[ENGLISH]

Hello, Cloud Gurus,

and welcome to this lecture where we're going to review everything that we've

learned about customer master keys, including my exam tips.

So let's get started. So, first of all, with a CMK,

remember,

you can use an alias to create a friendly name that you can use to refer

to the CMK.

The CMK also has a creation date,

so the date and time when the CMK was

created. You can add your own description that's meaningful to you to

describe the CMK. Every customer master key also has a key state,

and typically you'll see enabled, disabled, pending deletion,

or unavailable. And if you remember, in my account, we had my new key,

which was enabled, and we also saw one in there that was pending deletion.,

that was going to get deleted tomorrow.

In terms of key material,

you can provide your own key material that was generated externally,

or you can use AWS provided. And finally,

customer master keys cannot be exported outside of KMS.

So they stay within KMS, and they are managed within KMS.

So you cannot export your entire customer master key out of KMS

and administer it somewhere else.

So let's move on to some of our exam tips and review everything you need to do

in order to set up a customer master key. So, first of all,

to set up our customer master key, we can create an alias,

a friendly name that we can use to help identify our key.

We can add a description that's meaningful to us so that we know which keys to

use for which applications or which teams.

And we need to choose our key material option.

So are we going to use key material that was generated by KMS,

or are we going to provide our own key material,

or are we going to use a CloudHSM?

The next thing we need to do is define the key administrative permissions.

So this is going to be the Identity Access Management users and roles who are

allowed to administer and manage the key.

So this is all about the administrative side,

the lifecycle management of the key, being able to delete the key,

or disable it.

So we need to provide the name of the Identity Access Management users or

roles who are going to have administrative permissions.

And then finally, we need to set the key usage permissions.

So this will be the permissions for the Identity Access Management users and

roles who can use the key to encrypt and decrypt data.

So these are the users and roles who are going to be performing cryptographic

operations using CMK.

So we're going to provide the names of any users or roles who are

going to have key usage permissions.

And when you say the term AWS-managed key,

that simply to the AWS-provided an AWS-managed

CMK and these are the CMKs that are used on your behalf

with the services that are integrated with KMS.

So services like S3 and RDS.

When you select encryption in the console for those services,

it's these AWS-managed keys, which are used in the background.

And when you see the term customer-managed key,

this refers to keys that you create, own, and manage yourself.

So they're not created by AWS. You create them yourself,

either using the command-line interface or using the console.

And later on, that's exactly what we're going to be doing.

So we'll create our own customer-managed CMK using the AWS

console. And then finally, we have the data key.

And if you remember,

the data key is an encryption key that you can use to encrypt data,

including large amounts of data.

So you can use your customer-managed CMK to generate, encrypt,

and decrypt your data key.

So that is the end of this lecture. If you have any questions,

please do let me know. Otherwise, feel free to move on to the next lecture.

Thank you.

[SPANISH]

Hola, gurús de la nube,

y bienvenidos a esta conferencia donde vamos a revisar todo lo que hemos

aprendí sobre las claves maestras del cliente, incluidos mis consejos para el examen.

Entonces empecemos. En primer lugar, con una CMK,

recuerda ,

puede usar un alias para crear un nombre descriptivo que puede usar para referirse

a la CMK.

La CMK también tiene una fecha de creación,

por lo que la fecha y la hora en que se activó la CMK

creado \_ Puede agregar su propia descripción que sea significativa para usted para

describir la CMK. Cada clave maestra de cliente también tiene un estado de clave,

y normalmente verá habilitado, deshabilitado, pendiente de eliminación,

o no disponible. Y si te acuerdas, en mi cuenta teníamos mi clave nueva,

que estaba habilitado, y también vimos uno allí que estaba pendiente de eliminación.,

eso iba a ser borrado mañana.

En cuanto al material clave,

puede proporcionar su propio material clave que se generó externamente,

o puede usar AWS proporcionado. Y finalmente,

del cliente no se pueden exportar fuera de KMS.

Por lo tanto, permanecen dentro de KMS y se administran dentro de KMS.

Por lo tanto, no puede exportar su clave maestra de cliente completa fuera de KMS

y administrarlo en otro lugar.

Entonces, pasemos a algunos de nuestros consejos para el examen y revisemos todo lo que debe hacer.

para configurar una clave maestra de cliente. Entonces, en primer lugar,

para configurar la clave maestra de nuestro cliente, podemos crear un alias,

un nombre descriptivo que podemos usar para ayudar a identificar nuestra clave.

Podemos agregar una descripción que sea significativa para nosotros para que sepamos qué claves

uso para qué aplicaciones o qué equipos.

Y tenemos que elegir nuestra opción de material clave.

Entonces, ¿vamos a usar material clave generado por KMS,

o vamos a proporcionar nuestro propio material clave,

¿O vamos a usar un CloudHSM ?

Lo siguiente que debemos hacer es definir los permisos administrativos clave.

Entonces, estos serán los usuarios y roles de Identity Access Management que están

autorizado a administrar y gestionar la clave.

Así que esto es todo sobre el lado administrativo,

la gestión del ciclo de vida de la clave, pudiendo eliminar la clave,

o desactivarlo.

Por lo tanto, debemos proporcionar el nombre de los usuarios de Identity Access Management o

roles que van a tener permisos administrativos.

Y finalmente, necesitamos establecer los permisos de uso de claves.

Estos serán los permisos para los usuarios de Identity Access Management y

roles que pueden usar la clave para cifrar y descifrar datos.

Estos son los usuarios y roles que van a realizar criptografía.

operaciones usando CMK.

Así que vamos a proporcionar los nombres de cualquier usuario o rol que esté

va a tener permisos de uso de clave.

Y cuando dice el término clave administrada por AWS,

que simplemente a la AWS-proporcionó un AWS-administrado

CMK y estas son las CMK que se utilizan en su nombre

con los servicios que se integran con KMS.

Así que servicios como S3 y RDS.

Cuando selecciona el cifrado en la consola para esos servicios,

son estas claves administradas por AWS, las que se utilizan en segundo plano.

Y cuando vea el término clave administrada por el cliente,

esto se refiere a claves que usted mismo crea, posee y administra.

Entonces no son creados por AWS. Los creas tú mismo,

ya sea usando la interfaz de línea de comandos o usando la consola.

Y más adelante, eso es exactamente lo que vamos a hacer.

Así que crearemos nuestra propia CMK administrada por el cliente usando AWS

consola \_ Y finalmente, tenemos la clave de datos.

Y si recuerdas,

la clave de datos es una clave de cifrado que puede utilizar para cifrar datos,

incluyendo grandes cantidades de datos.

De modo que puede usar su CMK administrada por el cliente para generar, cifrar,

y descifrar su clave de datos.

Así que ese es el final de esta conferencia. Si tienes alguna pregunta,

por favor hágamelo saber. De lo contrario, siéntase libre de pasar a la siguiente lección.

Gracias.