[ENGLISH]

Hello, Cloud Gurus, and welcome to this lesson

where we'll get some experience working with Athena.

And we'll begin by creating a trail in CloudTrail,

and this is gonna generate an audit log

of all the user activity on our account.

Now, as you know, CloudTrail sends logs to S3,

and our new CloudTrail is gonna store

all the logs it creates in a brand new S3 bucket.

Next, we'll create an Athena table,

and we're gonna use standard SQL,

or structured query language,

to query the data stored in our S3 bucket.

So if you're ready to get your hands dirty with Athena,

then please join me in the AWS Console.

So from the AWS Console,

first of all, search for CloudTrail.

We can ignore these messages, so just close them down.

And then, from the CloudTrail dashboard,

select Create Trail.

We can ignore this message, so just close that down.

And our trail is gonna be called management-events.

And as you know, the CloudTrail logs

are gonna be stored in an S3 bucket

and it's gonna create a brand new S3 bucket for us.

By default, it's going to encrypt our CloudTrail

and we need to enter a new KMS key alias,

because we're gonna create a new KMS key

to handle the encryption.

Scrolling down, select Next.

Make sure that the event type

of management events is selected, hit Next.

Review and Create Trail.

So there we go, it's created our trail.

And if we select the S3 bucket over here,

we should see that it's already started

to create some folders.

So if you select the CloudTrail folder,

after a few minutes,

it should start to populate this folder structure.

So just be patient, and after a few minutes,

we should start to see some logs appearing,

but it might just take five minutes or so to get started.

After a few minutes, I'll refresh my view,

and here are all the logs it's created.

And if you select one of the regions

where it's already started logging and drill down,

here are the logs it's created.

So now we need to create another S3 bucket

that's going to be used to store

our Athena query results in,

and this is mandatory before we can use Athena.

So select Buckets on the left-hand side,

Create Bucket.

I'm gonna call it myathena-results-faye.

The region is gonna be US East 1.

Scroll down to the bottom and Create Bucket.

So now we are ready to configure our Athena database.

So search for Athena and open it up in a new browser tab.

Now before you run your first query,

you will need to set up the query result location in S3.

So first of all, on the left-hand menu select Query Editor.

And it's telling us here that before we run our Query,

we need to set up our query result location.

So select Edit Settings,

but if you don't see this message,

you can just edit your settings

by selecting the Settings tab here at the top of the screen.

Browse S3, select your results bucket

and hit Save.

So now we are good to go to create our Athena database,

and we're gonna do that using a simple SQL query.

So select Editor,

and this is where we're gonna type our query.

Click in the box

and I want you to type the following command,

create database athenadb,

and then select Run.

And if it's been successful,

if you scroll down at the bottom,

you will see a message saying Query Successful.

So that has created our database.

And on the left-hand side under database,

you should find our athenadb database.

And if you don't see it, you can just select the dropdown

and you should be able to find it.

Now our database is empty at the moment,

so we need to create a new table,

and then tell Athena where to find the data

that we want to use to populate our table.

And I've already prepared the SQL command

that we're gonna use to do this.

And in the resources section of this lesson,

you will find a link to the GitHub repository

that contains my query commands.

Now the first one I want you to take a look

at is the Athena\_Query\_Create\_Table.txt.

If we select Raw, we can then copy everything,

come back to Athena,

hit the plus sign to create our second query,

paste the code in here,

and let's take a look at our code.

So this is a really long piece of SQL code,

and all it does is create our table.

And our table is gonna be called cloudtrail\_logs.

And then, down here it's creating

all the different attributes

that are gonna be part of our table,

so things like the user identity, account id,

event time, and event source, AWS region, et cetera.

All the kind of information that you would expect to see

in a CloudTrail log.

So these are all of the attributes of our table.

And then, right down at the bottom here

this is where we need to specify the location of our data.

So we need to tell Athena where to find this data,

and it's gonna be in our CloudTrail log S3 bucket.

So if we head back to the S3 console,

select the CloudTrail log, go into AWSLogs,

and then the next folder,

which is named after your account number,

and your folder structure should look like this.

So here's your bucket name, then AWSLogs,

and then your AWS account number.

So now just copy the S3 URI,

come back to Athena,

and we need to replace this URI

with the one from our bucket.

And once you've done that, it should look like this.

So here's our bucket name, then AWSLogs,

and then our account number.

So if you've done that, just hit Run.

And if everything's worked correctly,

you should get a message at the bottom

saying Query Successful.

And if it hasn't been successful,

just make sure that you've specified

this location correctly.

'Cause if you don't specify this correctly,

then Athena will not be able to find your data.

So now under the table section on the left,

you should see a new table named cloudtrail\_logs,

expand the table and here are all the data attributes

that our query has just created.

And now we are actually ready

to start querying this data using Athena.

So at the top, click on the plus sign

to create another query.

And I've prepared this query for you already,

and you're gonna find it in the resources of the course.

So I'm gonna hit the Back button on this screen,

go up one directory,

and it's this file here called Athena\_Query.txt.

I'm gonna copy that,

paste it into my query window, and hit Run.

And this is just a really simple query

that selects the user identity ARN, event name,

source IP address, and event time,

from our cloudtrail\_logs table.

And then if you scroll down,

you can take a look at the results, and here they are.

So it selected the user identity, the event name,

source IP address, and event time,

from the data in our cloudtrail\_logs table.

So that is Athena,

and I hope you can see that it's really,

really simple to use.

And if you know how to use SQL,

then you can run all sorts of queries on your data

and you can really just treat it just like a database

and run whatever queries you want.

So let's move on to my exam tips.

And just remember that Athena is a query service

that supports standard SQL, or structured query language.

It's really easy to configure.

And all you do is point Athena to the data

that you want to query in S3,

define your table schema,

and then you can query your data using standard SQL.

So that's it for this lesson.

If you have any questions, please let me know.

Otherwise, I will see you in the next lesson, thank you.

[SPANISH]

Hola, Cloud Gurus, y bienvenidos a esta lección.

donde obtendremos algo de experiencia trabajando con Athena.

Y comenzaremos creando un rastro en CloudTrail ,

y esto va a generar un registro de auditoría

de toda la actividad del usuario en nuestra cuenta.

Ahora, como sabe, CloudTrail envía registros a S3,

y nuestro nuevo CloudTrail va a almacenar

todos los registros que crea en un cubo S3 completamente nuevo.

A continuación, crearemos una tabla de Athena,

y vamos a usar SQL estándar,

o lenguaje de consulta estructurado,

para consultar los datos almacenados en nuestro depósito S3.

Entonces, si estás listo para ensuciarte las manos con Athena,

entonces únase a mí en la consola de AWS.

Entonces, desde la consola de AWS,

primer lugar, busque CloudTrail .

Podemos ignorar estos mensajes, así que ciérralos.

Y luego, desde el tablero de CloudTrail ,

seleccione Crear ruta.

Podemos ignorar este mensaje, así que ciérralo.

Y nuestro rastro se llamará eventos de gestión.

Y como saben, los registros de CloudTrail

son se almacenará en un cubo S3

y va a crear un cubo S3 completamente nuevo para nosotros.

Por defecto, cifrará nuestro CloudTrail

y necesitamos ingresar un nuevo alias de clave KMS,

porque vamos a crear una nueva clave KMS

para manejar el cifrado.

Desplazándose hacia abajo, seleccione Siguiente .

Asegúrese de que el tipo de evento

de eventos de gestión está seleccionado, pulse Siguiente.

Revisar y crear sendero.

Así que ahí vamos, ha creado nuestro rastro.

Y si seleccionamos el cubo S3 aquí,

deberíamos ver que ya empezó

para crear algunas carpetas.

Entonces, si selecciona la carpeta CloudTrail ,

después de unos minutos,

debería comenzar a llenar esta estructura de carpetas.

Así que ten paciencia, y después de unos minutos,

deberíamos empezar a ver aparecer algunos registros,

pero puede que solo tarde unos cinco minutos en empezar.

Después de unos minutos, actualizaré mi vista,

y aquí están todos los registros que ha creado.

Y si selecciona una de las regiones

donde ya comenzó a iniciar sesión y profundizar,

aquí están los registros que ha creado.

Entonces ahora necesitamos crear otro depósito S3

que se va a utilizar para almacenar

nuestra consulta de Athena da como resultado,

y esto es obligatorio antes de que podamos usar Athena.

Así que seleccione Cubos en el lado izquierdo,

Crear cubo.

Voy a llamarlo myathena -resultados- faye .

La región será EE.UU. Este 1.

Desplácese hacia abajo hasta la parte inferior y Crear depósito.

Ahora estamos listos para configurar nuestra base de datos Athena.

Así que busque Athena y ábralo en una nueva pestaña del navegador.

Ahora, antes de ejecutar su primera consulta,

deberá configurar la ubicación del resultado de la consulta en S3.

En primer lugar, en el menú de la izquierda, seleccione Editor de consultas.

Y aquí nos dice que antes de ejecutar nuestra Consulta,

necesitamos configurar nuestra ubicación de resultados de consulta.

Así que seleccione Editar configuración,

pero si no ves este mensaje,

puedes editar tu configuración

seleccionando la pestaña Configuración aquí en la parte superior de la pantalla.

Explore S3, seleccione su grupo de resultados

y presiona Guardar.

Así que ahora estamos listos para ir a crear nuestra base de datos de Athena,

y lo haremos usando una simple consulta SQL.

Así que seleccione Editor,

y aquí es donde vamos a escribir nuestra consulta.

Haga clic en el cuadro

y quiero que escribas el siguiente comando,

crear base de datos athenadb ,

y luego seleccione Ejecutar.

Y si ha tenido éxito,

si se desplaza hacia abajo en la parte inferior,

verá un mensaje que dice Consulta exitosa.

Así que ha creado nuestra base de datos.

Y en el lado izquierdo debajo de la base de datos,

debe encontrar nuestra base de datos athenadb .

Y si no lo ves, puedes simplemente seleccionar el menú desplegable

y usted debe ser capaz de encontrarlo.

Ahora nuestra base de datos está vacía en este momento,

entonces necesitamos crear una nueva tabla,

y luego decirle a Athena dónde encontrar los datos

que queremos usar para llenar nuestra tabla.

Y ya he preparado el comando SQL

que vamos a usar para hacer esto.

Y en la sección de recursos de esta lección,

encontrará un enlace al repositorio de GitHub

que contiene mis comandos de consulta.

Ahora el primero quiero que le eches un vistazo

en es Athena\_Query\_Create\_Table.txt.

Si seleccionamos Raw, podemos copiar todo,

vuelve a Atenas,

presione el signo más para crear nuestra segunda consulta,

pega el código aquí,

y echemos un vistazo a nuestro código.

Así que esta es una pieza muy larga de código SQL,

y todo lo que hace es crear nuestra tabla.

Y nuestra tabla se llamará cloudtrail\_logs .

Y luego, aquí abajo está creando

todos los diferentes atributos

que van a ser parte de nuestra mesa,

como la identidad del usuario, la identificación de la cuenta,

del evento y origen del evento, región de AWS, etcétera.

Todo el tipo de información que esperarías ver

en un registro de CloudTrail .

Estos son todos los atributos de nuestra tabla.

Y luego, justo en el fondo aquí

aquí es donde necesitamos especificar la ubicación de nuestros datos.

Así que tenemos que decirle a Athena dónde encontrar estos datos,

y estará en nuestro depósito S3 de registro de CloudTrail .

Entonces, si volvemos a la consola S3,

seleccione el registro de CloudTrail , vaya a AWSLogs ,

y luego la siguiente carpeta,

que lleva el nombre de su número de cuenta,

y su estructura de carpetas debería verse así.

Este es el nombre de su depósito, luego AWSLogs ,

y luego su número de cuenta de AWS.

Así que ahora simplemente copie el URI de S3,

vuelve a Atenas,

y necesitamos reemplazar este URI

con el de nuestro cubo.

Y una vez que hayas hecho eso, debería verse así.

Este es el nombre de nuestro depósito, luego AWSLogs ,

y luego nuestro número de cuenta.

Entonces, si lo ha hecho, simplemente presione Ejecutar.

Y si todo ha funcionado correctamente,

deberías recibir un mensaje en la parte inferior

diciendo Consulta exitosa.

Y si no ha tenido éxito,

solo asegúrate de haber especificado

esta ubicación correctamente.

Porque si no especificas esto correctamente,

entonces Athena no podrá encontrar sus datos.

Así que ahora debajo de la sección de la mesa a la izquierda,

debería ver una nueva tabla llamada cloudtrail\_logs ,

expanda la tabla y aquí están todos los atributos de datos

que acaba de crear nuestra consulta.

Y ahora estamos realmente listos

para comenzar a consultar estos datos con Athena.

Entonces, en la parte superior, haga clic en el signo más

para crear otra consulta.

Y ya he preparado esta consulta para ti,

y lo vas a encontrar en los recursos del curso.

Voy a presionar el botón Atrás en esta pantalla,

subir un directorio,

y es este archivo aquí llamado Athena\_Query.txt.

voy a copiar eso,

péguelo en mi ventana de consulta y presione Ejecutar.

Y esta es solo una consulta realmente simple.

que selecciona el ARN de la identidad del usuario, el nombre del evento,

de origen y hora del evento,

de nuestra tabla cloudtrail\_logs .

Y luego, si te desplazas hacia abajo,

puedes echar un vistazo a los resultados, y aquí están.

Así que seleccionó la identidad del usuario, el nombre del evento,

de origen y hora del evento,

de los datos en nuestra tabla cloudtrail\_logs .

Entonces esa es Atenea,

y espero que puedas ver que es realmente,

muy simple de usar.

Y si sabes cómo usar SQL,

entonces puede ejecutar todo tipo de consultas en sus datos

y realmente puedes tratarlo como una base de datos

y ejecuta las consultas que quieras.

Así que pasemos a mis consejos para el examen.

Y recuerda que Athena es un servicio de consulta

que admita SQL estándar o lenguaje de consulta estructurado.

Es muy fácil de configurar.

Y todo lo que haces es apuntar a Athena a los datos.

que desea consultar en S3,

definir el esquema de su tabla,

y luego puede consultar sus datos usando SQL estándar.

Eso es todo por esta lección.

Si tiene alguna pregunta, por favor hágamelo saber.

De lo contrario, te veré en la próxima lección, gracias.