**Diagrama

Descripción generada automáticamenteUn dibujo de un animal con la boca abierta

Descripción generada automáticamente con confianza baja**

P3 Analyze audit logs using   
BigQuery

26 de junio de 2024

adrián gonzález iglesias

máster sistemas multicloud

INSTITUTO TAJAMAR

**Índice**

Contenido

[**Índice** 1](#_Toc170213642)

[**Analyze audit logs using BigQuery** 1](#_Toc170213643)

[**Activity overview** 2](#_Toc170213644)

[**Scenario** 2](#_Toc170213645)

[**Task 1. Generate account activity** 3](#_Toc170213646)

[**Task 2. Export the audit logs** 4](#_Toc170213647)

[**Task 3. Generate more account activity** 6](#_Toc170213648)

[**Task 4. Sign in as the second user** 7](#_Toc170213649)

[**Task 5. Analyze the Admin Activity logs** 8](#_Toc170213650)

[**Task 6. Use BigQuery to analyze the audit logs** 10](#_Toc170213651)

[**Conclusion** 13](#_Toc170213652)

[**End your lab** 13](#_Toc170213653)

**Analyze audit logs using BigQuery**

[Analyze audit logs using BigQuery | Google Cloud Skills Boost](https://www.cloudskillsboost.google/paths/419/course_templates/969/labs/485979)

important icon **IMPORTANT:**  
  
desktop/labtop icon Make sure to complete this hands-on lab on a desktop/laptop only.  
  
check icon There are only 5 attempts permitted per lab.  
  
quiz target icon As a reminder – it is common to not get every question correct on your first try, and even to need to redo a task; this is part of the learning process.  
  
timer icon Once a lab is started, the timer cannot be paused. After 1 hour and 30 minutes, the lab will end and you’ll need to start again.  
  
tip icon For more information review the **Lab technical tips** reading.

**Activity overview**

Google Cloud services write audit logs that record administrative activities and access within your Google Cloud resources. Audit log entries help you answer the questions "who did what, where, and when" within your Google Cloud projects. Enabling audit logs helps your security, auditing, and compliance entities monitor Google Cloud data and systems for possible vulnerabilities or external data misuse.

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

**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.

**Task 1. Generate account activity**

***Note:****Make sure you are on the****username 1: Google Cloud username 1****Google Cloud console.*

**Nos aseguramos de que estamos utilizando el username 1** *(student-02).* **para este apartado, ya que cada username tiene funciones distintas que emplearan en el trabajo.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

In this task, you'll create and delete cloud resources to generate account activity which you'll access as Cloud Audit Logs.

1. Copy the following commands into the Cloud Shell terminal:

**En el primer task, añadimos los siguientes comandos para crear y eliminar recursos de la nube, para poder generar actividad en la cuenta, que luego utilizaremos para acceder a esos registros.**

gcloud storage buckets create gs://$DEVSHELL\_PROJECT\_ID

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

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

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

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

1. Press **ENTER**.

Texto

Descripción generada automáticamente

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

|  |
| --- |
| Generate account activity  Check my progress |

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

**Task 2. Export the audit logs**

***Note:****Make sure you are on the****username 1: Google Cloud username 1****Google Cloud console.*

**Nos aseguramos de nuevo que estamos usando la cuenta de username 1 (student-02).**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

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

**Generados anteriormente registros al crear los recursos, vamos a exportar dichos registros a un conjunto de datos mediante BigQuery.**

1. In the Google Cloud console, in the **Navigation menu** (navigation menu icon) click **Logging > Logs Explorer**. The **Logs Explorer** page opens. (You may need to click **More Products** to expand the **Navigation menu** options and locate **Logging** under **Operations**.)

**Accedemos a Logs explorer, en la sección Logging.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. When exporting logs, the current filter will be applied to what is exported. Copy the following query into the **Query** builder:

**Ingresamos el siguiente comando para filtrar los registros de Cloud Audit dentro de nuestro proyecto.**

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

1. Click **Run query**. The query results should display on the **Query results** pane. This query filters for Cloud Audit logs within your project.

**Añadimos el comando en la Query y pulsamos Run Query para ejecutar.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Under the **Query editor** field, click **More actions > Create sink.** The **Create logs routing sink** dialog opens.

**A continuación, pulsamos en Create sink para exportar los logs a la BigQuery.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

***Note:****If your browser window is narrow, the UI may display****More****instead of****More actions****.*

1. In the **Create logs routing sink** dialog, specify the following settings and leave all other settings at their defaults:

**Añadimos los siguientes datos a nuestra sink (exportación de logs).**

|  |  |
| --- | --- |
| **Section** | **Field: values** |
| **Sink details** | Sink name: AuditLogsExport Click **Next.** |
| **Sink destination** | **Select sink service:** BigQuery dataset **Select BigQuery dataset:** Create new BigQuery dataset. The **Create dataset** dialog opens. |
| **Create dataset** | **Dataset ID:** auditlogs\_dataset Click **Create Dataset**. The **Create dataset** dialog closes, and you'll return to the **Sink destination** dialog. |
| **Sink destination** | Click **Next**. Uncheck the **Use Partitioned Tables** checkbox, if it is already selected, and click **Next**. |
| **Choose logs to include in sink** | Notice the pre-filled Build inclusion filter:logName=("projects/[PROJECT ID]/logs/cloudaudit.googleapis.com%2Factivity") Click **Next**. Click **Create Sink**. Return to the **Logs Explorer** page. |

**En el Sink Name, ingresamos AuditLogsExport.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Después, en el tipo de servicio, como ya hemos mencionado antes, seleccionamos BigQuery.**

**Y en Select BigQuery dataset creamos una nueva dataset llamada auditlogs\_dataset.**

Escala de tiempo

Descripción generada automáticamente

**Por último, dejamos por defecto los siguientes puntos y creamos nuestra sink.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto, Correo electrónico

Descripción generada automáticamente

1. In the **Logging** navigation pane, click **Log Router** to view the **AuditLogsExport** sink in the **Log Router Sinks** list.

**Accedemos al apartado Log Router para ver nuestro sink creado correctamente.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

**Pinchamos en los 3 puntos de la sink y entramos en view sink details, para observar los detalles.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

**Como podemos ver, nos indica el servicio que hemos utilizado (BigQuery), su destino, el nombre del recurso, etc.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Todos los registros futuros ahora se exportarán a BigQuery y las herramientas de BigQuery se pueden usar para realizar análisis de los datos del registro de auditoría.**

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

|  |
| --- |
| Export the audit logs  Check my progress |

Escala de tiempo

Descripción generada automáticamente

**Task 3. Generate more account activity**

***Note:****Make sure you are on the****username 1: Google Cloud username 1****Google Cloud console.*

**Nos aseguramos de nuevo que estamos usando la cuenta de username 1 (student-02).**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

In this task, you'll create and delete cloud resources to generate additional account activity which you'll then access in BigQuery to extract additional insights from the logs.

**Añadimos los siguientes comandos para, como hemos hecho anteriormente, crear y eliminar recursos de la nube, para poder generar actividad en la cuenta, que luego utilizaremos para acceder a esos registros.**

1. Copy the following commands into the Cloud Shell terminal:

gcloud storage buckets create gs://$DEVSHELL\_PROJECT\_ID

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

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

1. Press **ENTER**.

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

Texto

Descripción generada automáticamente

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

**Borramos los recursos creados, para generar registros.**

gcloud storage rm --recursive gs://$DEVSHELL\_PROJECT\_ID

gcloud storage rm --recursive gs://$DEVSHELL\_PROJECT\_ID-test

1. Press **ENTER**.

Texto

Descripción generada automáticamente

Notice you deleted both buckets.

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

|  |
| --- |
| Generate more account activity  Check my progress |

Escala de tiempo

Descripción generada automáticamente

**Task 4. Sign in as the second user**

You'll need to switch Google Cloud accounts by logging into the Google Cloud console using the second user account provided in the **Lab Details** panel. You will use this user account to analyze the logs.

1. In the Google Cloud console, click on the user icon in the top-right corner of the screen, and then click **Add account**.

**Añadimos nuestra Segunda cuenta proporcionada por el laboratorio, que se encargará de analizar los logs que hemos generado con el otro username (student-02).**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Navigate back to the **Lab Details** panel, copy the **Google Cloud username 2:** **Google Cloud username 2** and **password**. Then, paste the username and password into the Google Cloud console **Sign in** dialog.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Task 5. Analyze the Admin Activity logs**

***Note:****Make sure you are on the****username 2: Google Cloud username 2****Google Cloud console.*

**Nos aseguramos de que ahora estamos utilizando el username 2 (student-00).**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

In this task, you'll review the Admin activity logs generated in the previous task. Your goal is to identify and apply filters to isolate logs that may indicate suspicious activity. This will enable you to export this subset of logs and streamline the process of analyzing them for potential issues.

Admin Activity logs record the 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 when permissions are changed.

***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.*

1. In the Google Cloud console, click the **Navigation menu** (navigation menu icon).

**Ahora, revisaremos los registros administrativos previos para identificar actividades inusuales mediante filtros y facilitar su análisis. Estos registros documentan acciones como llamadas a la API, creación de VMs, despliegue de aplicaciones en App Engine y cambios de permisos.**

1. Select **Logging > Logs Explorer**. The **Logs Explorer** page opens. (You may need to expand the **More Products** drop-down menu within the **Navigation** menu and locate Logging under **Operations**.)
2. Ensure that the **Show query** toggle button is activated. This opens the **Query builder** field.

**Accedemos a Logs explorer y mostramos las consultas activando Show Query.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Copy and paste the following command into the **Query builder** field. Notice your Google Cloud project ID, project ID in the command.

**Ejecutamos el siguiente comando, introduciendo nuestro ID de proyecto.**

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

1. Click **Run query**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. In the **Query results**, locate the log entry indicating that a Cloud Storage bucket was deleted, it will contain the **storage.buckets.delete** summary field. Summary fields are included in the log results to highlight important information about the log entry.

**Con esta consulta conseguimos mostrar, los registros de borrado de bucket que hemos ejecutado en el anterior Task con la otra cuenta de usuario.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

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 your project id: PROJECT\_ID.

1. Within this entry, click on the **storage.googleapis.com** text, and select **Show matching entries**. The **Query results** should now display only six entries related to created and deleted cloud storage buckets.

**Si dentro de la Query mostramos las entradas, nos aparecerán los 6 registros de borrado que hemos provocado.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

**Como podemos ver aquí.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. In the Query editor field, notice the **protoPayload.serviceName="storage.googleapis.com"** line was added to the query builder, this filters your query to entries only matching **storage.googleapis.com**.

**Al usar la función de mostrar las entradas, automáticamente la sintaxis añade la línea protoPayload.serviceName="storage.googleapis.com” en la Query, ya que muestra solo las coincidentes con esta consulta.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Within those query results, click **storage.buckets.delete** in one of the entries, and select **Show matching entries.**

**Como vemos, pasa lo mismo que en el anteriore punto, automáticamente te cambia la sintaxis de la Query.**

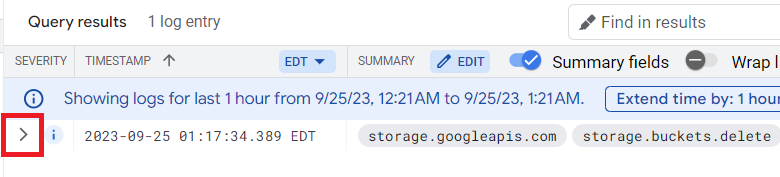
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

The **Query results** should now display all entries related to deleted Cloud Storage buckets. You can use this technique to easily locate specific events.

1. In the **Query results**, expand a **storage.buckets.delete** event by clicking the expand arrow **>** next to the line:

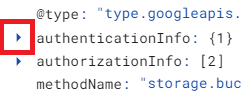
**Si abrimos una pestaña de la query, nos muestra lo siguiente que mostramos en el siguiente punto.**



Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Expand the **authenticatitonInfo** field by clicking the expand arrow **>** next to the line:



Notice the **principalEmail** field which displays the email address of the user account that performed this action which is the user 1 account you used to generate the user activity.

**El email principal que ha provocado estos registros, esto es de mucha utilidad en muchos más aspectos ,para saber quién ha provocados situaciones diferentes.**

**En este caso, sabemos que ha sido student-02, ya que lo hemos provocado nosotros para realizar las comprobaciones.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Task 6. Use BigQuery to analyze the audit logs**

***Note:****Make sure you are on the****username 2: Google Cloud username 2****Google Cloud console.*

**Nos aseguramos de que estamos utilizando el username 2 (student-00).**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

You've generated and exported logs to a BigQuery dataset. In this task, you'll analyze the logs using the 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. In the Google Cloud console, click the **Navigation menu** (navigation menu icon).
2. Click **BigQuery**.
3. In the **Explorer** pane, click the expand arrow beside your project, Google Cloud project ID. The **auditlogs\_dataset** dataset is displayed.

**Accedemos a BigQuery y expandimos la pestaña de nuestro ID Project.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. Click the **auditlogs\_dataset** dataset.

**Entramos en nuestra sink creada, llamada auditlogs\_dataset.**

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente con confianza media

1. In the auditlogs\_dataset toolbar, click the **Sharing** dropdown menu, and select **Permissions**.

**Pinchamos en los 3 puntos y entramos en manage permissions.**

Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente

1. On the **Share permission for "auditlogs\_dataset"** page, expand the **BigQuery Data Editor** section.

**Expandimos la pestaña del editor de datos BigQuery.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Confirm that the service account used for log exports is a listed permission. The service account is similar to: [service-xxxxxxxx@gcp-sa-logging.iam.gserviceaccount.com](mailto:service-xxxxxxxx@gcp-sa-logging.iam.gserviceaccount.com)

El permiso que vemos en la siguiente imagen, se asigna automáticamente cuando configuramos la exportación de logs (sink).

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Click **Close** to close the **Share Dataset** window.
2. In the **Explorer** pane, click the expander arrow next to the **auditlogs\_dataset** dataset to view the **cloudaudit\_googleapis\_com\_acitivty** table. This table contains your exported logs.
3. Select the **cloudaudit\_googleapis\_com\_acitivty** table. The table schema displays. Take a moment to review the table schema and details.

**Entramos en la table que ha generado nuestra sink.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente con confianza media

1. Expand the **Query** drop-down menu and select **In new tab**.

**Dentro de la tabla, abríamos una nueva pestaña para ejecutar consultas.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. In the Untitled tab of the query builder, delete any existing text and copy and paste the following command:

**Añadimos la siguiente consulta para observar los usuarios que eliminaros máquinas virtuales en los últimos 7 días.**

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;

1. Click **Run**.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Después de haber generado la exportación de logs, hemos borrado VM´s, desde la cuenta de student-02 únicamente, por lo que la consulta es correcta.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Replace the previous query in the **Untitled** tab with the following:

**En la siguiente consulta vamos a comprobar los usuarios que eliminaron Storage Buckets en los últimos días.**

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;

1. Click **Run**.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**La consulta es correcta ya que, en este caso, hemos borrado dos Storage Buckets con el mismo usuario.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

|  |
| --- |
| Use BigQuery to analyze the audit logs  Check my progress |

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Conclusion**

Great work! You have successfully queried in Logs Explorer. You then exported logs and created a dataset that you analyzed in BigQuery.

You have shown how you 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.

**End your lab**

Before you **end the lab**, make sure you’re satisfied that you’ve completed all the tasks. When you're ready, click **End Lab** and then click **Submit**.

Ending the lab will remove your access to the lab environment, and you won’t be able to access the work you've completed in it again.

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.