[ENGLISH]

Hello Cloud Gurus,

and welcome to this section of the course where we're going to take a look at

KMS, or Key Management Service.

So what is KMS? Well, it stands for Key Management Service,

and it's a managed service that makes it really easy for you to create

and control the encryption keys used to encrypt your data in

AWS.

And one of the great things about KMS is that it's completely integrated

with loads of different AWS services,

and that means that encrypting data in those services is as easy as checking

a box in the console. So services like S3,

RDS, Elastic Block Store, Elastic File System,

will all allow you to really easily encrypt any data that you store in these

services, just by checking a box in the console.

So by integrating KMS with lots of different AWS services,

they've made it really easy for you to encrypt your data. So with KMS,

it's really simple to encrypt your data using encryption keys that you

manage. So when should we use KMS? Well,

basically you should be using it whenever you're dealing with sensitive

information. So whenever you're storing sensitive data within AWS,

you should think about encrypting it using KMS.

So think any data that you want to keep secret. For example,

if you're storing customer data, financial data, passwords,

so anything like database passwords, any secrets for your application,

and credentials as well.

So if you're storing any of that kind of data within AWS,

you want to think about encrypting that data. Now, as I said earlier,

KMS integrates with most other AWS services,

and the ones that you'll be familiar with are things like S3, RDS,

DynamoDB, Lambda.

And the way that Lambda can integrate with KMS is that it can go in and encrypt

and decrypt data,

provided you give it access to the KMS service and your encryption keys.

It also integrates with Elastic Block Store, Elastic File System,

and also CloudTrail.

And the interesting thing about CloudTrail is that you'll get an audit trail of

all of the API calls into KMS.

So you'll know exactly who has been using your keys to encrypt and

decrypt, and who has been attempting to access your encrypted data.

And it also integrates really well with the AWS Developer Tools.

And this is just some of the services.

I just wanted to highlight the ones that you might be aware of,

or that we're going to be learning about in this course. Now,

one of the main features of KMS that you're going to need to be aware of

is this idea of a CMK. So what is a CMK?

Well, it stands for customer master key,

and the customer master key is capable of encrypting and decrypting

data up to 4 kilobytes.

So you might be thinking that doesn't sound like very much data.

So what is it actually used for? Well,

the customer master key is used to generate, encrypt,

and decrypt the data key. And it's this data key,

which is then used in turn to encrypt and decrypt your data.

And this idea of using the customer master key to encrypt a data key,

and then using that data key to encrypt your data is known as envelope

encryption. And don't worry,

we're going to look at this in a little bit more detail later on in this section

of the course,

but just be aware that the customer master key can only encrypt and decrypt up

to 4 kilobytes of data,

and then anything over and above that you're going to need to generate a data

key and use that to encrypt or decrypt your data.

Now as always,

the best way to learn about AWS services is to get your

hands dirty, and that is exactly what we're going to do in the next lecture.

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

we're going to have a go at creating our own customer master key.

[SPANISH]

Hola gurús de la nube,

y bienvenidos a esta sección del curso donde vamos a echar un vistazo a

KMS, o Servicio de administración de claves.

Entonces, ¿qué es KMS? Bueno, significa Servicio de administración de claves,

y es un servicio administrado que hace que sea realmente fácil para usted crear

y controlar las claves de cifrado utilizadas para cifrar sus datos en

AWS.

Y una de las mejores cosas de KMS es que está completamente integrado

con un montón de diferentes servicios de AWS,

y eso significa que cifrar datos en esos servicios es tan fácil como verificar

una caja en la consola. Así que servicios como S3,

RDS, tienda de bloques elásticos, sistema de archivos elástico,

todos le permitirán encriptar fácilmente cualquier dato que almacene en estos

servicios , simplemente marcando una casilla en la consola.

Entonces, al integrar KMS con muchos servicios diferentes de AWS,

han hecho que sea muy fácil para usted cifrar sus datos. Así que con KMS,

es muy sencillo cifrar sus datos utilizando claves de cifrado que usted

administrar \_ Entonces, ¿cuándo deberíamos usar KMS? Bien,

básicamente deberías usarlo siempre que estés tratando con personas sensibles

información \_ Entonces, cada vez que almacene datos confidenciales en AWS,

deberías pensar en cifrarlo usando KMS.

Así que piensa en cualquier dato que quieras mantener en secreto. Por ejemplo,

si está almacenando datos de clientes, datos financieros, contraseñas,

así que cualquier cosa como contraseñas de bases de datos, cualquier secreto para su aplicación,

y credenciales también.

Entonces, si está almacenando ese tipo de datos dentro de AWS,

quiere pensar en cifrar esos datos. Ahora, como dije antes,

KMS se integra con la mayoría de los otros servicios de AWS,

y con los que estará familiarizado son cosas como S3, RDS,

DynamoDB , Lambda.

Y la forma en que Lambda puede integrarse con KMS es que puede entrar y cifrar

y descifrar datos,

siempre que le dé acceso al servicio KMS y a sus claves de cifrado.

También se integra con Elastic Block Store, Elastic File System,

y también CloudTrail .

Y lo interesante de CloudTrail es que obtendrá un registro de auditoría de

todas las llamadas API a KMS.

Así sabrá exactamente quién ha estado usando sus claves para cifrar y

descifrar y quién ha intentado acceder a sus datos cifrados.

Y también se integra muy bien con las Herramientas para desarrolladores de AWS.

Y estos son solo algunos de los servicios.

Solo quería resaltar los que podrías conocer,

o que vamos a aprender en este curso. Ahora,

una de las características principales de KMS que deberá tener en cuenta

es esta idea de una CMK. Entonces, ¿qué es una CMK?

Bueno, significa clave maestra del cliente,

y la clave maestra del cliente es capaz de cifrar y descifrar

datos de hasta 4 kilobytes.

Así que podrías estar pensando que no suena como una gran cantidad de datos.

Entonces, ¿para qué se usa realmente? Bien,

la clave maestra del cliente se utiliza para generar, cifrar,

y descifrar la clave de datos. Y es esta clave de datos,

que luego se utiliza a su vez para cifrar y descifrar sus datos.

Y esta idea de usar la clave maestra del cliente para cifrar una clave de datos,

y luego usar esa clave de datos para cifrar sus datos se conoce como sobre

cifrado \_ Y no te preocupes,

vamos a ver esto con un poco más de detalle más adelante en esta sección

del curso,

pero tenga en cuenta que la clave maestra del cliente solo puede cifrar y descifrar

a 4 kilobytes de datos,

y luego cualquier cosa por encima de lo que va a necesitar para generar datos

key y utilícela para cifrar o descifrar sus datos.

Ahora como siempre,

la mejor manera de aprender sobre los servicios de AWS es obtener su

manos sucias, y eso es exactamente lo que vamos a hacer en la próxima lección.

Entonces, si desea unirse a mí en la consola,

vamos a intentar crear nuestra propia clave maestra de cliente.