[ENGLISH]

Hello, Cloud Gurus, and welcome to this lesson,

where we are going to be creating

our own customer master key.

So if you'd like to join me in the console,

we'll get started.

So here I am in the AWS console.

And first of all, I'm going to search for IAM

because we need to create a couple of users

that are going to be able to manage and use the CMK.

And we're going to provide these usernames

when we create our CMK.

So first of all, I'm going to create a group.

So head to Groups,

Create Group,

and I'm going to call it myKMSGroup.

Scroll down to attach permissions.

And I'm going to give my group

administrator-level permissions.

So I want you to select AdministratorAccess.

Now, typically in real life,

this would maybe be your data center, security team,

or your security administration team--something like that.

And those people are going to need

administrator-level permissions

in order to do everything that they need to with KMS,

so that's why we select AdministratorAccess.

Once you've selected that, Create Group.

And the next thing we'll do is create a couple of users.

So select Users,

Add Users.

The first one I'm going to create is myKeyManager.

I'll give them programmatic access

and console access

with a custom password.

Deselect the password reset just to make it easier.

Hit Next.

And we're going to add this user

to the group we just created.

So hit Next,

Next,

and Create User.

So that is our key manager created.

And I'm also going to create a key user.

So back in IAM,

Users,

Add User.

Our second user is myKeyUser.

And once again, programmatic access and console access.

Deselect the password reset

and hit Next.

Add them to our KMS group.

Next, Next, and Create User.

So now we've got our 2 users set up.

We are ready to go and create our customer master key.

So at the top, let's search for KMS,

and select Key Management Service.

Select Create Key.

And the first option it gives you

is whether to use a symmetric key or an asymmetric key.

Now with symmetric encryption,

you've got a single encryption key,

which is used for both the encrypt

and the decrypt operations.

And then, with asymmetric encryption,

you get a public key and a private key pair.

And this key pair can be used for encrypting and decrypting,

and it can also be used for sign and verify operations.

But generally, for the majority of use cases,

we are going to use a symmetric key.

But if you use a symmetric key, that does require

that anyone who's going to encrypt or decrypt using this key

must have valid AWS credentials to use KMS.

However, if you do have a requirement

to encrypt data outside of KMS,

then you will need to use the asymmetric key.

So then you've got a public portion of the key,

which is used to encrypt the data outside of KMS,

and then your applications

are going to use the private portion of the key

to decrypt the data.

And for this course, we're going to be focusing

on symmetric keys because that's what comes up in the exam.

And if you'd like more detail,

then you can just click on this link here,

and it will open up a page in the documentation,

which explains everything in a little bit more detail.

So we're using a symmetric key here

for encryption and decryption,

but you can also use a symmetric key

for generating hash-based message authentication codes,

or HMAC codes.

And these are typically used

when you want to determine the authenticity of a message.

For instance, a JWT token, a JSON web token,

or even tokenized credit card information,

that kind of thing.

So it creates a special kind of message authentication code

that is used to verify the integrity

and the authenticity of a message.

So that's just another capability within KMS.

Moving down, we come to the advanced options,

and this is where you can select

where the key material for your CMK

is going to come from.

And when they say key material, what they really mean

is the cryptographic secrets that make up the key.

So the cryptographic secrets, which are going to be used

for the encryption and decryption processes.

So we need to select

where we're going to get our key material from,

and we've got 3 choices.

So firstly, we can just keep it to the default,

which is that KMS is going to generate

the key material for us.

Alternatively, we can provide our own key material

from an external source.

Let's say we already had our own cryptographic

infrastructure in our data center,

well we can use that to generate our own key material.

And then the third option is to use a custom key store,

like Cloud HSM.

And Cloud HSM is basically the next-level service to KMS,

and you pay an awful lot more,

but you do get your own dedicated single tenant hardware.

And you can use that to create

and manage your encryption keys.

And it is completely dedicated to you.

And it's really for customers that are operating

in a very highly regulated environment.

And maybe for compliance reasons,

they can't use multi-tenant hardware.

But don't worry too much about Cloud HSM

because that's out of scope for the exam,

but it's just another option with KMS.

And just remember that for the majority of customers

and for the majority of use cases,

using KMS to store your key material is absolutely fine.

Down here, we can select whether we want our key

to be used just in 1 single region,

or if we want to create a multi-region set of keys.

And if we select Multi-Region,

it's going to replicate our key to different regions.

And that allows you to encrypt your data in 1 region

and decrypt it in a different region.

And it's effectively using the same key,

so using the same key ID and the same key material--

very cool.

But we are going to just select 1 single region.

And with this option,

I can only encrypt and decrypt my data,

which is stored in the Northern Virginia region

that I'm operating in.

And I won't be able to use this key in any other region.

So if you're happy with that, hit Next.

At this stage, we can create an alias.

And my alias is going to be myCMK.

And you can use this alias to reference your key

in some of the KMS operations.

And it's just a more user-friendly way

of referring to your CMK.

So you can reference it just using this alias

instead of a really long key ID.

You can add tags if you want to.

I'm just going to skip that and hit Next.

And this is where we need to add our key administrator.

So who do we want to be able to administer the key

using the KMS API?

And it's listing out all of our users down here.

And we can just select the ones that we want.

So for our key administrator,

that's going to be myKeyManager.

So select that user,

and hit Next.

Here we're going to define who can actually use the key

to encrypt and decrypt data.

And that's going to be myKeyUser.

So select your user.

Down here, you can actually specify a different AWS account

that can use this key.

So if you've got another account that needs to use the key,

you can add it in here.

If you're happy with that, hit Next.

And after selecting our key user and our key administrator,

it's created this key policy,

and it's actually showing us the policy here.

So a key policy is a resource-based policy,

and it's similar to an IAM policy.

The syntax is very similar, so you should recognize it.

And if we scroll down,

we can see our key administrator access is defined here.

So here's our key manager

and all of the allowed actions for our key manager.

And then if we scroll down a little bit further,

we'll find our key usage permissions.

Here's myKeyUser,

and these are all the actions allowed for myKeyUser.

So now, we can go ahead and hit Finish.

And there is our CMK.

So here's the alias.

And here's our key ID.

And I think you'll agree that it's much easier

to refer to it using this alias than it is with this key ID.

Here's our status.

And the key is enabled in my account

and the specification of the key, which is a symmetric key.

And it also tells us the key usage.

And this key can be used for encryption and decryption.

And then one last thing that I wanted to show you

while we're in the console,

is that you can actually take a look

at your AWS managed keys in your account

by selecting AWS Managed Keys on the left.

And it should look similar to this,

but I think it all depends on which services

you've been using in your account.

Because when you come to use a service,

then AWS will create the CMK

for each of those services that you are using.

So when you come to use a service, AWS will create a CMK

for each of the services that you are using.

And I think what you see in this view all depends

on which services you've been using in your account.

And these are the CMKs that will be used by default

when we select encryption using any of these services.

So when you go to encrypt

or decrypt your data using services

like RDS or Elastic File System or S3, for instance,

these are the AWS managed keys that are going to be used.

So there we go.

We've just created our very first customer master key.

And later on in this section,

we're going to have a go at encrypting

and decrypting some data using this customer master key.

So please don't delete this customer master key

or the users that we just created

because we are going to be using them in the next lesson.

So if you're ready to continue,

please join me in the next lesson.

Thank you.

[SPANISH]

Hola, Cloud Gurus, y bienvenidos a esta lección.

donde vamos a estar creando

nuestra propia clave maestra de cliente.

Entonces, si desea unirse a mí en la consola,

vamos a empezar

Así que aquí estoy en la consola de AWS.

Y antes que nada, voy a buscar IAM

porque necesitamos crear un par de usuarios

que van a poder administrar y utilizar la CMK.

Y vamos a proporcionar estos nombres de usuario

cuando creamos nuestra CMK.

Primero que nada, voy a crear un grupo.

Dirígete a Grupos,

Crea un grupo,

y lo llamaré myKMSGroup .

Desplácese hacia abajo para adjuntar permisos.

Y le voy a dar a mi grupo

de nivel de administrador .

Así que quiero que selecciones AdministratorAccess .

Ahora, típicamente en la vida real,

este podría ser su centro de datos, equipo de seguridad,

o su equipo de administración de seguridad, algo así.

Y esa gente va a necesitar

permisos de nivel de administrador

para hacer todo lo que necesitan con KMS,

por eso seleccionamos AdministratorAccess .

Una vez que hayas seleccionado eso, Crear grupo.

Y lo siguiente que haremos será crear un par de usuarios.

Así que selecciona Usuarios,

Agregar usuarios.

El primero que voy a crear es myKeyManager .

Les daré acceso programático

y acceso a la consola

con una contraseña personalizada.

Anule la selección del restablecimiento de contraseña solo para que sea más fácil.

Presiona Siguiente.

Y vamos a agregar este usuario

al grupo que acabamos de crear.

Así que presiona Siguiente ,

Próximo,

y Crear usuario.

Así que ese es nuestro administrador de claves creado.

Y también voy a crear un usuario clave.

De vuelta en IAM,

usuarios,

Agregar usuario.

Nuestro segundo usuario es myKeyUser .

Y una vez más, acceso programático y acceso a consola.

Deseleccione el restablecimiento de contraseña

y presiona Siguiente.

Agrégalos a nuestro grupo KMS.

Siguiente, Siguiente y Crear usuario.

Así que ahora tenemos nuestros 2 usuarios configurados.

Estamos listos para ir y crear nuestra clave maestra de cliente.

Entonces, en la parte superior, busquemos KMS,

y seleccione Servicio de administración de claves.

Seleccione Crear clave.

Y la primera opción que te da

es si usar una clave simétrica o una clave asimétrica.

Ahora con cifrado simétrico,

tienes una única clave de cifrado,

que se utiliza tanto para el cifrado

y las operaciones de descifrado.

Y luego, con el cifrado asimétrico,

obtienes una clave pública y un par de claves privadas.

Y este par de claves se puede utilizar para cifrar y descifrar,

y también se puede utilizar para operaciones de firma y verificación.

Pero en general, para la mayoría de los casos de uso,

vamos a utilizar una clave simétrica.

Pero si usa una clave simétrica, eso requiere

que cualquiera que vaya a cifrar o descifrar usando esta clave

debe tener credenciales de AWS válidas para usar KMS.

Sin embargo, si tiene un requisito

para cifrar datos fuera de KMS,

entonces necesitará usar la clave asimétrica.

Entonces tienes una parte pública de la clave,

que se utiliza para cifrar los datos fuera de KMS,

y luego sus aplicaciones

van a utilizar la parte privada de la clave

para descifrar los datos.

Y para este curso, nos vamos a centrar

en claves simétricas porque eso es lo que surge en el examen.

Y si quieres más detalles,

entonces puedes simplemente hacer clic en este enlace aquí,

y se abrirá una página en la documentación,

que explica todo con un poco más de detalle.

Así que estamos usando una clave simétrica aquí

para el cifrado y descifrado,

pero también puedes usar una clave simétrica

para generar códigos de autenticación de mensajes basados en hash,

o códigos HMAC.

Y estos se utilizan normalmente

cuando desee determinar la autenticidad de un mensaje.

Por ejemplo, un token JWT, un token web JSON,

o incluso información de tarjeta de crédito tokenizada,

ese tipo de cosas

Entonces crea un tipo especial de código de autenticación de mensajes.

que se utiliza para verificar la integridad

y la autenticidad de un mensaje.

Así que esa es solo otra capacidad dentro de KMS.

Descendiendo, llegamos a las opciones avanzadas,

y aquí es donde puedes seleccionar

donde el material clave para su CMK

va a venir.

Y cuando dicen material clave, lo que realmente quieren decir

son los secretos criptográficos que componen la clave.

Así que los secretos criptográficos, que se van a utilizar

para los procesos de cifrado y descifrado.

Así que tenemos que seleccionar

dónde vamos a obtener nuestro material clave,

y tenemos 3 opciones.

Entonces, en primer lugar, podemos mantenerlo en el valor predeterminado,

que es que KMS va a generar

el material clave para nosotros.

Alternativamente, podemos proporcionar nuestro propio material clave.

de una fuente externa.

Digamos que ya tuviéramos nuestro propio criptográfico

infraestructura en nuestro centro de datos,

bueno, podemos usar eso para generar nuestro propio material clave.

Y luego, la tercera opción es usar un almacén de claves personalizado,

como la nube HSM.

Y Cloud HSM es básicamente el servicio de siguiente nivel para KMS,

y pagas muchísimo más,

pero usted obtiene su propio hardware de inquilino único dedicado.

Y puedes usar eso para crear

y administre sus claves de encriptación.

Y está completamente dedicado a ti.

Y es realmente para los clientes que están operando

en un entorno muy regulado.

Y tal vez por razones de cumplimiento,

pueden usar hardware multiusuario.

Pero no se preocupe demasiado por Cloud HSM

porque eso está fuera del alcance del examen,

pero es solo otra opción con KMS.

Y recuerde que para la mayoría de los clientes

y para la mayoría de los casos de uso,

usar KMS para almacenar su material clave está absolutamente bien.

Aquí abajo, podemos seleccionar si queremos nuestra clave

para ser utilizado solo en 1 sola región,

o si queremos crear un conjunto de claves multi-región.

Y si seleccionamos Multi-Región,

va a replicar nuestra clave a diferentes regiones.

Y eso le permite encriptar sus datos en 1 región

y descifrarlo en una región diferente.

Y está usando efectivamente la misma clave,

entonces usando la misma ID de clave y el mismo material de clave--

muy bueno

Pero solo vamos a seleccionar 1 sola región.

Y con esta opción,

Solo puedo cifrar y descifrar mis datos,

que se almacena en la región del norte de Virginia

que estoy operando.

Y no podré usar esta clave en ninguna otra región.

Entonces, si está satisfecho con eso, presione Siguiente .

En esta etapa, podemos crear un alias.

Y mi alias será myCMK .

Y puede usar este alias para hacer referencia a su clave

en algunas de las operaciones de KMS.

Y es solo una forma más fácil de usar

de hacer referencia a su CMK.

Para que pueda hacer referencia a él simplemente usando este alias

en lugar de una ID de clave realmente larga.

Puede agregar etiquetas si lo desea.

Voy a omitir eso y presionar Siguiente .

Y aquí es donde necesitamos agregar nuestro administrador clave.

Entonces, ¿quién queremos que pueda administrar la clave?

usando la API de KMS?

Y está enumerando a todos nuestros usuarios aquí abajo.

Y podemos simplemente seleccionar los que queramos.

Entonces, para nuestro administrador clave,

eso va a ser myKeyManager .

Así que seleccione ese usuario,

y presiona Siguiente.

Aquí vamos a definir quién puede realmente usar la clave.

para cifrar y descifrar datos.

Y ese va a ser myKeyUser .

Así que selecciona tu usuario.

Aquí abajo, puede especificar una cuenta de AWS diferente

que puede utilizar esta clave.

Entonces, si tiene otra cuenta que necesita usar la clave,

Puedes agregarlo aquí.

Si está satisfecho con eso, presione Siguiente .

Y después de seleccionar nuestro usuario clave y nuestro administrador clave,

ha creado esta política clave,

y en realidad nos está mostrando la política aquí.

Entonces, una política clave es una política basada en recursos,

y es similar a una política de IAM.

La sintaxis es muy similar, por lo que debe reconocerla.

Y si nos desplazamos hacia abajo,

podemos ver que nuestro acceso de administrador clave está definido aquí.

Así que aquí está nuestro administrador de claves

y todas las acciones permitidas para nuestro administrador de claves.

Y luego, si nos desplazamos hacia abajo un poco más,

encontraremos nuestros permisos de uso clave.

Aquí está myKeyUser ,

y estas son todas las acciones permitidas para myKeyUser .

Así que ahora, podemos seguir adelante y pulsar Finalizar .

Y ahí está nuestra CMK.

Así que aquí está el alias.

Y aquí está nuestra clave de identificación.

Y creo que estarás de acuerdo en que es mucho más fácil

para referirse a él usando este alias de lo que es con este ID de clave.

Aquí está nuestro estado.

Y la clave está habilitada en mi cuenta.

y la especificación de la clave, que es una clave simétrica.

Y también nos dice el uso de la clave.

Y esta clave se puede usar para cifrar y descifrar.

Y luego una última cosa que quería mostrarte

mientras estamos en la consola,

es que en realidad puedes echar un vistazo

en sus claves administradas por AWS en su cuenta

seleccionando AWS Managed Keys a la izquierda.

Y debería verse similar a esto,

pero creo que todo depende de qué servicios

has estado usando en tu cuenta.

Porque cuando llegas a usar un servicio,

entonces AWS creará la CMK

para cada uno de esos servicios que está utilizando.

Entonces, cuando use un servicio, AWS creará una CMK

para cada uno de los servicios que está utilizando.

Y creo que lo que ves en esta vista todo depende

en qué servicios has estado usando en tu cuenta.

Y estas son las CMK que se usarán por defecto

cuando seleccionamos el cifrado utilizando cualquiera de estos servicios.

Así que cuando vas a encriptar

o descifrar sus datos usando servicios

como RDS o Elastic File System o S3, por ejemplo,

estas son las claves administradas por AWS que se van a utilizar.

Así que ahí vamos.

Acabamos de crear nuestra primera clave maestra de cliente.

Y más adelante en esta sección,

vamos a intentar cifrar

y descifrar algunos datos utilizando esta clave maestra de cliente.

Por lo tanto, no elimine esta clave maestra de cliente

o los usuarios que acabamos de crear

porque los vamos a usar en la próxima lección.

Entonces, si está listo para continuar,

por favor únase a mí en la próxima lección.

Gracias.