**Using BigQuery and Cloud Logging to Analyze BigQuery Usage**

experimentLabschedule45 minutesuniversal\_currency\_alt1 Creditshow\_chartIntroductory

infoThis lab may incorporate AI tools to support your learning.

**GSP617**



**Overview**

Cloud Logging serves as a central repository for logs from various Google Cloud services, including BigQuery, and is ideal for short to mid-term log storage. Many industries require logs to be retained for extended periods. To keep logs for extended historical analysis or complex auditing, you can set up a sink to export specific logs to BigQuery.

In this lab you view the BigQuery logs inside Cloud Logging, set up a sink to export them into BigQuery, and then use SQL to analyze the logs.

**Setup and requirements**

Before you click the Start Lab button

Read these instructions. Labs are timed and you cannot pause them. The timer, which starts when you click **Start Lab**, shows how long Google Cloud resources will be made available to you.

This hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that you use to sign in and access Google Cloud for the duration of the lab.

To complete this lab, you need:

* Access to a standard internet browser (Chrome browser recommended).

**Note:** Use an Incognito or private browser window to run this lab. This prevents any conflicts between your personal account and the Student account, which may cause extra charges incurred to your personal account.

* Time to complete the lab---remember, once you start, you cannot pause a lab.

**Note:** If you already have your own personal Google Cloud account or project, do not use it for this lab to avoid extra charges to your account.

How to start your lab and sign in to the Google Cloud 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 the **Lab Details** panel with the following:
   * The **Open Google Cloud console** button
   * Time remaining
   * The temporary credentials that you must use for this lab
   * Other information, if needed, to step through this lab
2. Click **Open Google Cloud console** (or right-click and select **Open Link in Incognito Window** if you are running the Chrome browser).

The lab spins up resources, and then opens another tab that shows the **Sign in** page.

***Tip:*** Arrange the tabs in separate windows, side-by-side.

**Note:**If you see the **Choose an account** dialog, click **Use Another Account**.

1. If necessary, copy the **Username** below and paste it into the **Sign in** dialog.

student-00-72e4be373c4d@qwiklabs.net

Copied!

content\_copy

You can also find the **Username** in the **Lab Details** panel.

1. Click **Next**.
2. Copy the **Password** below and paste it into the **Welcome** dialog.

UNPt6IvTAIOH

Copied!

content\_copy

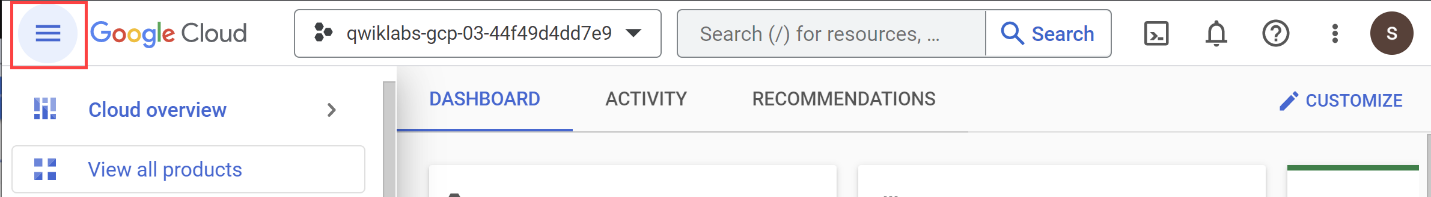
You can also find the **Password** in the **Lab Details** panel.

1. Click **Next**.

**Important:**You must use the credentials the lab provides you. Do not use your Google Cloud account credentials.**Note:**Using your own Google Cloud account for this lab may incur extra charges.

1. 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 Google Cloud console opens in this tab.

**Note:** To view a menu with a list of Google Cloud products and services, click the **Navigation menu** at the top-left. 

Activate Cloud Shell

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

1. Click **Activate Cloud Shell** Activate Cloud Shell icon at the top of the Google Cloud console.

When you are connected, you are already authenticated, and the project is set to your **Project\_ID**, qwiklabs-gcp-01-aa37830c928a. The output contains a line that declares the **Project\_ID** for this session:

Your Cloud Platform project in this session is set to qwiklabs-gcp-01-aa37830c928a

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

1. (Optional) You can list the active account name with this command:

gcloud auth list

Copied!

content\_copy

1. Click **Authorize**.

**Output:**

ACTIVE: \*

ACCOUNT: student-00-72e4be373c4d@qwiklabs.net

To set the active account, run:

$ gcloud config set account `ACCOUNT`

1. (Optional) You can list the project ID with this command:

gcloud config list project

Copied!

content\_copy

**Output:**

[core]

project = qwiklabs-gcp-01-aa37830c928a

**Note:**For full documentation of gcloud, in Google Cloud, refer to [the gcloud CLI overview guide](https://cloud.google.com/sdk/gcloud).

**Task 1. Open BigQuery**

Open the BigQuery console

1. In the Google Cloud Console, select **Navigation menu** > **BigQuery**.

The **Welcome to BigQuery in the Cloud Console** message box opens. This message box provides a link to the quickstart guide and the release notes.

1. Click **Done**.

The BigQuery console opens.

**Task 2. Create a dataset**

1. Under the **Explorer** section, click on the three dots next to the project that starts with qwiklabs-gcp-.
2. Click **Create dataset**.
3. Set *Dataset ID* to **bq\_logs**.
4. Click **CREATE DATASET**.

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

Assessment Completed!

Create a Dataset

Check my progress

*Assessment Completed!*

**Task 3. Run a query**

First, run a simple query which generates a log. Later you will use this log to set up the log export from to BigQuery.

1. Copy and paste the following query into the BigQuery Query editor:

SELECT current\_date

Copied!

content\_copy

1. Click **RUN**.

**Task 4. Set up log export from Cloud Logging**

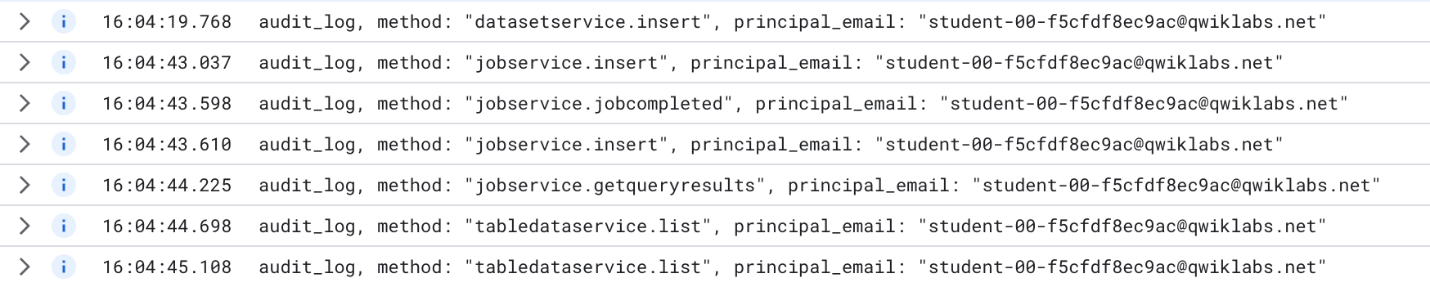
1. In the Cloud console, select **Navigation menu** > **View All Products** > **Logging** > **Logs Explorer**.

**Note:** If prompted, Click LEAVE for Unsaved work.

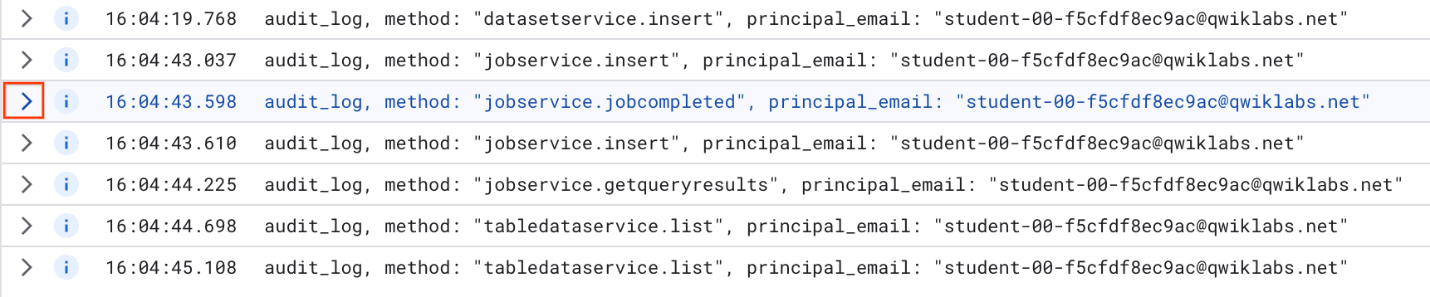
1. In **All resources**, select **BigQuery**, then click **Apply**.
2. Now, click **Run query** button in the top right.

A few log entries from the query should appear.

Look for the entry that contains the word "jobcompleted".



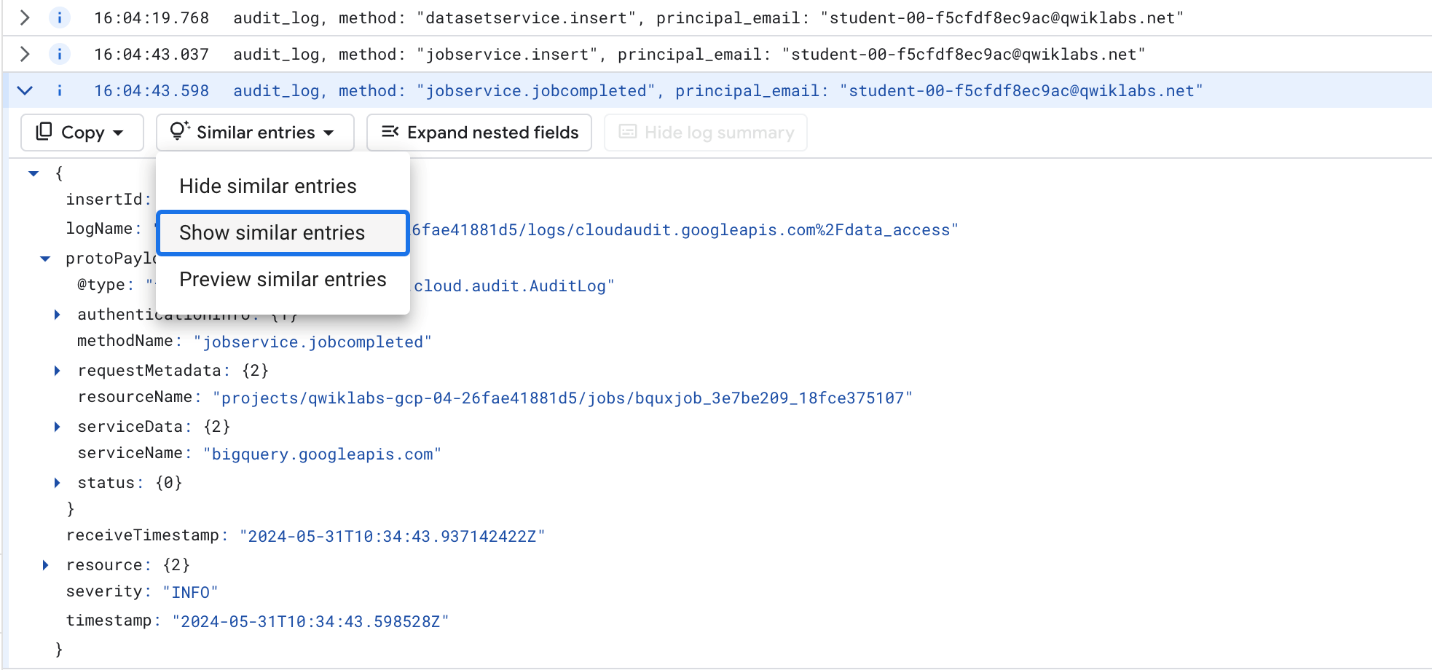
1. Click on the arrow on the left to expand the entry.



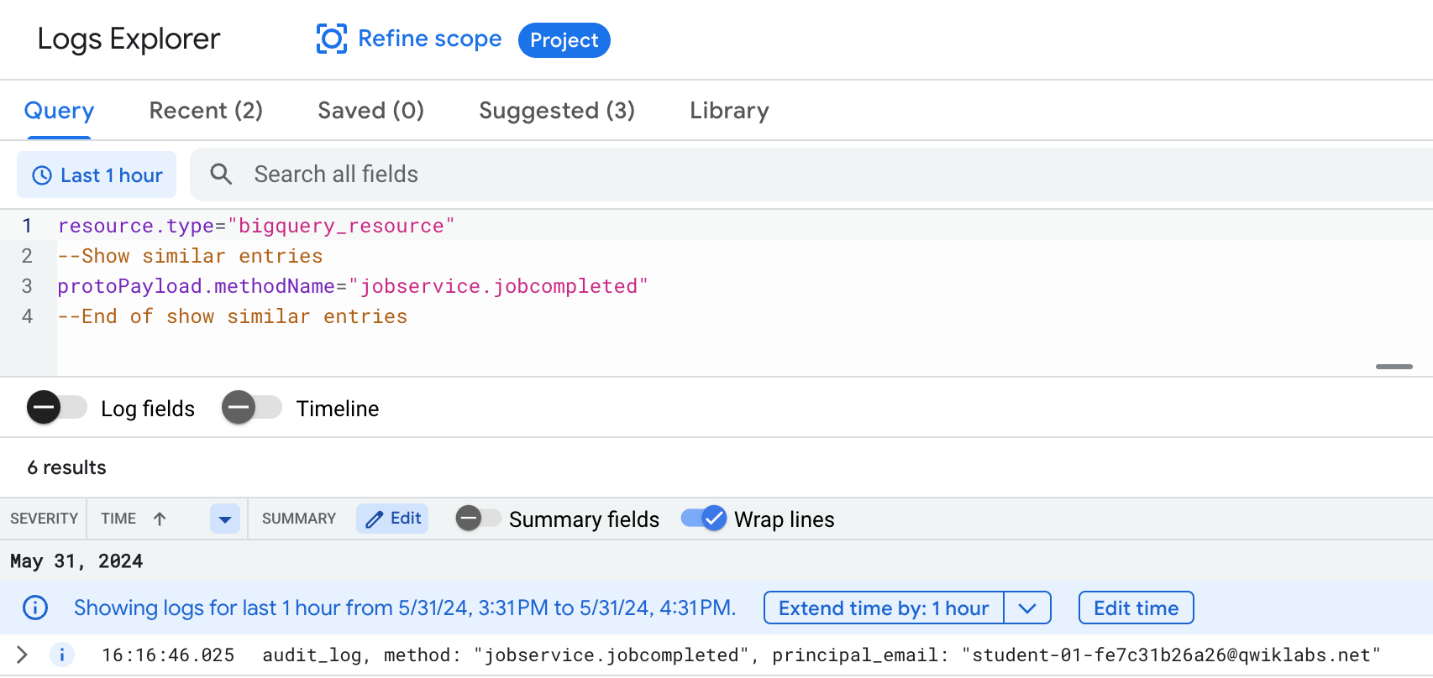
Then click on **Expand nested fields** button on the right hand side.

This shows the full JSON log entry. Scroll down and have a look at the different fields.

1. Scroll back up to the header of the entry, click on **Similar entries** button and choose **Show similar entries**.



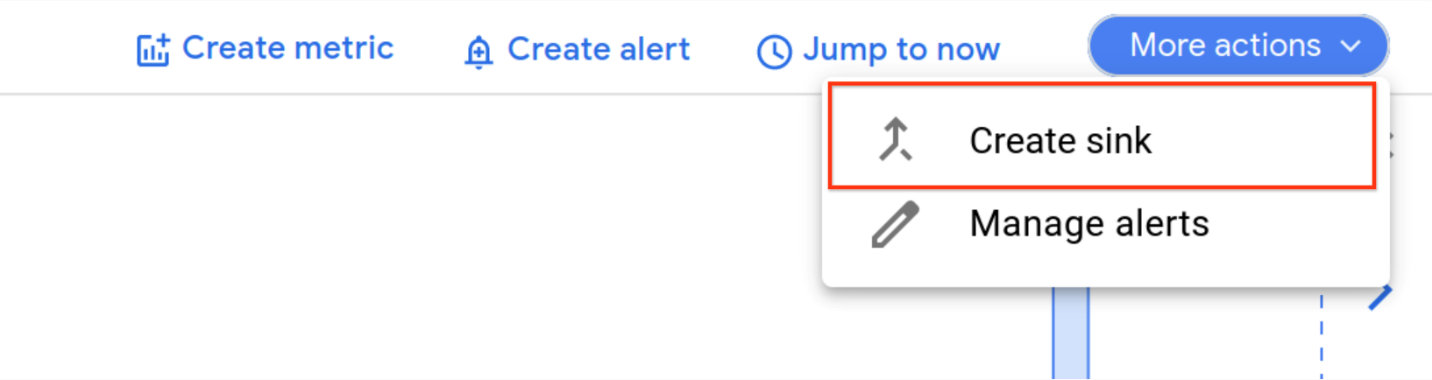
This sets up the search with the correct terms. You may need to toggle the **Show Query** button to see it.



Create sink

Now that you have the logs you need, time to set up a sink.

1. Click **Create sink** from the **More actions** drop-down.



1. Fill in the fields as follows:

* Sink name: **JobComplete** and click **NEXT**.
* Select sink service: **BigQuery dataset**
* Select Bigquery dataset (Destination): **bq\_logs** (The dataset you setup previously)
* Leave the rest of the options at the default settings.

1. Click **CREATE SINK**.

Any subsequent log entries from BigQuery are now exported to a table in the **bq\_logs** dataset.

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

Assessment Completed!

Create a Sink

Check my progress

*Assessment Completed!*

**Task 5. Run example queries**

To populate your new table with some logs, run some example queries.

* Navigate to **Cloud Shell**, then add each of the following BigQuery commands into Cloud Shell:

bq query --location=us --use\_legacy\_sql=false --use\_cache=false \

'SELECT fullName, AVG(CL.numberOfYears) avgyears

FROM `qwiklabs-resources.qlbqsamples.persons\_living`, UNNEST(citiesLived) as CL

GROUP BY fullname'

Copied!

content\_copy

bq query --location=us --use\_legacy\_sql=false --use\_cache=false \

'select month, avg(mean\_temp) as avgtemp from `qwiklabs-resources.qlweather\_geo.gsod`

where station\_number = 947680

and year = 2010

group by month

order by month'

Copied!

content\_copy

bq query --location=us --use\_legacy\_sql=false --use\_cache=false \

'select CONCAT(departure\_airport, "-", arrival\_airport) as route, count(\*) as numberflights

from `bigquery-samples.airline\_ontime\_data.airline\_id\_codes` ac,

`qwiklabs-resources.qlairline\_ontime\_data.flights` fl

where ac.code = fl.airline\_code

and regexp\_contains(ac.airline , r"Alaska")

group by 1

order by 2 desc

LIMIT 10'

Copied!

content\_copy

You should see the results of each query returned.

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

Assessment Completed!

Run example queries

Check my progress

*Assessment Completed!*

**Task 6. Viewing the logs in BigQuery**

1. Navigate back to BigQuery (**Navigation menu** > **BigQuery**).
2. Expand your resource starting with the name **qwiklabs-gcp-** and expand your dataset **bq\_logs**.

The name may vary, but you should see a "cloudaudit\_googleapis\_com\_data\_access" table.

**Note:** You may have to re-run the example queries to get the table to show up.

1. Click on the table name, then inspect the schema of the table and notice it has a very large number of fields.

If you clicked **Preview** and wondered why it doesn't show the logs for the recently run queries, its because the logs are streamed into the table, which means that the new data can be queried but won't show up in Preview for a little while.

To make the table more usable, create a **VIEW**, which pulls out subset of fields and also performs some calculations to derive a metric for query time.

1. Click **Compose New Query**. In the BigQuery query EDITOR, run the following SQL after replacing with the name of your project (the Project ID can be easily copied from the **Lab Details** panel on the left side of the lab page):

CREATE OR REPLACE VIEW

bq\_logs.v\_querylogs AS

SELECT

resource.labels.project\_id,

protopayload\_auditlog.authenticationInfo.principalEmail,

protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobConfiguration.query.query,

protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobConfiguration.query.statementType,

protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatus.error.message,

protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatistics.startTime,

protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatistics.endTime,

TIMESTAMP\_DIFF(protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatistics.endTime, protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatistics.startTime, MILLISECOND)/1000 AS run\_seconds,

protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatistics.totalProcessedBytes,

protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatistics.totalSlotMs,

ARRAY(SELECT as STRUCT datasetid, tableId FROM UNNEST(protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatistics.referencedTables)) as tables\_ref,

protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatistics.totalTablesProcessed,

protopayload\_auditlog.servicedata\_v1\_bigquery.jobCompletedEvent.job.jobStatistics.queryOutputRowCount,

severity

FROM

`<YOUR-PROJECT-ID>.bq\_logs.cloudaudit\_googleapis\_com\_data\_access\_\*`

ORDER BY

startTime

Copied!

content\_copy

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

Assessment Completed!

Viewing the logs in BigQuery

Check my progress

*Assessment Completed!*

1. Now query the VIEW. Compose a new query, and run the following command:

SELECT \* FROM bq\_logs.v\_querylogs

Copied!

content\_copy

1. Scroll through the results of the executed queries.

**Congratulations!**

You successfully exported BigQuery logs from Cloud Logging to a BigQuery table, then analyzed them with SQL.

Next steps / Learn more

* Read through the [Cloud Logging](https://cloud.google.com/logging/docs/) documentation.
* Read through the [BigQuery](https://cloud.google.com/bigquery/docs/" \t "_blank) documentation.

Google Cloud training and certification

...helps you make the most of Google Cloud technologies. [Our classes](https://cloud.google.com/training/courses) 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](https://cloud.google.com/certification/) help you validate and prove your skill and expertise in Google Cloud technologies.

**Manual Last Updated: May 31, 2024**

**Lab Last Tested: May 31, 2024**

Copyright 2024 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.