[ENGLISH]

Hello, Cloud Gurus and welcome to this lesson,

which is going to cover S3 Encryption.

And we'll begin,

with why we should encrypt in the first place.

We'll take a look at the S3 encryption options,

and cover my exam tips as well.

Now, if you've ever heard the Amazon CTO, Werner Vogels,

talk about data in the cloud,

then you've probably heard this catchy quote before,

"Dance like nobody's watching, encrypt like everyone is."

And that is because protecting your data

is a security best practice.

Data is a valuable business asset

and all businesses store data that needs to be protected.

Think about financial data, customer data, business plans,

or even proprietary code,

and encryption is a great way to protect your data

against unauthorized access.

Now with S3, you get a few different encryption options.

First of all, it supports encryption in transit using SLL,

which stands for Secure Sockets Layer, and TLS,

which stands for Transport Layer Security.

And these are industry standard protocols

for encrypting data that is traveling across a network.

And these protocols allow us to use HTTPS

to access a website securely.

So when we use HTTPS when accessing a website,

our communication with that website is encrypted.

For instance, when we type in a password,

that communication is encrypted.

Now, S3 also supports encryption at rest,

also known as server-side encryption,

and there are three different options available.

So first of all, you've got SSE-S3,

which uses S3-managed encryption keys,

and it uses the industry standard AES 256-bit encryption.

And this method of encryption

is actually enabled by default,

so when you create an S3 bucket, and upload an object to S3,

it's going to be encrypted using this method.

Next, there's SSE-KMS, and this is encryption at rest

using encryption keys that are managed

by the AWS Key Management Service.

And this is a good one to use

if you have regulatory requirements

that mean you need to be the one creating

and managing your encryption keys.

And then there's also SSE-C,

which is encryption using customer-provided keys.

And this is for customers who want to generate

their own keys and manage them outside of AWS.

And then the final type of encryption that's supported

is encryption at rest using client-side encryption.

And this is where you encrypt the files yourself

before uploading them into S3.

So for the exam, just remember that S3 supports encryption

in transit using SSL/TLS, and its encryption in transit

that we're using when we access a website using HTTPS.

Encryption at rest is also known as server-side encryption,

and S3 gives us three different options.

So we've got SSE-S3, which is the default, SSE-KMS,

where the encryption keys are managed

within the key management service, and SSE-C,

and this is for customers

who want to generate their own keys outside of AWS.

And then finally, there's client-side encryption,

where you encrypt the files yourself

before uploading them into S3.

And just remember, that it's SSE-S3

that is enabled by default.

So encryption using SSE-S3

is enabled when you first create an S3 bucket

and when you upload a new object.

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,

que cubrirá el cifrado S3.

Y vamos a empezar,

con por qué debemos cifrar en primer lugar.

Echaremos un vistazo a las opciones de cifrado S3,

y cubrir mis consejos de examen también.

Ahora, si alguna vez ha escuchado al CTO de Amazon, Werner Vogels ,

hablar de datos en la nube,

entonces probablemente hayas escuchado esta cita pegadiza antes,

"Baila como si nadie estuviera mirando, encripta como todos".

Y eso es porque proteger sus datos

es una práctica recomendada de seguridad.

Los datos son un activo comercial valioso

y todas las empresas almacenan datos que deben protegerse.

Piense en datos financieros, datos de clientes, planes de negocios,

o incluso código propietario,

y el cifrado es una excelente manera de proteger sus datos

contra el acceso no autorizado.

Ahora, con S3, obtiene algunas opciones de cifrado diferentes.

En primer lugar, admite el cifrado en tránsito mediante SLL,

que significa Capa de sockets seguros y TLS,

que significa Seguridad de la capa de transporte.

Y estos son protocolos estándar de la industria.

para cifrar datos que viajan a través de una red.

Y estos protocolos nos permiten usar HTTPS

para acceder a un sitio web de forma segura.

Entonces, cuando usamos HTTPS al acceder a un sitio web,

nuestra comunicación con ese sitio web está encriptada.

Por ejemplo, cuando escribimos una contraseña,

que la comunicación está encriptada.

Ahora, S3 también admite el cifrado en reposo,

también conocido como cifrado del lado del servidor,

y hay tres opciones diferentes disponibles.

En primer lugar, tienes SSE-S3,

que utiliza claves de cifrado administradas por S3,

y utiliza el cifrado AES de 256 bits estándar de la industria.

Y este método de encriptación

está habilitado de forma predeterminada,

entonces , cuando crea un depósito S3 y carga un objeto en S3,

va a ser encriptado usando este método.

A continuación, está SSE-KMS, y esto es cifrado en reposo

usando claves de encriptación que son administradas

por el servicio de administración de claves de AWS.

Y este es bueno para usar

si tiene requisitos reglamentarios

eso significa que usted necesita ser el que crea

y la gestión de sus claves de cifrado.

Y luego también está SSE-C,

que es el cifrado utilizando claves proporcionadas por el cliente.

Y esto es para clientes que quieren generar

sus propias claves y administrarlas fuera de AWS.

Y luego el último tipo de encriptación que se admite

es el cifrado en reposo utilizando el cifrado del lado del cliente.

Y aquí es donde usted mismo encripta los archivos

antes de cargarlos en S3.

Entonces, para el examen, recuerde que S3 admite el cifrado

en tránsito usando SSL/TLS, y su encriptación en tránsito

que estamos usando cuando accedemos a un sitio web usando HTTPS.

El cifrado en reposo también se conoce como cifrado del lado del servidor,

y S3 nos da tres opciones diferentes.

Así que tenemos SSE-S3, que es el predeterminado, SSE-KMS,

donde se gestionan las claves de cifrado

dentro del servicio de gestión de claves, y SSE-C,

y esto es para los clientes

que quieran generar sus propias claves fuera de AWS.

Y finalmente, está el cifrado del lado del cliente,

donde encriptas los archivos tú mismo

antes de cargarlos en S3.

Y recuerda, que es SSE-S3

que está habilitado por defecto.

Entonces encriptación usando SSE-S3

está habilitado cuando crea un depósito S3 por primera vez

y cuando subes un nuevo objeto.

Eso es todo por esta lección.

Cualquier pregunta, hágamelo saber.

De lo contrario, te veré en la próxima.

Gracias.