**Configuring and Viewing Cloud Audit Logs**

experimentLabschedule1 hour 30 minutesuniversal\_currency\_alt1 Creditshow\_chartIntroductory

infoThis lab may incorporate AI tools to support your learning.

**Overview**

In this lab, you will investigate [Cloud Audit Logs](https://cloud.google.com/logging/docs/audit). Cloud Audit Logs maintains two audit logs for each project and organization: Admin Activity and Data Access.

Google Cloud services write audit log entries to these logs to help you answer the questions of "who did what, where, and when" within your Google Cloud projects.

Objectives

In this lab, you will learn how to perform the following tasks:

* View audit logs in the Activity page.
* View and filter audit logs in Cloud Logging.
* Retrieve log entries with gcloud.
* Export 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.

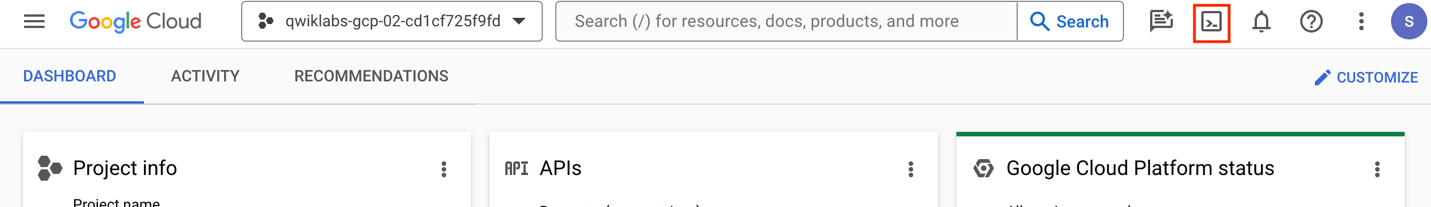
**Note:** Do not click **End Lab** unless you have finished the lab or want to restart it. This clears your work and removes the project.

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]

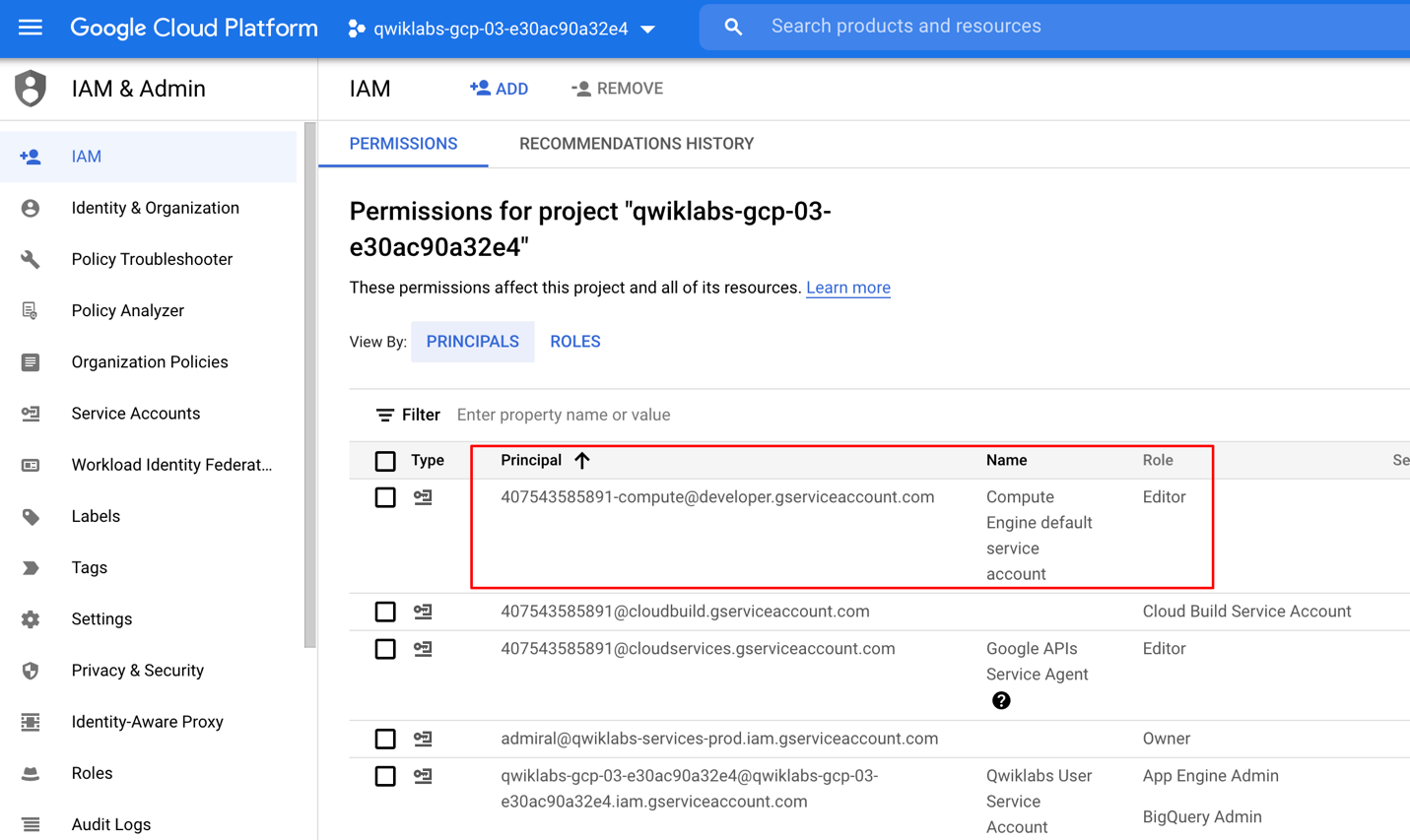
project = qwiklabs-gcp-44776a13dea667a6

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

Check project permissions

Before you begin your work on Google Cloud, you need to ensure that your project has the correct permissions within Identity and Access Management (IAM).

1. In the Google Cloud console, on the **Navigation menu** (Navigation menu icon), select **IAM & Admin** > **IAM**.
2. Confirm that the default compute Service Account {project-number}-compute@developer.gserviceaccount.com is present and has the editor role assigned. The account prefix is the project number, which you can find on **Navigation menu > Cloud overview > Dashboard**.



**Note:**If the account is not present in IAM or does not have the `editor` role, follow the steps below to assign the required role.

1. In the Google Cloud console, on the **Navigation menu**, click **Cloud overview > Dashboard**.
2. Copy the project number (e.g. 729328892908).
3. On the **Navigation menu**, select **IAM & Admin** > **IAM**.
4. At the top of the **IAM** page, click **+ Grant Access**.
5. For **New principals**, type:

{project-number}-compute@developer.gserviceaccount.com

Copied!

content\_copy

1. Replace {project-number} with your project number.
2. For **Select a role**, select **Project** (or Basic) > **Editor**.
3. Click **Save**.

**Task 1. Enable data access audit logs**

In this task, you enable data access audit logs.

Data access audit logs (except for BigQuery) are disabled by default, so you must first enable all audit logs. Logging charges for the volume of log data that exceeds the free monthly logs allotment.

All logs received by Logging count towards the logs allotment limit, except for the Cloud Audit Logs that are enabled by default. This includes all Google Cloud Admin Activity audit logs, System Event logs, plus data access audit logs from BigQuery only.

1. If you have not activated cloud shell yet then, on the Google Cloud Console title bar, click **Activate Cloud Shell** (Activate Cloud Shell icon). If prompted, click **Continue**.
2. At the command prompt, run this command to retrieve the current IAM policy for your project and save it as policy.json:

gcloud projects get-iam-policy $DEVSHELL\_PROJECT\_ID \

--format=json >./policy.json

Copied!

content\_copy

1. Click the **Open Editor** button to view the Cloud Shell code editor.

If an error indicates that the code editor could not be loaded because third-party cookies are disabled, click **Open in New Window** and switch to the new tab.

1. In the Cloud Shell code editor, click the **policy.json** file to expose its contents.
2. Add the following text to the policy.json file to enable data Access audit logs for all services. This text should be added just after the first { and before "bindings": [. (Be careful not to change anything else in the file).

"auditConfigs": [

{

"service": "allServices",

"auditLogConfigs": [

{ "logType": "ADMIN\_READ" },

{ "logType": "DATA\_READ" },

{ "logType": "DATA\_WRITE" }

]

}

],

Copied!

content\_copy

The file will look similar to below.



1. Click the **Open Terminal** button to return to the Cloud Shell command line.
2. At the command line, run the following command to set the IAM policy:

gcloud projects set-iam-policy $DEVSHELL\_PROJECT\_ID \

./policy.json

Copied!

content\_copy

The command will return and display the new IAM policy.

**Task 2. Generate some account activity**

In this task, you create resources that generate log activty that you can view in Cloud Audit logs.

* In Cloud Shell, run the following commands to create a few resources. This will generate some activity that you will view in the audit logs:

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

echo "this is a sample file" > sample.txt

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

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

gcloud compute instances create default-us-vm \

--machine-type=e2-micro \

--zone="ZONE" --network=mynetwork

Copied!

content\_copy

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

Copied!

content\_copy

**Task 3. View the Admin Activity logs**

In this task, you view the Admin Activity 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 and 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.

**Note:** You can view audit log entries in the Logs Viewer, Cloud Logging, and in the Cloud SDK. You can also export audit log entries to Pub/Sub, BigQuery, or Cloud Storage.

Use the Cloud Logging page

1. From the Cloud Console, select **Navigation menu > Logging > Logs Explorer**.
2. Paste the following in the **Query builder** field and replace [PROJECT\_ID] with your project ID. You can copy the **PROJECT\_ID** from the **Qwiklabs Connection Details**.

logName = ("projects/[PROJECT\_ID]/logs/cloudaudit.googleapis.com%2Factivity")

Copied!

content\_copy

1. Click the **Run Query** button.
2. Locate the log entry indicating that a Cloud Storage bucket was deleted. This entry will refer to storage.googleapis.com, which calls the storage.buckets.delete method to delete a bucket. The bucket name is the same name as your project id.
3. Within that entry, click on the **storage.googleapis.com** text and select **Show matching entries**.
4. Notice a line was added to the query preview textbox (located where the query builder had been) to show only storage events.

logName = ("projects/qwiklabs-gcp-xxxxxxxxx/logs/cloudaudit.googleapis.com%2Factivity")

protoPayload.serviceName="storage.googleapis.com"

Copied!

content\_copy

You should now see only the cloud storage entries.

1. Within that entry, click on the **storage.buckets.delete** text and select **Show matching entries**.
2. Notice another line was added to the Query preview textbox and now you can only see storage delete entries.

This technique can be used to easily locate desired events.

1. In the Query results, expand the **Cloud Storage delete** entry and then expand the **protoPayload** field.
2. Expand the **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.

Use the Cloud SDK

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

**Example output:**

gcloud logging read [FILTER]

* In the Cloud Shell pane, use this command to retrieve only the audit activity for storage bucket deletion:

**Note:** If Cloud Shell is disconnected, then click **reconnect**.

gcloud logging read \

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

AND protoPayload.serviceName=storage.googleapis.com \

AND protoPayload.methodName=storage.buckets.delete"

Copied!

content\_copy

**Task 4. Export the audit logs**

In this task, you export audit logs. Individual audit log entries are kept for a specified length of time and are then deleted. The Cloud Logging [Quota Policy](https://cloud.google.com/logging/quotas) explains how long log entries are retained. You cannot otherwise delete or modify audit logs or their entries.

|  |  |
| --- | --- |
| **Audit log type** | **Retention period** |
| Admin Activity | 400 days |
| Data Access | 30 days |

For longer retention, you can export audit log entries like any other Cloud Logging log entries and keep them for as long as you wish.

Export audit logs

When exporting logs, the current filter will be applied to what is exported.

1. In Logs Explorer, enter a query string in the **Query builder** to display all the audit logs. (This can be done by deleting all lines in the filter except the first one.) Your filter will look like what is shown below. (Note that your project ID will be different.)

logName = ("projects/[PROJECT\_ID]/logs/cloudaudit.googleapis.com%2Factivity")

Copied!

content\_copy

1. Click the **Run Query** button.
2. Click on **Actions > Create Sink** button.
3. For the **Sink Name** name, enter AuditLogsExport and click **Next**.
4. For the **Sink service**, enter BigQuery dataset.
5. Click **Select BigQuery dataset** and then select **Create new BigQuery dataset**.
6. For the **Dataset ID**, enter auditlogs\_dataset and click **Create Dataset**.
7. Uncheck the **Use Partitioned Tables** checkbox, if it is already selected, and click **Next**.
8. In the Build inclusion filter list box, make sure that this filter text is entered logName = ("projects/[PROJECT\_ID]/logs/cloudaudit.googleapis.com%2Factivity").
9. Click the **Create Sink** button. The Logs Router Sinks page appears. Now, click on **Logs Router**.

On this page, you should be able to see the AuditLogsExport sink.

1. To the right of the AuditLogsExport sink, click the button with three dots (More icon) and select **View sink details**.

This will show information about the sink that you created.

1. Click **Cancel** when done.

**Note:** You could also export log entries to Pub/Sub or Cloud Storage. Exporting to Pub/Sub can be useful if you want to flow through an ETL process prior to storing in a database **(Cloud Operations > PubSub > Dataflow > BigQuery/Bigtable)**. Exporting to Cloud Storage will batch up entries and write them into Cloud Storage objects approximately once an hour.**Note:** All future logs will now be exported to BigQuery and the BigQuery tools can be used to perform analysis on the audit log data. The export does not export existing log entries.

1. In Cloud Shell, run the following commands to generate some more activity that you will view in the audit logs exported to BigQuery:

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

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

echo "this is another sample file" > sample2.txt

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

gcloud compute instances delete --zone="ZONE" \

--delete-disks=all default-us-vm

Copied!

content\_copy

When prompted, enter y.

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

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

Copied!

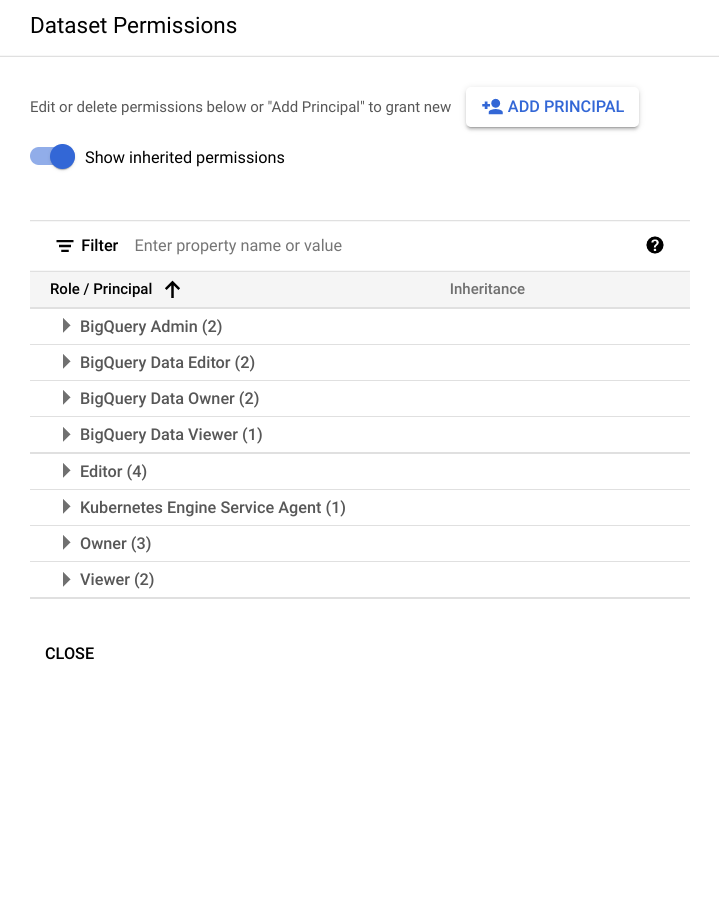
content\_copy

**Task 5. Use BigQuery to analyze logs**

In this task, you export logs to a BigQuery dataset. You then analyze the logs using Query editor.

**Note:** When you export logs to a BigQuery dataset, Cloud Logging creates dated tables to hold the exported log entries. Log entries are placed in tables whose names are based on the entries' log names.

1. Go to **Navigation menu > BigQuery**. If prompted, log in with the Qwiklabs-provided credentials.
2. The *Welcome to BigQuery in the Cloud Console* message box opens. This message box provides a link to the quickstart guide and lists UI updates.
3. Click **Done**.
4. In the left pane, under the **Explorer** section, click your project. This starts with (qwiklabs-gcp-xxx). You should see an **auditlogs\_dataset** dataset under it.
5. Verify that the BigQuery dataset has appropriate permissions to allow the export writer to store log entries. Click on the **auditlogs\_dataset** dataset.
6. From the **Sharing** dropdown, select **Permissions**.
7. On the Dataset Permission page, you will see the service account listed as **BigQuery Data Editor** member. If it's not already listed, you can add a service account under **Add Principal** and grant it the data editor role.



1. Click the **Close** button to close the **Share Dataset** screen.
2. Expand the **dataset** to see the table with your exported logs. (Click on the expand icon to expand the dataset.)
3. Click on the **table name** and take a moment to review the **schemas** and **details** of the tables that are being used.
4. Click the **Query > In new tab** button.
5. In Cloud Shell, run the following commands again to generate some more activity that you will view in the audit logs exported to BigQuery:

gcloud compute instances create default-us-vm \

--zone="ZONE" --network=mynetwork

Copied!

content\_copy

gcloud compute instances delete --zone="ZONE" \

--delete-disks=all default-us-vm

Copied!

content\_copy

When prompted, enter y.

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

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

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

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

Copied!

content\_copy

1. Delete the text provided in the **Query editor** window and paste in the query below. This query will return the users that deleted virtual machines in the last 7 days.

#standardSQL

SELECT

timestamp,

resource.labels.instance\_id,

protopayload\_auditlog.authenticationInfo.principalEmail,

protopayload\_auditlog.resourceName,

protopayload\_auditlog.methodName

FROM

`auditlogs\_dataset.cloudaudit\_googleapis\_com\_activity\_\*`

WHERE

PARSE\_DATE('%Y%m%d', \_TABLE\_SUFFIX) BETWEEN

DATE\_SUB(CURRENT\_DATE(), INTERVAL 7 DAY) AND

CURRENT\_DATE()

AND resource.type = "gce\_instance"

AND operation.first IS TRUE

AND protopayload\_auditlog.methodName = "v1.compute.instances.delete"

ORDER BY

timestamp,

resource.labels.instance\_id

LIMIT

1000

Copied!

content\_copy

1. Click the **Run** button. After a couple of seconds you will see each time someone deleted a virtual machine within the past 7 days. You should see two entries, which is the activity you generated in this lab. Remember, BigQuery is only showing activity since the export was created.
2. Delete the text in the **Query\_editor** window and paste in the query below. This query will return the users that deleted storage buckets in the last 7 days.

#standardSQL

SELECT

timestamp,

resource.labels.bucket\_name,

protopayload\_auditlog.authenticationInfo.principalEmail,

protopayload\_auditlog.resourceName,

protopayload\_auditlog.methodName

FROM

`auditlogs\_dataset.cloudaudit\_googleapis\_com\_activity\_\*`

WHERE

PARSE\_DATE('%Y%m%d', \_TABLE\_SUFFIX) BETWEEN

DATE\_SUB(CURRENT\_DATE(), INTERVAL 7 DAY) AND

CURRENT\_DATE()

AND resource.type = "gcs\_bucket"

AND protopayload\_auditlog.methodName = "storage.buckets.delete"

ORDER BY

timestamp,

resource.labels.instance\_id

LIMIT

1000

Copied!

content\_copy

1. Click the **Run** button. After a couple seconds you will see entries showing each time someone deleted a storage bucket within the past 7 days.

**Note:** As you can see, the ability to analyze audit logs in BigQuery is very powerful. In this activity, you viewed just two examples of querying audit logs.

Click *Check my progress* to verify the objective.

Export audit logs and use BigQuery to analyze logs

Check my progress

**Congratulations!**

In this lab, you have done the following:

1. Viewed audit logs on the activity page.
2. Viewed and filtered audit logs in Cloud Operations.
3. Retrieved log entries with gcloud.
4. Exported audit logs.

**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.

Copyright 2022 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.