[ENGLISH]

Hello, cloud gurus, and welcome to this lesson,

which is a summary of the KMS section,

including my exam tips.

So when it comes to creating a customer master key,

first of all, we'll create an alias and a description

and select a key material option.

So do we want to use key material generated by KMS

or do we want to provide our own key material?

Next, we set up the key administrators.

So that's the identity access management users and roles

that can administer the key.

Then finally, we also need to set up

the key usage permissions,

and that's the users and roles that can use the key

to encrypt and decrypt data in our account.

An AWS managed key is an AWS provided and managed CMK

and it's used on your behalf with the AWS services

that are integrated with KMS,

whereas a customer managed key is one that you create,

own and manage yourself.

It can be used to encrypt and decrypt files

up to four kilobytes in size and generate the data key.

And a data key is an encryption key

that you can use to encrypt data,

including large amounts of data.

And you can use a CMK to generate,

encrypt and decrypt data keys.

If you see anything in the exam

relating to envelope encryption,

this is all about encrypting the key that encrypts our data

and it provides an extra layer of protection.

The CMK is used to encrypt the data key,

also known as the envelope key,

and then the data key encrypts our data

and it's the data key that is used for encrypting anything

over four kilobytes in size.

And by using envelope encryption,

this avoids sending all your data into KMS over the network.

AWS provide lots of default keys, which are the CMKs

in your account that are created,

managed and used on your behalf

by an AWS service that is integrated with KMS.

For example, when you create an S3 bucket

and upload an object,

by default, it's gonna use this encryption key

to encrypt the object.

KMS API calls to be aware of are aws kms encrypt

and this encrypts plain text into ciphertext

using a customer master key,

aws kms decrypt decrypts ciphertext

that was encrypted using a customer master key,

aws kms re-encrypt decrypts ciphertext

and then re-encrypts it using a CMK that you specify,

for instance, if you change or manually rotate the CMK,

aws kms enables automatic key rotation every 365 days.

And aws kms generate-data-key uses the CMK

to generate a data key

to encrypt data using envelope encryption.

We can also enable automatic key rotation

using a checkbox in the console and when enabled,

KMS will rotate the cryptographic material

on a yearly basis.

And the great thing about automatic rotation

is that it saves previous versions

of the cryptographic material

so that you can still decrypt the files

that were previously encrypted using the old material.

Well, that's it for this lesson.

Any questions, let me know,

otherwise, I'll see you in the next one.

Thank you.

[SPANISH]

Hola, gurús de la nube, bienvenidos a esta lección.

que es un resumen de la sección KMS,

incluyendo mis consejos de examen.

Entonces, cuando se trata de crear una clave maestra de cliente,

primer lugar, crearemos un alias y una descripción

y seleccione una opción de material clave.

Entonces, ¿queremos usar material clave generado por KMS?

¿O queremos proporcionar nuestro propio material clave?

A continuación, configuramos los administradores de claves.

Así que esos son los usuarios y roles de administración de acceso de identidad

que puede administrar la clave.

Finalmente, también tenemos que configurar

los permisos de uso de claves,

y esos son los usuarios y roles que pueden usar la clave

para cifrar y descifrar datos en nuestra cuenta.

Una clave administrada por AWS es una CMK proporcionada y administrada por AWS

y se utiliza en su nombre con los servicios de AWS

que están integrados con KMS,

mientras que una clave administrada por el cliente es una que usted crea,

poseer y administrarse a sí mismo.

Se puede utilizar para cifrar y descifrar archivos

hasta cuatro kilobytes de tamaño y generar la clave de datos.

Y una clave de datos es una clave de cifrado

que puede usar para cifrar datos,

incluyendo grandes cantidades de datos.

Y puede usar una CMK para generar,

cifrar y descifrar claves de datos.

Si ves algo en el examen

relacionado con el cifrado de sobres,

se trata de cifrar la clave que cifra nuestros datos

y proporciona una capa extra de protección.

La CMK se utiliza para cifrar la clave de datos,

también conocida como la llave del sobre,

y luego la clave de datos encripta nuestros datos

y es la clave de datos que se utiliza para cifrar cualquier cosa

más de cuatro kilobytes de tamaño.

Y al usar el cifrado de sobres,

esto evita enviar todos sus datos a KMS a través de la red.

AWS proporciona muchas claves predeterminadas, que son las CMK.

en tu cuenta que se crean,

gestionado y utilizado en su nombre

por un servicio de AWS que está integrado con KMS.

Por ejemplo, cuando crea un depósito S3

y sube un objeto,

de forma predeterminada, usará esta clave de cifrado

para cifrar el objeto.

Las llamadas a la API de KMS para tener en cuenta son aws encriptar kms

y esto cifra el texto sin formato en texto cifrado

utilizando una clave maestra de cliente,

aws kms descifrar descifrar texto cifrado

que fue encriptado usando una clave maestra de cliente,

aws kms volver a cifrar descifrar texto cifrado

y luego lo vuelve a cifrar usando una CMK que usted especifique,

por ejemplo, si cambia o gira manualmente la CMK,

aws kms permite la rotación automática de claves cada 365 días.

y aws kms generar clave de datos utiliza la CMK

para generar una clave de datos

para cifrar los datos mediante el cifrado de sobres.

También podemos habilitar la rotación automática de claves

usando una casilla de verificación en la consola y cuando está habilitado,

KMS rotará el material criptográfico

sobre una base anual.

Y lo bueno de la rotación automática

es que guarda versiones anteriores

del material criptográfico

para que aún pueda descifrar los archivos

que fueron previamente encriptados utilizando el material antiguo.

Bueno, eso es todo por esta lección.

Cualquier pregunta, hágamelo saber,

de lo contrario , te veré en la próxima.

Gracias.