Course 4_Lab 3: Analyzing Audit logs using BigQuery

Scenario

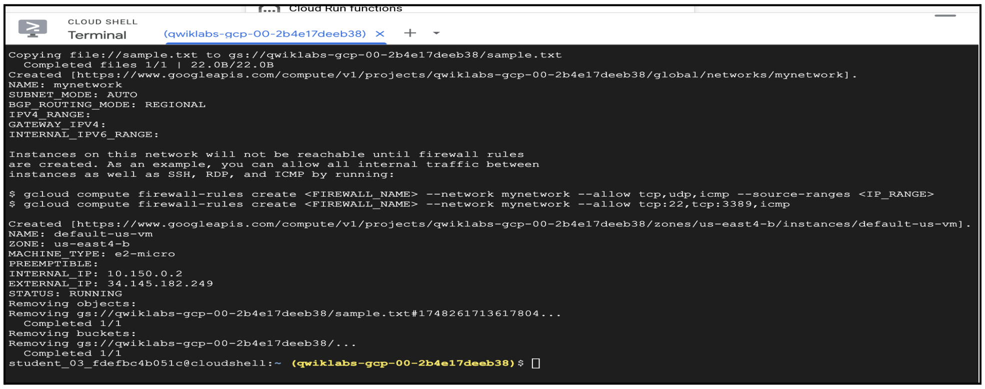
Cymbal Bank has officially migrated to its hybrid cloud solution and successfully deployed its workflows on the new cloud environment. Unfortunately, the Security Engineering team has been notified of a high severity alert involving unauthorized access to several of its cloud resources. This is alarming since malicious actors can use compromised cloud resources to exfiltrate data and launch attacks on other systems. It is your first time experiencing a security incident. Your team lead, Chloe, recognizes this as a valuable opportunity for you to learn the processes and procedures involved with incident response. You've been assigned to shadow and observe Hannah, an incident responder on the Incident Response Team which is a unit of the Security Engineering department. Hannah has provided you with access to the alert's logs which you'll use to investigate the malicious activity. You want to get a better understanding of the security incident so you have set up a test environment to recreate the incident and analyze the artifacts. You will use two separate user accounts: one account will generate the malicious activity, and the other account will be used to investigate the activity.

Here's how you'll do this task. **First**, you'll recreate the security incident by generating activity from the first user account. **Next**, you'll export the logs for further analysis. **Then**, you'll continue recreating the incident and generate additional user activity. **Finally**, you'll utilize BigQuery to analyze the logs.

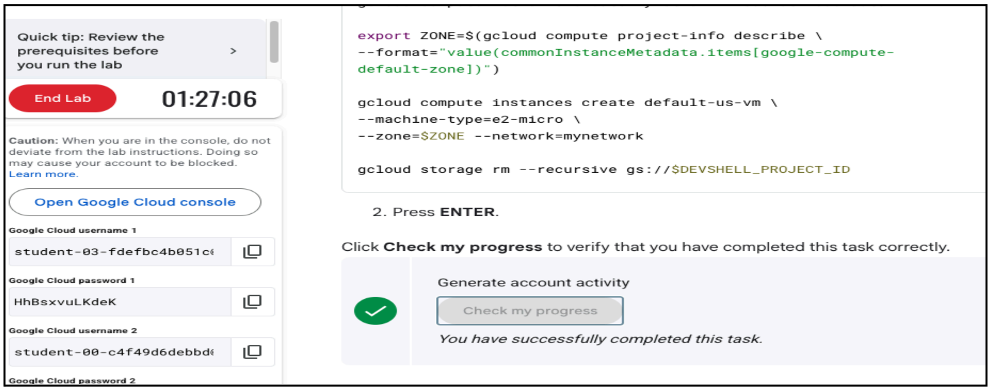
MY WORK:

Task 1: Generate account activity

In this task, a command provided by Google was added to Cloud Shell to generate account activity.



```
Copying file://sample.txt to gs://qwiklabs-gcp-00-2b4e17deeb38/sample.txt
  Completed files 1/1 | 22.0B/22.0B
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-2b4e17deeb38/global/networks/mynetwork].
NAME: mynetwork
SUBNET_MODE: AUTO
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
INTERNAL_IPV6_RANGE:

Instances on this network will not be reachable until firewall rules
are created. As an example, you can allow all internal traffic between
instances as well as SSH, RDP, and ICMP by running:

$ gcloud compute firewall-rules create <FIREWALL_NAME> --network mynetwork --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network mynetwork --allow tcp:22,tcp:3389,icmp

Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-2b4e17deeb38/zones/us-east4-b/instances/default-us-vm].
NAME: default-us-vm
ZONE: us-east4-b
MACHINE_TYPE: e2-micro
PREEMPTIBLE:
INTERNAL_IP: 10.150.0.2
EXTERNAL_IP: 34.145.182.249
STATUS: RUNNING
Removing objects:
Removing gs://qwiklabs-gcp-00-2b4e17deeb38/sample.txt#1748261713617804...
  Completed 1/1
Removing buckets:
Removing gs://qwiklabs-gcp-00-2b4e17deeb38/...
  Completed 1/1
student_03_fdefbc4b051c@cloudshell:~ (qwiklabs-gcp-00-2b4e17deeb38)$ 
```



Quick tip: Review the prerequisites before you run the lab

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1: student-03-fdefbc4b051c

Google Cloud password 1: HhBsxvuLKdeK

Google Cloud username 2: student-00-c4f49d6debbd

Google Cloud password 2

```
export ZONE=$(gcloud compute project-info describe \
--format="value(commonInstanceMetadata.items[google-compute-
default-zone])")

gcloud compute instances create default-us-vm \
--machine-type=e2-micro \
--zone=$ZONE --network=mynetwork

gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID
```

2. Press **ENTER**.

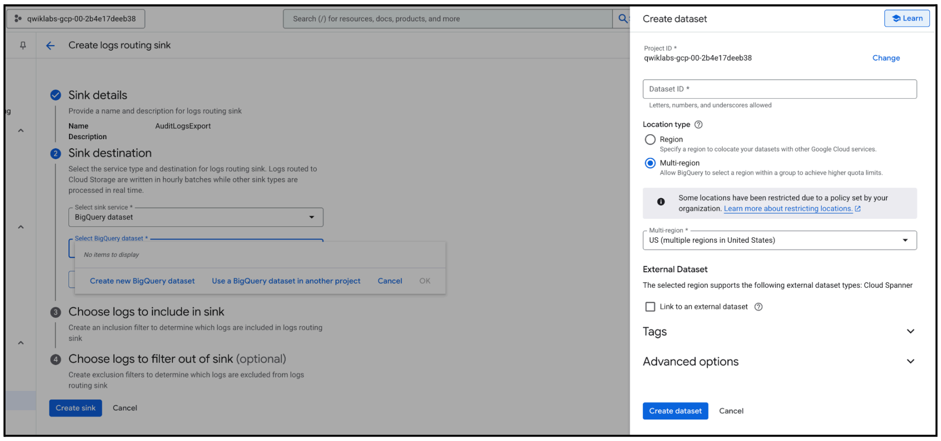
Click **Check my progress** to verify that you have completed this task correctly.

✓ Generate account activity

You have successfully completed this task.

Task 2: Export the audit logs

This task focused on exporting the cloud logs. I used Logs Explorer to run a query and create a sink to export the logs based on details provided by Google. Specifically a sink is a configuration that specifies how and where log entries are exported. Future logs will be exported to Big Query, per this lab.


qwiklabs-gcp-00-2b4e17deeb38
Search (/) for resources, docs, products, and more

Create logs routing sink

Sink details

Provide a name and description for logs routing sink

Name AuditLogsExport

Description

Sink destination

Select the service type and destination for logs routing sink. Logs routed to Cloud Storage are written in hourly batches while other sink types are processed in real time.

Select sink service * BigQuery dataset

Select BigQuery dataset *

No items to display

Create new BigQuery dataset
Use a BigQuery dataset in another project
Cancel
OK

Choose logs to include in sink

Create an inclusion filter to determine which logs are included in logs routing sink

Choose logs to filter out of sink (optional)

Create exclusion filters to determine which logs are excluded from logs routing sink

Create dataset

Project ID *
qwiklabs-gcp-00-2b4e17deeb38

Dataset ID *

Letters, numbers, and underscores allowed

Location type

○ Region
Specify a region to colocate your datasets with other Google Cloud services.

● Multi-region
Allow BigQuery to select a region within a group to achieve higher quota limits.

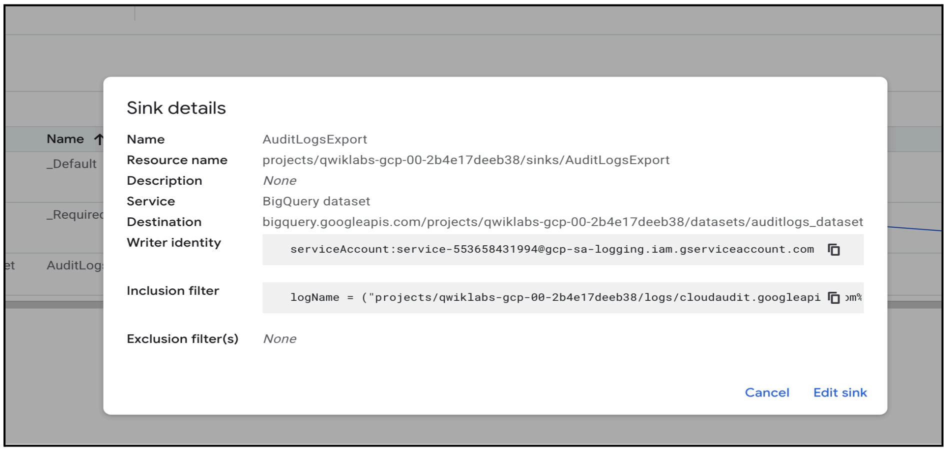
Some locations have been restricted due to a policy set by your organization. Learn more about restricting locations.

Multi-region * US (multiple regions in United States)

External Dataset

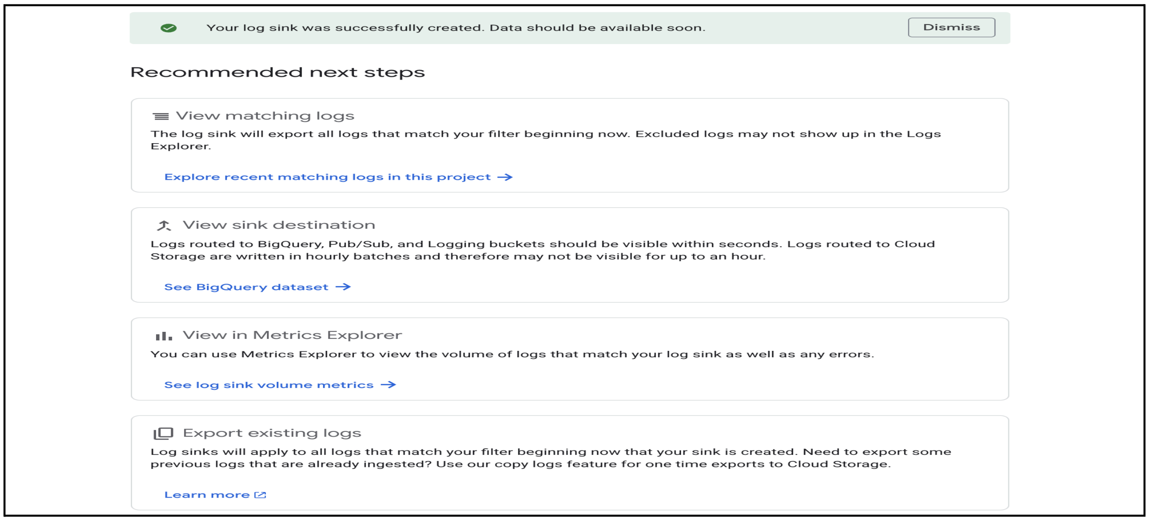
The selected region supports the following external dataset types: Cloud Spanner

□ Link to an external dataset



Sink details

Name	AuditLogsExport
Resource name	projects/qwiklabs-gcp-00-2b4e17deeb38/sinks/AuditLogsExport
Description	*None*
Service	BigQuery dataset
Destination	bigquery.googleapis.com/projects/qwiklabs-gcp-00-2b4e17deeb38/datasets/auditlogs_dataset
Writer identity	`serviceAccount:service-553658431994@gcp-sa-logging.iam.gserviceaccount.com`
Inclusion filter	`logName = ("projects/qwiklabs-gcp-00-2b4e17deeb38/logs/cloudaudit.googleapi ɔm%`
Exclusion filter(s)	*None*


Your log sink was successfully created. Data should be available soon.

Recommended next steps

View matching logs

The log sink will export all logs that match your filter beginning now. Excluded logs may not show up in the Logs Explorer.

View sink destination

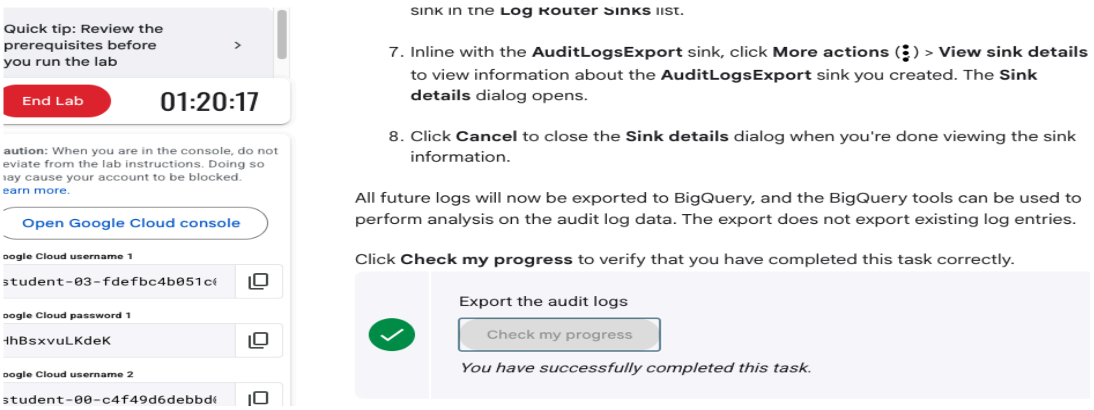
Logs routed to BigQuery, Pub/Sub, and Logging buckets should be visible within seconds. Logs routed to Cloud Storage are written in hourly batches and therefore may not be visible for up to an hour.

View in Metrics Explorer

You can use Metrics Explorer to view the volume of logs that match your log sink as well as any errors.

Export existing logs

Log sinks will apply to all logs that match your filter beginning now that your sink is created. Need to export some previous logs that are already ingested? Use our copy logs feature for one time exports to Cloud Storage.



Quick tip: Review the prerequisites before you run the lab

01:20:17

aution: When you are in the console, do not eviate from the lab instructions. Doing so ıay cause your account to be blocked. earn more.

oogle Cloud username 1

student-03-fdefbc4b051c(

oogle Cloud password 1

HhBsxvuLKdeK

oogle Cloud username 2

student-00-c4f49d6debbd(

sink in the **Log Router Sinks** list.

7. Inline with the **AuditLogsExport** sink, click **More actions** (⋮) > **View sink details** to view information about the **AuditLogsExport** sink you created. The **Sink details** dialog opens.

8. Click **Cancel** to close the **Sink details** dialog when you're done viewing the sink information.

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.

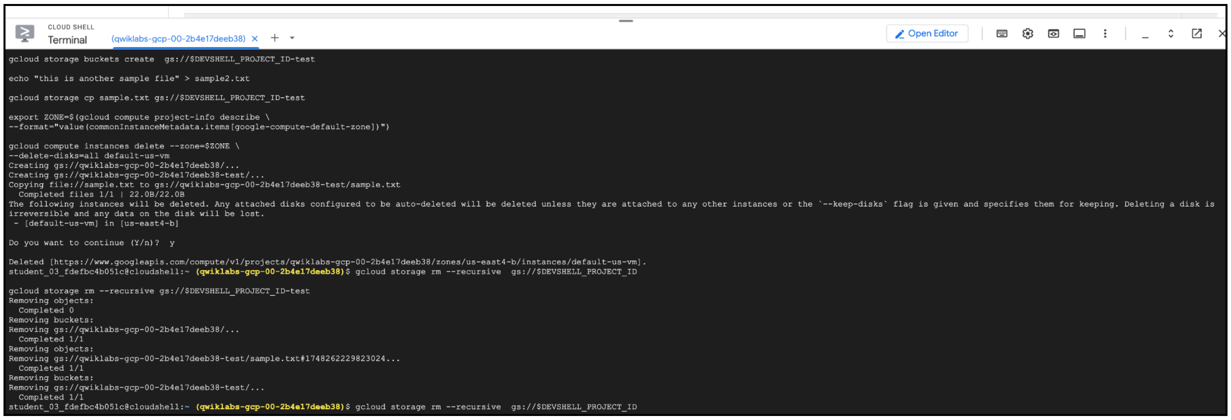
Click **Check my progress** to verify that you have completed this task correctly.

✓ Export the audit logs

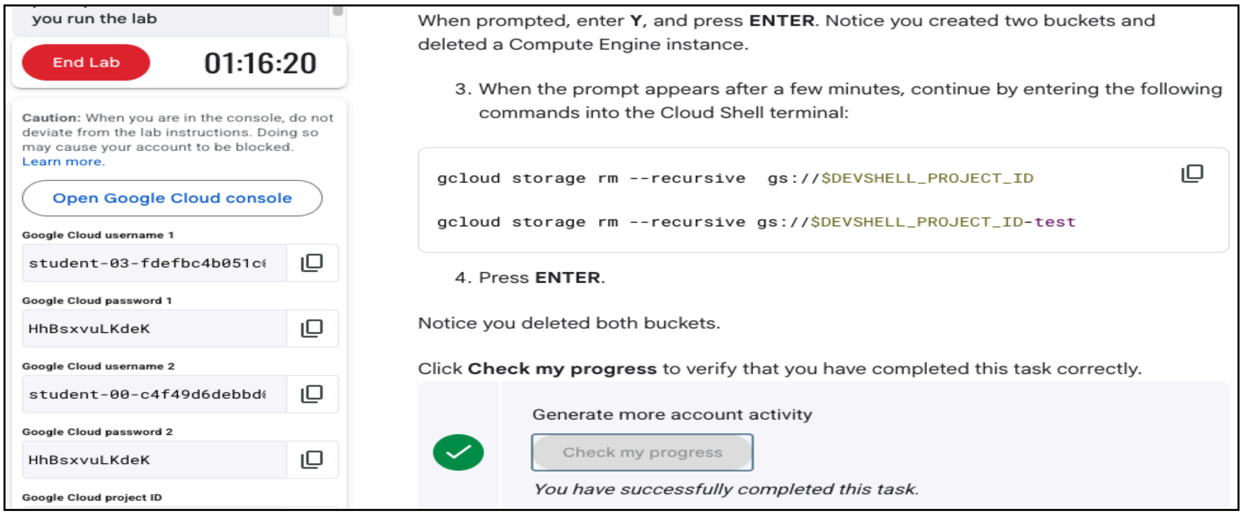
You have successfully completed this task.

Task 3: Generate more account activity

For this task more account activity was generated. A Google command was input into the Cloud Shell terminal to create two storage buckets and delete a Compute Engine instance. Within this task, the buckets were also deleted.



```
gcloud storage buckets create  gs://$DEVSHELL_PROJECT_ID-test

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

gcloud storage cp sample.txt gs://$DEVSHELL_PROJECT_ID-test

export ZONE=$(gcloud compute project-info describe \
--format="value(commonInstanceMetadata.items[google-compute-default-zone])")

gcloud compute instances delete --zone=$ZONE \
--delete-disks=all default-us-vm
Creating gs://qwiklabs-gcp-00-2b4e17deeb38/...
Creating gs://qwiklabs-gcp-00-2b4e17deeb38-test/...
Copying file://sample.txt to gs://qwiklabs-gcp-00-2b4e17deeb38-test/sample.txt
  Completed files 1/1 | 22.0B/22.0B
The following instances will be deleted. Any attached disks configured to be auto-deleted will be deleted unless they are attached to any other instances or the `--keep-disks` flag is given and specifies them for keeping. Deleting a disk is
irreversible and any data on the disk will be lost.
 - [default-us-vm] in [us-east4-b]

Do you want to continue (Y/n)?  y

Deleted [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-2b4e17deeb38/zones/us-east4-b/instances/default-us-vm].
student_03_fdefbc4b051c@cloudshell:~ (qwiklabs-gcp-00-2b4e17deeb38)$ gcloud storage rm --recursive  gs://$DEVSHELL_PROJECT_ID

gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID-test
Removing objects:
  Completed 0
Removing buckets:
Removing gs://qwiklabs-gcp-00-2b4e17deeb38/...
  Completed 1/1
Removing objects:
Removing gs://qwiklabs-gcp-00-2b4e17deeb38-test/sample.txt#1748262229823024...
  Completed 1/1
Removing buckets:
Removing gs://qwiklabs-gcp-00-2b4e17deeb38-test/...
  Completed 1/1
student_03_fdefbc4b051c@cloudshell:~ (qwiklabs-gcp-00-2b4e17deeb38)$ gcloud storage rm --recursive  gs://$DEVSHELL_PROJECT_ID
```



you run the lab

01:16:20

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1

student-03-fdefbc4b051c(

Google Cloud password 1

HhBsxvuLKdeK

Google Cloud username 2

student-00-c4f49d6debbd(

Google Cloud password 2

HhBsxvuLKdeK

Google Cloud project ID

When prompted, enter **Y**, and press **ENTER**. Notice you created two buckets and deleted a Compute Engine instance.

3. When the prompt appears after a few minutes, continue by entering the following commands into the Cloud Shell terminal:

```
gcloud storage rm --recursive  gs://$DEVSHELL_PROJECT_ID

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

4. Press **ENTER**.

Notice you deleted both buckets.

Click **Check my progress** to verify that you have completed this task correctly.

✓ Generate more account activity

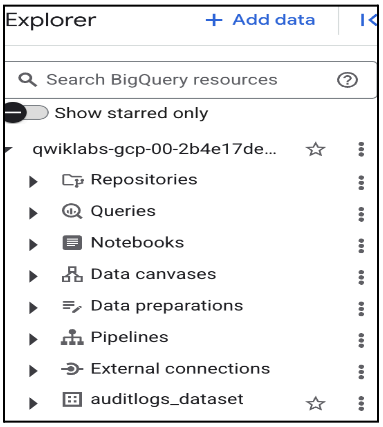
You have successfully completed this task.

Task 4: Sign in as the second user

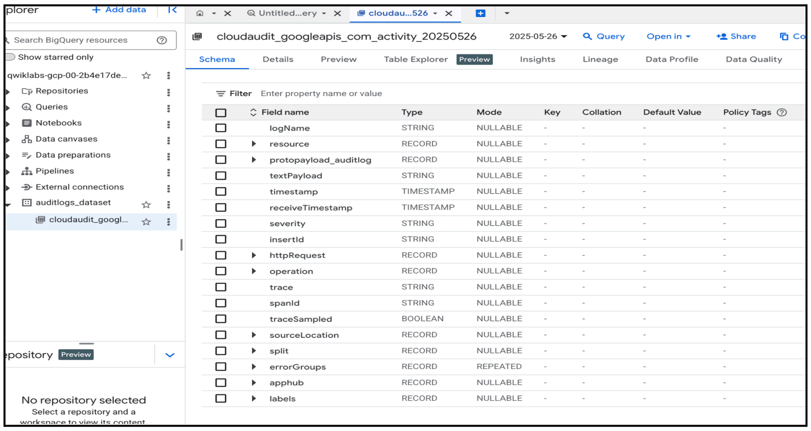
For this task, no screenshots were taken as I simply signed into a second account user.

Task 5: Analyze the Admin Activity logs

In this task, I reviewed the Admin activity logs generated in Task 3. In the screenshots below, it shows the different stages to complete the task as well as the logs that were reviewed. Running the queries for the deleted storage buckets allowed for more information to analyze within the logs.



Explorer
+ Add data
Search BigQuery resources
Show starred only
qwiklabs-gcp-00-2b4e17de...
- Repositories
- Queries
- Notebooks
- Data canvases
- Data preparations
- Pipelines
- External connections
- auditlogs_dataset

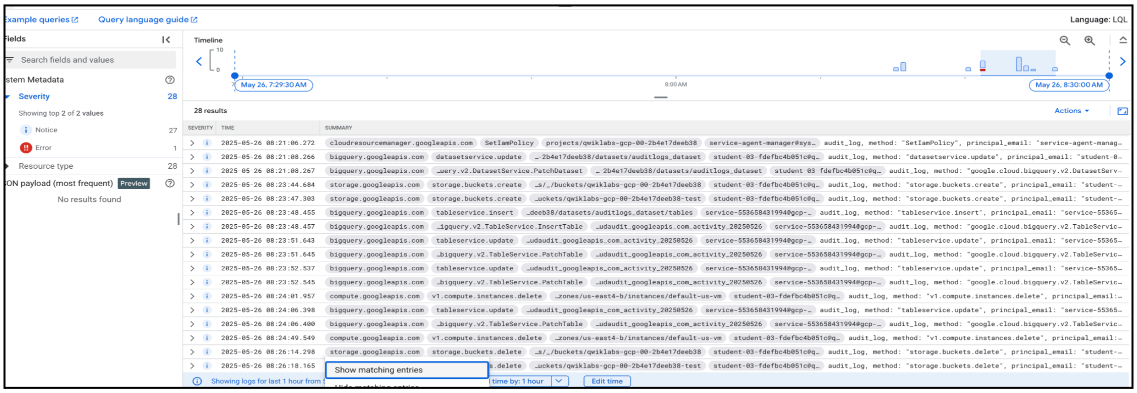


No repository selected
Select a repository and a workspace to view its content

cloudaudit_googleapis_com_activity_20250526 2025-05-26

Filter Enter property name or value

	Field name	Type	Mode	Key	Collation	Default Value	Policy Tags
□	logName	STRING	NULLABLE	-	-	-	-
□	▸ resource	RECORD	NULLABLE	-	-	-	-
□	▸ protopayload_auditlog	RECORD	NULLABLE	-	-	-	-
□	textPayload	STRING	NULLABLE	-	-	-	-
□	timestamp	TIMESTAMP	NULLABLE	-	-	-	-
□	receiveTimestamp	TIMESTAMP	NULLABLE	-	-	-	-
□	severity	STRING	NULLABLE	-	-	-	-
□	insertId	STRING	NULLABLE	-	-	-	-
□	▸ httpRequest	RECORD	NULLABLE	-	-	-	-
□	▸ operation	RECORD	NULLABLE	-	-	-	-
□	trace	STRING	NULLABLE	-	-	-	-
□	spanId	STRING	NULLABLE	-	-	-	-
□	traceSampled	BOOLEAN	NULLABLE	-	-	-	-
□	▸ sourceLocation	RECORD	NULLABLE	-	-	-	-
□	▸ split	RECORD	NULLABLE	-	-	-	-
□	▸ errorGroups	RECORD	REPEATED	-	-	-	-
□	▸ apphub	RECORD	NULLABLE	-	-	-	-
□	▸ labels	RECORD	NULLABLE	-	-	-	-

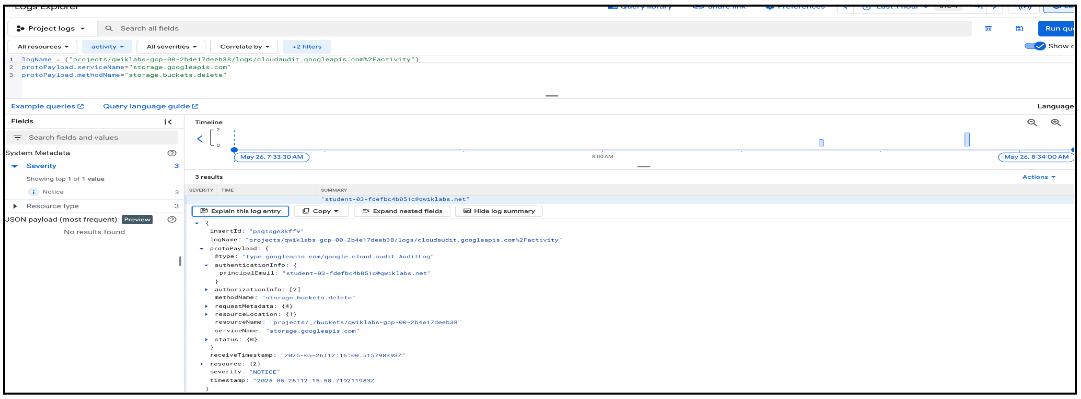


stem Metadata
Severity 28
Showing top 2 of 2 values
Notice 27
Error 1
Resource type 28
ON payload (most frequent) Preview
No results found

28 results

```
SEVERITY TIME                     SUMMARY
>  i  2025-05-26 08:21:06.272  cloudresourcemanager.googleapis.com  SetIamPolicy  projects/qwiklabs-gcp-00-2b4e17deeb38  service-agent-manager@sys…  audit_log, method: "SetIamPolicy", principal_email: "service-agent-manag…
>  i  2025-05-26 08:21:08.266  bigquery.googleapis.com  datasetservice.update  …-2b4e17deeb38/datasets/auditlogs_dataset  student-03-fdefbc4b051c@q…  audit_log, method: "datasetservice.update", principal_email: "student-0…
>  i  2025-05-26 08:21:08.267  bigquery.googleapis.com  …uery.v2.DatasetService.PatchDataset  …-2b4e17deeb38/datasets/auditlogs_dataset  student-03-fdefbc4b051c@q…  audit_log, method: "google.cloud.bigquery.v2.DatasetServ…
>  i  2025-05-26 08:23:44.684  storage.googleapis.com  storage.buckets.create  …s/_/buckets/qwiklabs-gcp-00-2b4e17deeb38  student-03-fdefbc4b051c@q…  audit_log, method: "storage.buckets.create", principal_email: "student-…
>  i  2025-05-26 08:23:47.303  storage.googleapis.com  storage.buckets.create  …uckets/qwiklabs-gcp-00-2b4e17deeb38-test  student-03-fdefbc4b051c@q…  audit_log, method: "storage.buckets.create", principal_email: "student-…
>  i  2025-05-26 08:23:48.455  bigquery.googleapis.com  tableservice.insert  …deeb38/datasets/auditlogs_dataset/tables  service-553658431994@gcp-…  audit_log, method: "tableservice.insert", principal_email: "service-55365…
>  i  2025-05-26 08:23:48.457  bigquery.googleapis.com  …igquery.v2.TableService.InsertTable  …udaudit_googleapis_com_activity_20250526  service-553658431994@gcp-…  audit_log, method: "google.cloud.bigquery.v2.TableServic…
>  i  2025-05-26 08:23:51.643  bigquery.googleapis.com  tableservice.update  …udaudit_googleapis_com_activity_20250526  service-553658431994@gcp-…  audit_log, method: "tableservice.update", principal_email: "service-55365…
>  i  2025-05-26 08:23:51.645  bigquery.googleapis.com  …bigquery.v2.TableService.PatchTable  …udaudit_googleapis_com_activity_20250526  service-553658431994@gcp-…  audit_log, method: "google.cloud.bigquery.v2.TableServic…
>  i  2025-05-26 08:23:52.537  bigquery.googleapis.com  tableservice.update  …udaudit_googleapis_com_activity_20250526  service-553658431994@gcp-…  audit_log, method: "tableservice.update", principal_email: "service-55365…
>  i  2025-05-26 08:23:52.545  bigquery.googleapis.com  …bigquery.v2.TableService.PatchTable  …udaudit_googleapis_com_activity_20250526  service-553658431994@gcp-…  audit_log, method: "google.cloud.bigquery.v2.TableServic…
>  i  2025-05-26 08:24:01.957  compute.googleapis.com  v1.compute.instances.delete  …zones/us-east4-b/instances/default-us-vm  student-03-fdefbc4b051c@q…  audit_log, method: "v1.compute.instances.delete", principal_email:…
>  i  2025-05-26 08:24:06.398  bigquery.googleapis.com  tableservice.update  …udaudit_googleapis_com_activity_20250526  service-553658431994@gcp-…  audit_log, method: "tableservice.update", principal_email: "service-55365…
>  i  2025-05-26 08:24:06.400  bigquery.googleapis.com  …bigquery.v2.TableService.PatchTable  …udaudit_googleapis_com_activity_20250526  service-553658431994@gcp-…  audit_log, method: "google.cloud.bigquery.v2.TableServic…
>  i  2025-05-26 08:24:49.549  compute.googleapis.com  v1.compute.instances.delete  …zones/us-east4-b/instances/default-us-vm  student-03-fdefbc4b051c@q…  audit_log, method: "v1.compute.instances.delete", principal_email:…
>  i  2025-05-26 08:26:14.298  storage.googleapis.com  storage.buckets.delete  …s/_/buckets/qwiklabs-gcp-00-2b4e17deeb38  student-03-fdefbc4b051c@q…  audit_log, method: "storage.buckets.delete", principal_email: "student-…
>  i  2025-05-26 08:26:18.165  s.delete  …uckets/qwiklabs-gcp-00-2b4e17deeb38-test  student-03-fdefbc4b051c@q…  audit_log, method: "storage.buckets.delete", principal_email: "student-…
```

Showing logs for last 1 hour from



```
logName = ("projects/qwiklabs-gcp-00-2b4e17deeb38/logs/cloudaudit.googleapis.com%2Factivity")
protoPayload.serviceName="storage.googleapis.com"
protoPayload.methodName="storage.buckets.delete"
```

System Metadata
Severity 3
Showing top 1 of 1 value
Notice 3
Resource type 3
JSON payload (most frequent) Preview
No results found

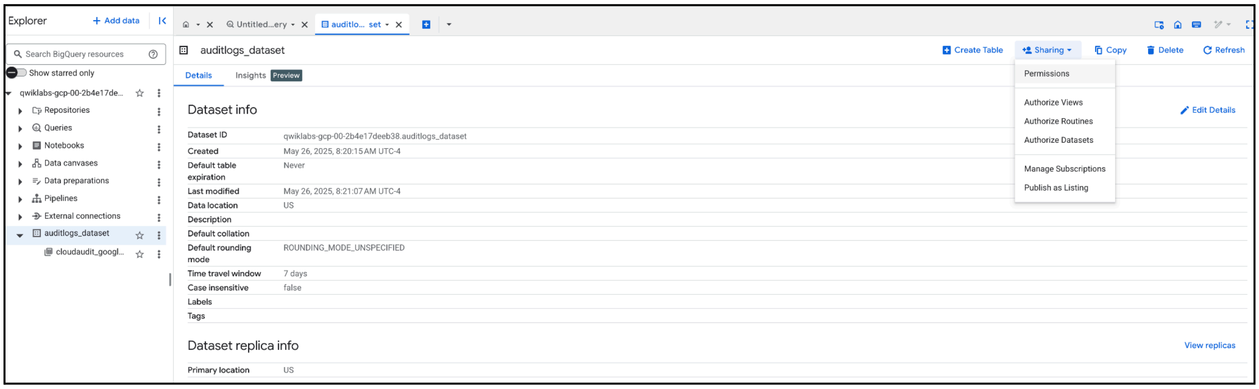
3 results

SEVERITY TIME SUMMARY
"student-03-fdefbc4b051c@qwiklabs.net"

```
{
  insertId: "paq1sge3kff9"
  logName: "projects/qwiklabs-gcp-00-2b4e17deeb38/logs/cloudaudit.googleapis.com%2Factivity"
  protoPayload: {
   @type: "type.googleapis.com/google.cloud.audit.AuditLog"
   authenticationInfo: {
    principalEmail: "student-03-fdefbc4b051c@qwiklabs.net"
   }
   authorizationInfo: [2]
   methodName: "storage.buckets.delete"
   requestMetadata: {4}
   resourceLocation: {1}
   resourceName: "projects/_/buckets/qwiklabs-gcp-00-2b4e17deeb38"
   serviceName: "storage.googleapis.com"
   status: {0}
  }
  receiveTimestamp: "2025-05-26T12:16:00.515798393Z"
  resource: {2}
  severity: "NOTICE"
  timestamp: "2025-05-26T12:15:58.719211983Z"
}
```

Task 6: Use BigQuery to analyze the audit logs

This task focused on analyzing the logs in Big Query that were generated in the previous tasks.



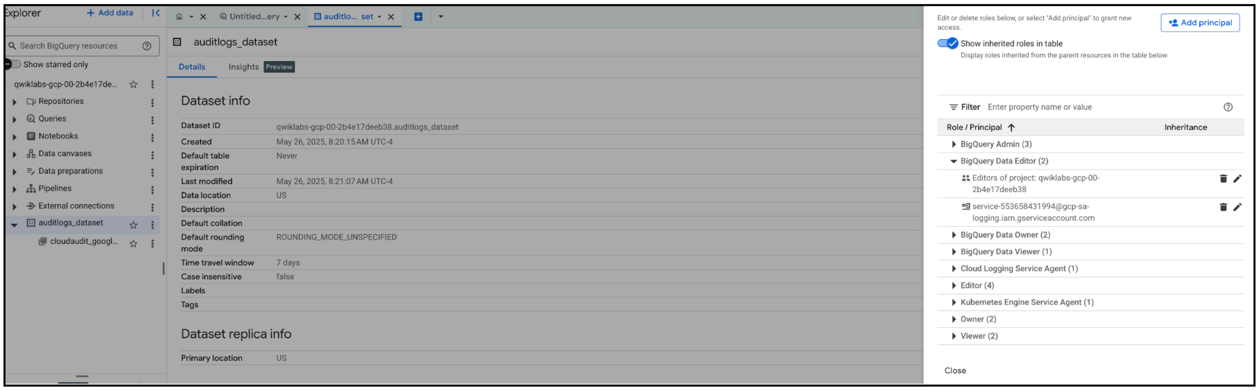
auditlogs_dataset

Dataset info

Dataset ID	qwiklabs-gcp-00-2b4e17deeb38.auditlogs_dataset
Created	May 26, 2025, 8:20:15 AM UTC-4
Default table expiration	Never
Last modified	May 26, 2025, 8:21:07 AM UTC-4
Data location	US
Description	
Default collation	
Default rounding mode	ROUNDING_MODE_UNSPECIFIED
Time travel window	7 days
Case insensitive	false
Labels	
Tags	

Dataset replica info

Primary location	US



auditlogs_dataset

Dataset info

Dataset ID	qwiklabs-gcp-00-2b4e17deeb38.auditlogs_dataset
Created	May 26, 2025, 8:20:15 AM UTC-4
Default table expiration	Never
Last modified	May 26, 2025, 8:21:07 AM UTC-4
Data location	US
Description	
Default collation	
Default rounding mode	ROUNDING_MODE_UNSPECIFIED
Time travel window	7 days
Case insensitive	false
Labels	
Tags	

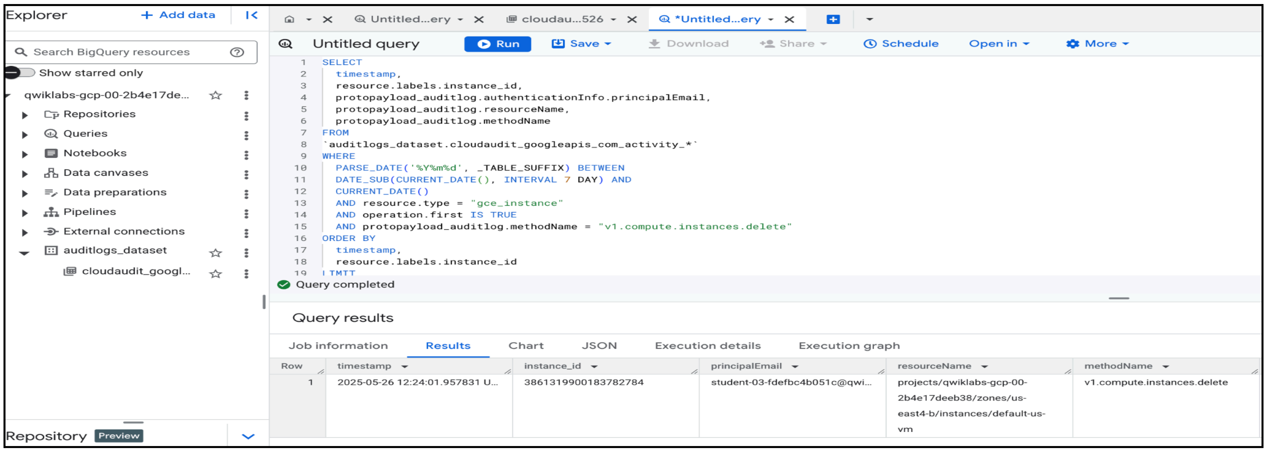
Dataset replica info

Primary location	US

Edit or delete roles below, or select "Add principal" to grant new access.

☑ Show inherited roles in table
Display roles inherited from the parent resources in the table below

Role / Principal	Inheritance
BigQuery Admin (3)	
BigQuery Data Editor (2)	
Editors of project: qwiklabs-gcp-00-2b4e17deeb38	
service-553658431994@gcp-sa-logging.iam.gserviceaccount.com	
BigQuery Data Owner (2)	
BigQuery Data Viewer (1)	
Cloud Logging Service Agent (1)	
Editor (4)	
Kubernetes Engine Service Agent (1)	
Owner (2)	
Viewer (2)	



Untitled query

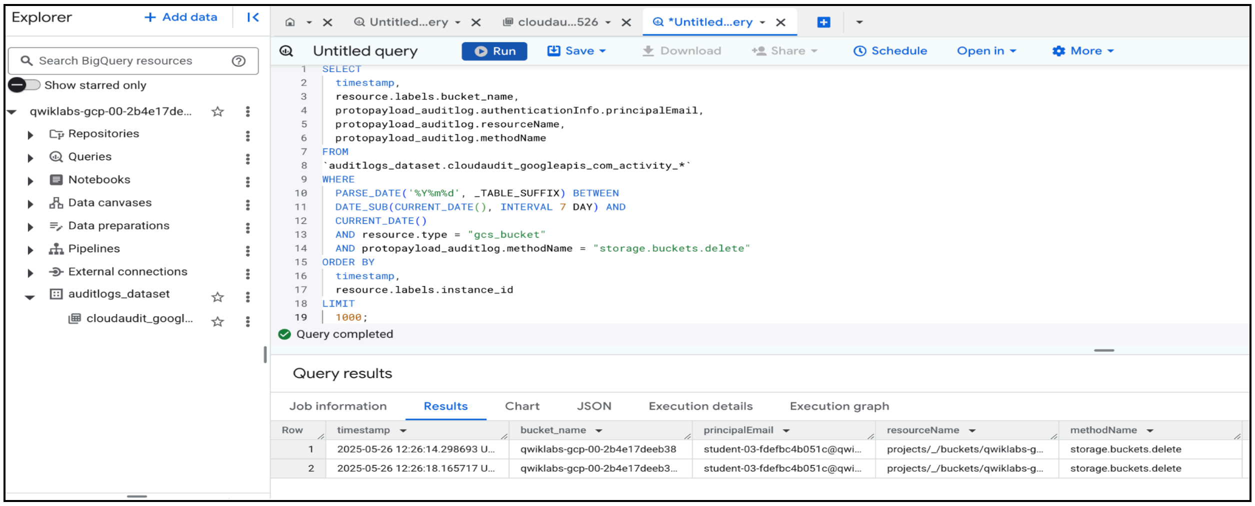
```
SELECT
  timestamp,
  resource.labels.instance_id,
  protopayload_auditlog.authenticationInfo.principalEmail,
  protopayload_auditlog.resourceName,
  protopayload_auditlog.methodName
FROM
`auditlogs_dataset.cloudaudit_googleapis_com_activity_*`
WHERE
  PARSE_DATE('%Y%m%d', _TABLE_SUFFIX) BETWEEN
  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
```

Query completed

Query results

Job information | Results | Chart | JSON | Execution details | Execution graph

Row	timestamp	instance_id	principalEmail	resourceName	methodName
1	2025-05-26 12:24:01.957831 U...	3861319900183782784	student-03-fdefbc4b051c@qwi...	projects/qwiklabs-gcp-00-2b4e17deeb38/zones/us-east4-b/instances/default-us-vm	v1.compute.instances.delete

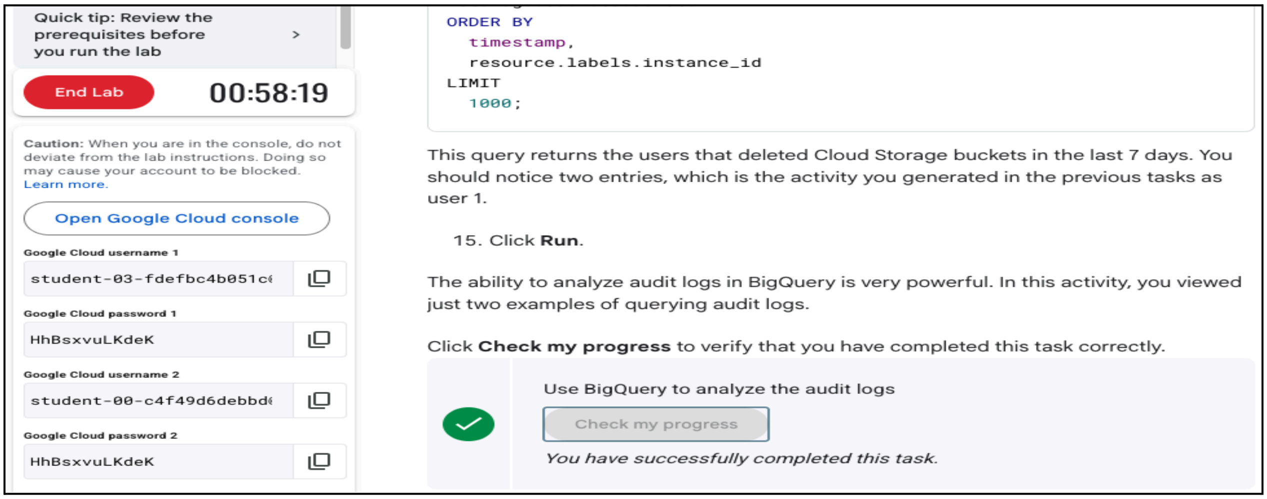


```
SELECT
  timestamp,
  resource.labels.bucket_name,
  protopayload_auditlog.authenticationInfo.principalEmail,
  protopayload_auditlog.resourceName,
  protopayload_auditlog.methodName
FROM
`auditlogs_dataset.cloudaudit_googleapis_com_activity_*`
WHERE
  PARSE_DATE('%Y%m%d', _TABLE_SUFFIX) BETWEEN
  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;
```

Query completed

Query results

Row	timestamp	bucket_name	principalEmail	resourceName	methodName
1	2025-05-26 12:26:14.298693 U...	qwiklabs-gcp-00-2b4e17deeb38	student-03-fdefbc4b051c@qwi...	projects/_/buckets/qwiklabs-g...	storage.buckets.delete
2	2025-05-26 12:26:18.165717 U...	qwiklabs-gcp-00-2b4e17deeb3...	student-03-fdefbc4b051c@qwi...	projects/_/buckets/qwiklabs-g...	storage.buckets.delete


Quick tip: Review the prerequisites before you run the lab
End Lab
00:58:19

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username 1: student-03-fdefbc4b051c

Google Cloud password 1: HhBsxvuLKdeK

Google Cloud username 2: student-00-c4f49d6debbd

Google Cloud password 2: HhBsxvuLKdeK

```
ORDER BY
  timestamp,
  resource.labels.instance_id
LIMIT
  1000;
```

This query returns the users that deleted Cloud Storage buckets in the last 7 days. You should notice two entries, which is the activity you generated in the previous tasks as user 1.

15. Click **Run**.

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 that you have completed this task correctly.

Use BigQuery to analyze the audit logs

You have successfully completed this task.

My Assessment

This lab focused on analyzing logs in Big Query after using Cloud Shell to generate account activity. This lab, specifically, provided a lot of insight as I was seeking a way to learn how to review and analyze logs.