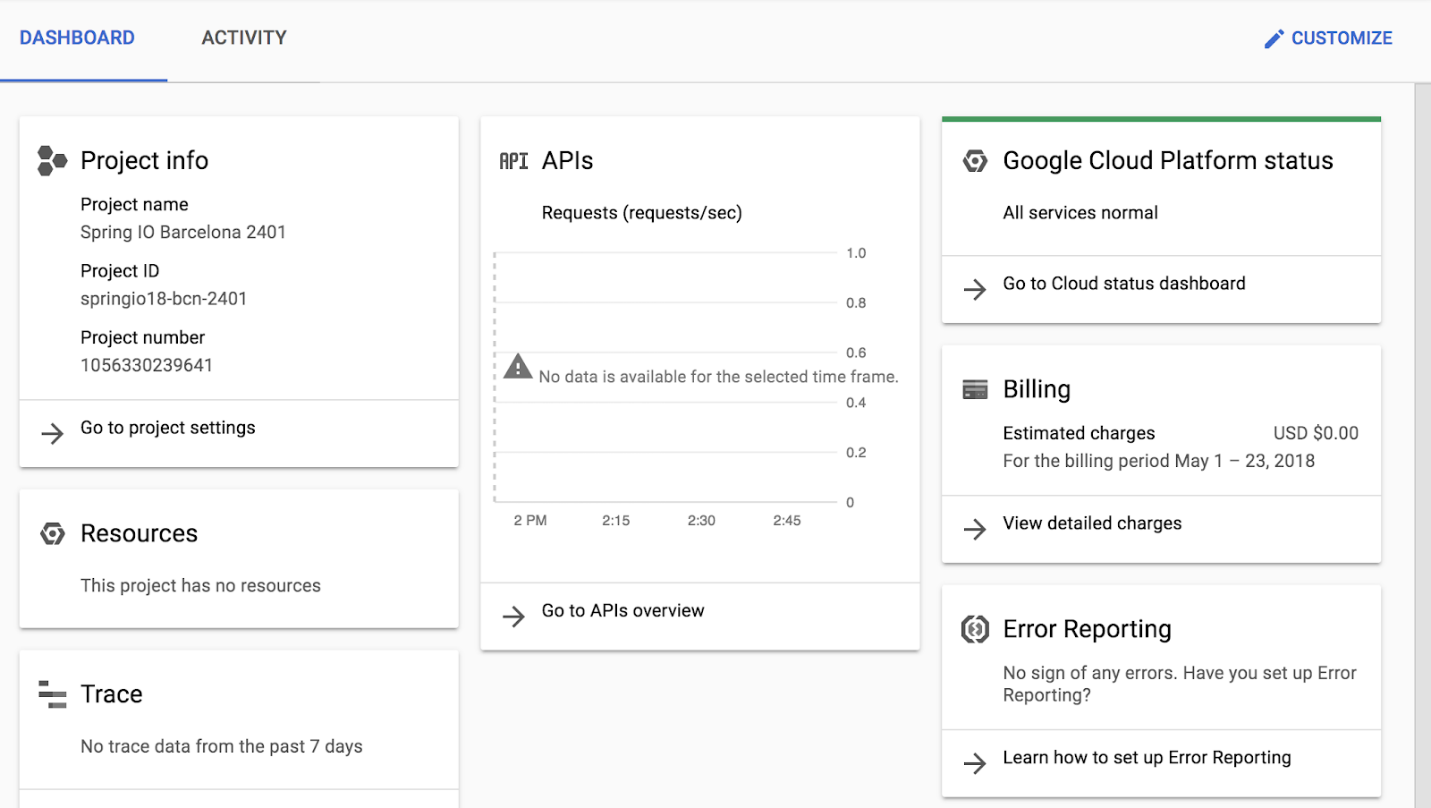
**Setup and requirements**

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.

**Note:** Do not click **End Lab** unless you have finished the lab or want to restart it. This clears your work and removes the project.

After you complete the initial sign-in steps, the project dashboard appears.

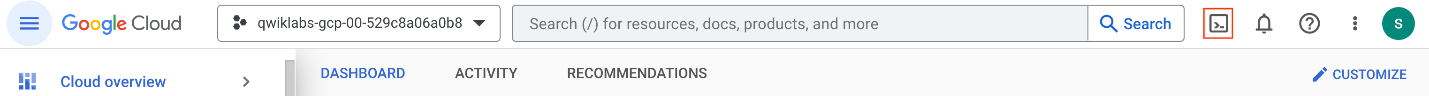


Activate Google Cloud Shell

Google Cloud Shell is a virtual machine that is loaded with development tools. It offers a persistent 5GB home directory and runs on the Google Cloud.

Google Cloud Shell provides command-line access to your Google Cloud resources.

1. In Cloud console, on the top right toolbar, click the Open Cloud Shell button.



1. Click **Continue**.

It takes a few moments to provision and connect to the environment. When you are connected, you are already authenticated, and the project is set to your *PROJECT\_ID*. For example:



**gcloud** is the command-line tool for Google Cloud. It comes pre-installed on Cloud Shell and supports tab-completion.

* You can list the active account name with this command:

gcloud auth list

Copied!

content\_copy

**Output:**

Credentialed accounts:

- @.com (active)

**Example output:**

Credentialed accounts:

- google1623327\_student@qwiklabs.net

* You can list the project ID with this command:

gcloud config list project

Copied!

content\_copy

**Output:**

[core]

project =

**Example output:**

[core]

project = qwiklabs-gcp-44776a13dea667a6

**Note:**Full documentation of **gcloud** is available in the [gcloud CLI overview guide](https://cloud.google.com/sdk/gcloud" \t "_blank).

**Task 1. Enable data access logs on Cloud Storage**

Data Access audit logs (except for BigQuery) are disabled by default. Let's start by enabling data access logs on Cloud Storage.

1. In the Google Cloud Console window, use the **Navigation menu** (Navigation menu icon) to navigate to **IAM & Admin > Audit Logs**.
2. Scroll or use Filter to locate Google Cloud Storage, then check the box next to it. This should display the Info Panel with options on LOG TYPES.

Data Access audit logs are divided into different categories:

* Admin Read: Records operations that read metadata or configuration information. Admin Activity audit logs record writes of metadata and configuration information. They can't be disabled.
* Data Read: Records operations that read user-provided data.
* Data Write: Records operations that write user-provided data.

1. Select **Admin Read**, **Data Read** and **Data Write**, and then click **SAVE**.

Click *Check my progress* to verify the objective.

Assessment Completed!

Enable data access logs on Cloud Storage

Check my progress

*Assessment Completed!*

**Task 2. Generate some admin and data access activity**

The data access logs are now enabled for Cloud Storage. Use Cloud Shell to upload a file to a new storage bucket, create a network, create a VM, and then examine the Cloud Audit Logs.

1. Open or switch to your Cloud Shell terminal.
2. Use gsutil to create a Cloud Storage bucket with the same name as your project:

gsutil mb gs://$DEVSHELL\_PROJECT\_ID

Copied!

content\_copy

1. Make sure the bucket successfully created:

gsutil ls

Copied!

content\_copy

1. Create a simple "Hello World" type of text file and upload it to your bucket:

echo "Hello World!" > sample.txt

gsutil cp sample.txt gs://$DEVSHELL\_PROJECT\_ID

Copied!

content\_copy

1. Verify the file is in the bucket:

gsutil ls gs://$DEVSHELL\_PROJECT\_ID

Copied!

content\_copy

1. Create a new auto mode network named **mynetwork**, then create a new virtual machine and place it on the new network:

gcloud compute networks create mynetwork --subnet-mode=auto

Copied!

content\_copy

gcloud compute instances create default-us-vm \

--zone=us-east4-c --network=mynetwork \

--machine-type=e2-medium

Copied!

content\_copy

Click *Check my progress* to verify the objective.

Assessment Completed!

Check the creation of bucket, network and virtual machine instance

Check my progress

*Assessment Completed!*

1. Delete the storage bucket:

gsutil rm -r gs://$DEVSHELL\_PROJECT\_ID

Copied!

content\_copy

**Task 3. Viewing audit logs**

Admin Activity logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, the logs record when VM instances and App Engine applications are created, or when permissions are changed. To view the logs, you must have the Cloud Identity and Access Management roles Logging/Logs Viewer or Project/Viewer.

Admin Activity logs are always enabled so there is no need to enable them. There is no charge for your Admin Activity audit logs.

1. Use the **Navigation menu** to navigate to **Logging > Logs Explorer**.
2. Enable **Show query** and delete the contents of **Query** box.
3. Click the **Log name** dropdown and use the filter to locate the **activity** log under **CLOUD AUDIT** section and **Apply** it to the query.
4. Press the **Run query** button, and then use the Log fields explorer to filter to **GCS Bucket** entries.
5. Locate the log entry for when the Cloud Storage was deleted.
6. Expand the delete entry, then drill into **protoPayload** > **authenticationInfo** field and notice you can see the email address of the user that performed this action.

Feel free to explore other fields in the entry. Also, notice how many of the values can be clicked to add inclusions/exclusions to the query.

1. Delete the existing query and use **Log Name** to view the **data\_access** logs.

What operations can you see now?

Click *Check my progress* to verify the objective.

Assessment Completed!

Viewing audit logs

Check my progress

*Assessment Completed!*

Using the Cloud SDK

Log entries can also be read using the Cloud SDK command:

Example:

gcloud logging read [FILTER]

Copied!

content\_copy

1. Switch to or reopen a Cloud Shell terminal.
2. If we wanted to see those same data access logs using the command line, we could run the following:

gcloud logging read \

"logName=projects/$DEVSHELL\_PROJECT\_ID/logs/cloudaudit.googleapis.com%2Fdata\_access"

Copied!

content\_copy

Congratulations!

In this exercise, you examined and worked with Google Cloud's Audit Logs. Now you can do a better job figuring out exactly who, did what, when. Nice job.