[ENGLISH]

Hello Cloud Gurus and welcome to this lesson

where we'll be getting our hands dirty

with S3 and configuring encryption.

We'll begin by creating an S3 bucket,

and note that encryption is enabled by default.

Next, we'll review the encryption options.

So we'll take a look at the server side encryption

options that are available within S3.

And then lastly, we'll configure the use

of SSE-KMS encryption.

So we'll configure SSE-KMS

as the encryption type for this bucket.

So if you're ready to get your hands dirty with S3,

please join me in the AWS console.

From the console, first of all, search for S3.

Select Create Bucket.

I'll call it My Encrypted Files

and add a load of random numbers on the end.

Then scroll down to the bottom,

and this is where you will find default encryption.

And you'll see that SSE S3 is the default encryption type.

So this is encryption using S3 managed keys.

So let's select the other option,

AWS Key Management Service.

After you've selected that,

it's gonna reveal some additional options.

And with KMS, you manage the key

using the Key Management Service.

So we will need to create a new KMS key.

So first of all, select Choose From Your AWS KMS Keys.

Select Create a KMS Key.

It's gonna be a symmetric key,

so we'll use the same key to encrypt and decrypt.

Key usage is going to be to encrypt and decrypt our files.

Select Next.

We'll give it an alias so that we can identify it later.

Call it My KMS Key.

Then hit Next.

At this point, we need to add the name

of a key administrator, and this could be a user or role

in our account that has permissions to administer the key.

And I'm gonna select Admin.

Scroll down to the bottom, hit Next.

At this point, we're gonna add a key user,

and this is gonna be our cloud user account.

So this is the user that will be able to use the KMS key

in cryptographic operations.

So to encrypt and decrypt our files.

Then hit Next.

We can review our config.

Scroll down to the bottom and finish.

And there we go.

So we've created our key and we've added our key user

and our key administrator as well.

So with KMS, you define who within your organization

has access to the keys, and that's just another way

to determine who is authorized to access the files

that you've encrypted when they've been uploaded to S3.

So now back in the S3 console,

I'm gonna hit this refresh button.

And then once you've done that,

you should be able to locate your key.

And there it is.

It's called My KMS Key.

So select that one and create bucket.

So that is our bucket created,

and if we select our bucket, select Properties,

and then scroll down to Default Encryption,

you will see the encryption type

is AWS Key Management Service.

So for the exam, the main things to remember are that

with S3, you get encryption in transit using SSL or TLS,

and that's what we're using

when we access a website using HTTPS.

We can also configure encryption at rest,

which is server side encryption.

By default, you've got SSE-S3

with S3 managed keys, but you can also configure SSE-KMS

using the AWS Key Management Service.

Or you can configure SSE-C,

which is where you provide your own keys.

And then there's also the option

to use encryption at rest client side encryption.

And that's when you encrypt your files yourself

before going ahead and uploading them into S3.

So that's it for this lesson.

Any questions, let me know.

Otherwise, I will see you in the next one.

Thank you.

[SPANISH]

Hola Cloud Gurus y bienvenidos a esta lección.

donde nos estaremos ensuciando las manos

con S3 y configurando el cifrado.

Comenzaremos creando un depósito S3,

y tenga en cuenta que el cifrado está habilitado de forma predeterminada.

A continuación, revisaremos las opciones de encriptación.

Echaremos un vistazo al cifrado del lado del servidor.

opciones disponibles en S3.

Y por último, configuraremos el uso

de cifrado SSE-KMS.

Entonces configuraremos SSE-KMS

como el tipo de cifrado para este depósito.

Entonces, si está listo para ensuciarse las manos con S3,

Únase a mí en la consola de AWS.

Desde la consola, en primer lugar, busque S3.

Seleccione Crear depósito.

Lo llamaré Mis archivos cifrados

y agregue una carga de números aleatorios al final.

Luego desplácese hacia abajo hasta la parte inferior,

y aquí es donde encontrará el cifrado predeterminado.

Y verá que SSE S3 es el tipo de cifrado predeterminado.

Esto es encriptación usando claves administradas por S3.

Así que vamos a seleccionar la otra opción,

Servicio de administración de claves de AWS.

Después de haber seleccionado eso,

es Voy a revelar algunas opciones adicionales.

Y con KMS, tú gestionas la clave

mediante el Servicio de administración de claves.

Entonces necesitaremos crear una nueva clave KMS.

En primer lugar, seleccione Elegir entre sus claves de AWS KMS.

Seleccione Crear una clave KMS.

Va a ser una clave simétrica,

entonces usaremos la misma clave para cifrar y descifrar.

El uso de la clave será para cifrar y descifrar nuestros archivos.

Seleccione Siguiente.

Le daremos un alias para poder identificarlo más tarde.

Llámelo Mi clave KMS.

Luego presione Siguiente .

En este punto, necesitamos agregar el nombre

de un administrador clave, y este podría ser un usuario o rol

en nuestra cuenta que tiene permisos para administrar la clave.

Y voy a seleccionar Admin.

Desplácese hacia abajo hasta la parte inferior, presione Siguiente .

En este punto, vamos a agregar un usuario clave,

y esta será nuestra cuenta de usuario en la nube.

Así que este es el usuario que podrá usar la clave KMS

en operaciones criptográficas.

Así que para cifrar y descifrar nuestros archivos.

Luego presione Siguiente .

Podemos revisar nuestra configuración .

Desplácese hacia abajo hasta el final y termine.

Y ahí vamos.

Hemos creado nuestra clave y hemos agregado nuestro usuario clave

y nuestro administrador clave también.

Entonces, con KMS, usted define quién dentro de su organización

tiene acceso a las llaves, y esa es solo otra forma

para determinar quién está autorizado a acceder a los archivos

que ha cifrado cuando se cargaron en S3.

Así que ahora de vuelta en la consola S3,

Voy a pulsar este botón de actualización.

Y luego, una vez que hayas hecho eso,

deberías poder localizar tu llave.

Y ahí está.

Se llama Mi clave KMS.

Así que seleccione ese y cree un depósito.

Así que ese es nuestro cubo creado,

y si seleccionamos nuestro cubo, seleccionamos Propiedades,

y luego desplácese hacia abajo hasta Cifrado predeterminado,

verá el tipo de cifrado

es el servicio de administración de claves de AWS.

Entonces, para el examen, lo principal que debe recordar es que

con S3, obtiene encriptación en tránsito usando SSL o TLS,

y eso es lo que estamos usando

cuando accedemos a un sitio web mediante HTTPS.

También podemos configurar el cifrado en reposo,

que es el cifrado del lado del servidor.

Por defecto, tienes SSE-S3

con claves administradas por S3, pero también puede configurar SSE-KMS

mediante el Servicio de administración de claves de AWS.

O puede configurar SSE-C,

que es donde usted proporciona sus propias claves.

Y luego también está la opción

para usar el cifrado en reposo del lado del cliente.

Y ahí es cuando encriptas tus archivos tú mismo

antes de continuar y cargarlos en S3.

Eso es todo por esta lección.

Cualquier pregunta, hágamelo saber.

De lo contrario, te veré en la próxima.

Gracias.