

ANALYZE AUDIT LOGS USING BigQuery

PROJECT DESCRIPTION

In this lab, I'll investigate audit logs to identify patterns of suspicious activity involving cloud resources.

SCENARIO

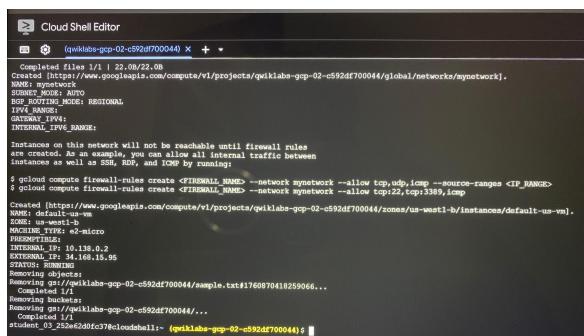
To get a better understanding of security incidents I have set up a test environment to recreate an incident and analyze the artifacts.

I will be using two separate accounts on the google cloud console: one account will generate the malicious activity and the other account will be used to investigate the activity.

First Step: Generate Account Activity

Here, I created and deleted cloud resources to generate account activity which I'll access as Cloud Audit logs.

I inputted the following command into the cloud shell terminal;



```
Cloud Shell Editor
(qwiklabs-gcp-02-c592df700044) ~ + 
Completed files 1/1 | 22:08/22:08
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-c592df700044/global/networks/synetwork].
NAME: synetwork
SUBNET_MODE: AUTO
REGION: us-central1
INTERNAL_IPV4:
INTERNAL_IPV4_RANGE:
Instances on this network will not be reachable until firewall rules
are created. Firewall rules allow all external traffic between
instances as well as SSH, EDNS, and ICMP by running:
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network synetwork --allow tcp:udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network synetwork --allow tcp:22,top:5389,icmp
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-c592df700044/regions/us-central1/instances/default-us-vn].
NAME: default-us-vn
ZONE: us-central1-b
MACHINE_TYPE: e2-micro
PREEMPTIBLE: False
INTERNAL_IP: 10.138.0.2
EXTERNAL_IP: 34.168.15.95
CPU: 1
MEMORY: 1.75GB
Removing objects:
Deleting bucket [qwiklabs-gcp-02-c592df700044/sample]
Completed 1/1
Removing bucket:
Deleting bucket [qwiklabs-gcp-02-c592df700044/...]
Completed 0/1
student_03_25@e6dd9c37@cloudshell:~ (qwiklabs-gcp-02-c592df700044) $
```

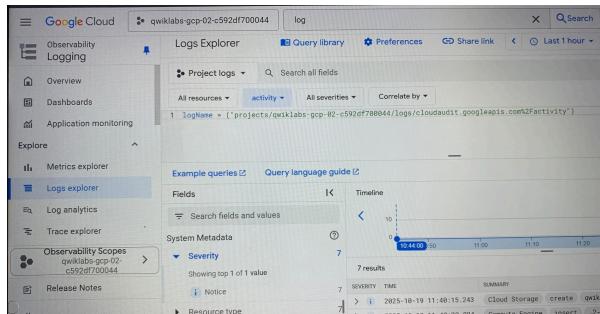
This command removes the google cloud storage bucket that was created earlier along with all of its contents.

Second Step: Export The Audit Logs

The activity I generated in the previous task was recorded as audit logs. Here, I'll export these logs to a BigQuery dataset for further analysis.

I inputted the following query into the Query builder.

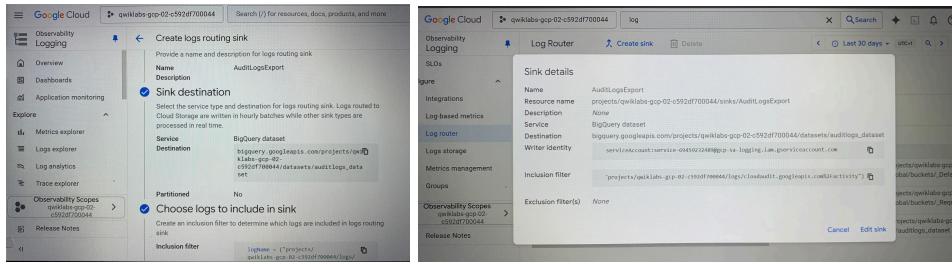
`logName = ("projects/Project ID/logs/cloudaudit.googleapis.com%2Factivity")`



The screenshot shows the Google Cloud Logging interface with the "Logs Explorer" tab selected. A search bar at the top contains the query: `logName = ("projects/qwiklabs-gcp-02-c592df700044/logs/cloudaudit.googleapis.com%2Factivity")`. Below the search bar, there are sections for "Fields" and "Timeline". The timeline shows a single event from 2025-10-19 11:48:15.243. The event details are listed in a table:

SEVERITY	TIME	SUMMARY
INFO	2025-10-19 11:48:15.243	Cloud Storage create (qwiklab...)
INFO	2025-10-19 11:48:20.894	Compute Engine insert -

This query filters for Cloud Audit within your project.



After creating an **AuditLogsExport** sink, all future logs will now be exported to BigQuery and the BigQuery tools can be used to perform analysis on the audit log data.

Third Step: Generate More Account Activity

Here, I created and deleted cloud resources to generate additional account activity which I'll then access in BigQuery to extract additional insights from the logs.

I inputted the following commands into the cloud shell terminal;

```

gcloud storage buckets create gs://$DEVSHELL_PROJECT_ID-test
echo "this is another sample file" > sample.txt
gcloud storage cp sample.txt gs://$DEVSHELL_PROJECT_ID-test
gcloud compute instances delete --zone=us-west1-b
Creating gs://$DEVSHELL_PROJECT_ID-test/
Creating gs://$DEVSHELL_PROJECT_ID-test/sample.txt
Completed file 1/1 22.08/22.08
The 'keep-disk' flag is given and specifies them for keeping. Deleting a disk is irreversible and any data on the disk will be lost.
- (default=us-west1-b) I
Do you want to continue (Y/n)? Y

```

These commands generate more activity to view in the audit logs exported to BigQuery.

I was prompted to input **Y**, upon this I noticed I created two buckets and deleted a Compute Engine Instance.

When the prompt appeared after a few minutes, I continued by inputting the following commands into the cloud shell terminal.

gcloud storage rm --recursive gs://\$DEVSHELL_PROJECT_ID-test

```

gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID-test
Completed file 1/1 22.08/22.08
The 'keep-disk' flag is given and specifies them for keeping. Deleting a disk is irreversible and any data on the disk will be lost.
- (default=us-west1-b) I
Do you want to continue (Y/n)? Y
Deleted https://www.googleapis.com/storage/v1/b/projects/quicklab-gcp-02-c592d7f00044/o/us-west1-b/instances/default-us-west1
student_03_23abed0fcfc@cloudshell: ~ (quicklab-gcp-02-c592d7f00044) gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID-test
Completed 0
Removing object
Removing object
Completed 0
Removing object
Removing object
Completed 1/1
Removing object
Completed 1/1
Removing object
Completed 1/1
student_03_23abed0fcfc@cloudshell: ~ (quicklab-gcp-02-c592d7f00044) I

```

With this, I deleted both buckets.

Fourth Step: Signed In As The Second User

I switched google cloud accounts by logging into the google cloud console using the second user account provided in the Lab details.

I used this account to analyze the logs.

Fifth Step: Analyze The Admin Activity Logs

Here, I'll review the admin activity logs generated in the previous step. My goal is to identify and apply filters to isolate logs that may indicate suspicious activity. This will enable me to export this subset of logs and streamline the process of analyzing them for potential issues.

I inputted the following command into the **Query builder** field;

```
logName = ("projects/"PROJECT_ID"/logs/cloudaudit.googleapis.com%2Factivity")
```

The screenshot shows the Google Cloud Logging interface with the project set to "qwiklabs-gcp-02-c592df700044". The "Logs Explorer" tab is selected. In the "Query builder" field, the query `logName = ("projects/qwiklabs-gcp-02-c592df700044/logs/cloudaudit.googleapis.com%2Factivity")` is entered. The results pane shows 25 results, all of which are severity: NOTICE. One result is expanded to show details like insertId, logName, protoPayload, and resource. The timeline at the top indicates the data covers from 2025-10-14 12:13:45.579 to 2025-10-14 12:14:42.937.

In the **Query results**, I located the entry indicating that a cloud storage bucket was deleted, it contained the **storage.bucket.delete** summary field. Summary fields are included in the log results to highlight important information about the log entry. This entry refers to [storage.googleapis.com](#), which calls the **storage.buckets.delete** method to delete a bucket. The bucket name is the same name as my project : **PROJECT_ID**

This screenshot shows the same Google Cloud Logging interface as above, but with a specific log entry expanded. The expanded entry shows the full `protoPayload` object, which includes fields like `insertId`, `logName`, `protoPayload` (containing `type`, `authenticationInfo`, `principalEmail`, `authorizationInfo`, `methodType`, `requestMetadata`, `resourceLocation`, `resourceName`, `serviceName`, `status`, and `receiveTimestamp`), and `severity`. The `protoPayload` object is very large and truncated.

Within this entry, I clicked on the [storage.googleapis.com](#) text, and selected **Show matching entries**. The **Query results** now display only six entries related to **created and deleted** cloud storage buckets. In the Query editor field, I noticed the; **protoPayload.serviceName="storage.googleapis.com"** line was added to the query builder, this filters my query to entries only matching [storage.googleapis.com](#). Within those query results, I clicked **storage.buckets.delete** in one of the entries, and selected

Show matching entries. I Notice another line was added to the Query builder text:

The screenshot shows the Google Cloud Logs Explorer interface. The left sidebar has 'Logs explorer' selected. The main area shows a query builder with the following text:

```
1 logName = ('projects/qwiklabs-gcp-02-c592df700044/logs/cloudaudit.googleapis.com%2Factivity'
2 protoPayload.methodName='storage.buckets.delete'
```

Below the query, there's a 'Fields' section with 'Severity' expanded, showing 'Notice' as the top value. A timeline at the bottom indicates the results are from 11:40 AM to 12:50 PM on October 19, 2025. The results pane shows 3 results.

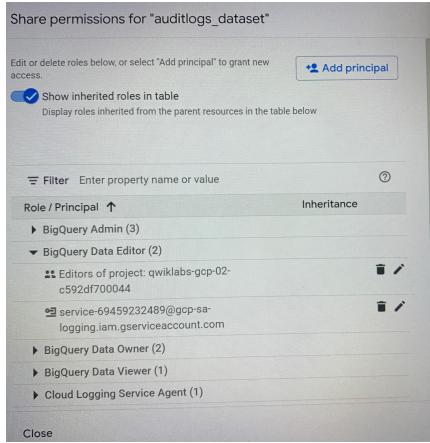
The **Query results** now display all entries related to deleted Cloud Storage buckets. I can use this technique to easily locate specific events. In the **Query results**, I expanded a **storage.buckets.delete** event and noticed the **principalEmail** field which displays the email address of the user account that performed this action which is the user 1 account I used to generate the user activity.

The screenshot shows the 'Logs Explorer' results page. It displays a single log entry for a Cloud Storage bucket deletion on October 19, 2025, at 11:41:12.702. The log entry details the event type, time, source, method, resource, and principal email.

TYPE	TIME	SUMMARY
i	2025-10-19 11:41:12.702	Cloud Storage delete qwiklabs-gcp-02-c592df700044 student-03-252e62d9fc3787e "storage.buckets.delete", principal_email: "student-03-252e62d9fc37@qwiklabs.net"

Final Step: Use BigQuery to analyze the audit log.

I've generated and exported logs to a BigQuery dataset. In this step, I'll analyze the logs using the Query editor. I expanded the **explorer** pane and the **auditlogs_dataset** dataset is displayed. Next, I verified that the BigQuery dataset has appropriate permissions to allow the export writer to store log entries.



Then, I expanded the **explorer** pane next to the **auditlogs_dataset** dataset to view the **cloudaudit_googleapis_com_acitivity** table. This table contains my exported logs. I selected the **cloudaudit_googleapis_com_acitivity** table. The table schema displays. I took a moment to review the table schema and details.

Field name	Type	Mode	Description	Key
logname	STRING	NULLABLE		
resource	RECORD	NULLABLE		
protoPayload.auditLog	RECORD	NULLABLE		
protoPayload.timestamp	STRING	NULLABLE		
protoPayload.receiveTimestamp	TIMESTAMP	NULLABLE		
severity	STRING	NULLABLE		

I Expanded the **Open** in the drop-down menu and selected **SQL Query > New tab**. In the **Untitled query** tab of the query builder, I deleted any existing text and inputted the following command:

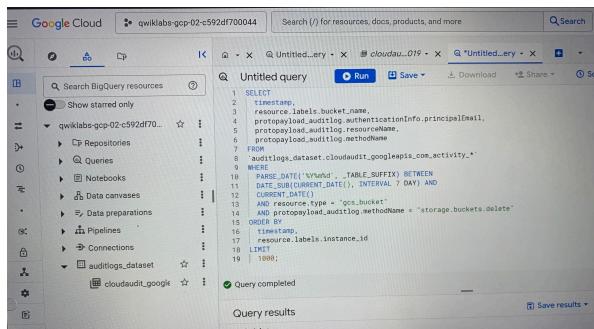
```

SELECT
  timestamp,
  resource.labels.instance_id,
  protoPayload.auditLog.authenticationInfo.principalEmail,
  protoPayload.auditLog.resourceName,
  protoPayload.auditLog.methodName,
  protoPayload.auditLog.labels,
  auditLogs.dataset,
  cloudaudit.googleapis.com.activity.*
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.name = 'CREATE'
  AND protoPayload.auditLog.methodName = 'V1'
  AND protoPayload.auditLog.labels.compute.instances.delete = 0
ORDER BY
  timestamp DESC
LIMIT 10000;
  
```

This query returns the users that deleted virtual machines in the last 7 days.

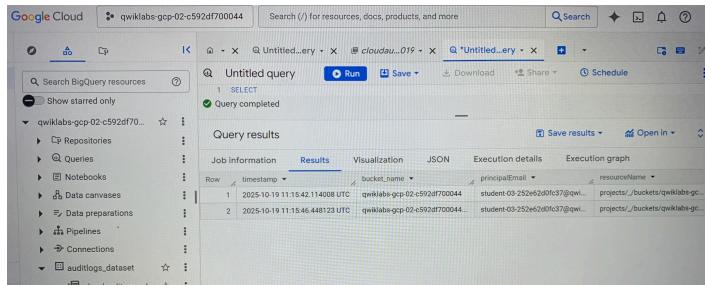
After a couple of seconds, BigQuery returns each time a user deleted a Compute Engine virtual machine within the past 7 days. I noticed one entry, which is the activity I generated in the previous steps as user 1. BigQuery shows only the activity that occurred after I created the export.

I Replaced the previous query in the **Untitled query** tab with the following:



```
SELECT
    timestamp,
    resource.labels.bucket_name,
    protosPayload.auditLog.authenticationInfo.principalEmail,
    protosPayload.auditLog.authenticationInfo.principalName,
    protosPayload.auditLog.methodName
FROM
    `cloudaudit.googleapis.com_activity_*`
WHERE
    PARSE_DATE('%Y-%m-%dT%H:%M:%S.%fZ', timestamp) >= DATE_SUB(CURRENT_DATE(), INTERVAL 7 DAY) AND
    PARSE_DATE('%Y-%m-%dT%H:%M:%S.%fZ', timestamp) < CURRENT_DATE()
AND
    protosPayload.auditLog.methodName = "storage.buckets.delete"
ORDER BY
    timestamp
LIMIT
    1000;
```

This query returns the users that deleted Cloud Storage buckets in the last 7 days. I noticed two entries, which is the activity I generated in the previous Steps as user 1.



Row	timestamp	bucket.name	principalEmail	resourceName
1	2025-10-19 11:15:42.114008 UTC	qwiklabs-gcp-02-c592df700044	student-03-252e020fc37@qwi...	projects/_buckets/qwiklabs-g...
2	2025-10-19 11:15:46.448123 UTC	qwiklabs-gcp-02-c592df700044..	student-03-252e020fc37@qwi...	projects/_buckets/qwiklabs-g...

The ability to analyze audit logs in BigQuery is very powerful. In this lab activity, I viewed just two examples of querying audit logs.

CONCLUSION

I have successfully queried in Logs Explorer. I then exported logs and created a dataset that I analyzed in BigQuery. I have shown how I can use audit logs and filter for types of malicious activity and then further analyze those logs in BigQuery as a way to analyze the threats.

