[ENGLISH]

Hello Cloud Gurus and welcome to this lesson

which is going to cover Certificate Management in AWS.

We'll cover what is AWS Certificate Manager or ACM.

What are SSL TLS certificates, ACM and CloudFront.

And finish off with my exam tips.

So what is AWS Certificate Manager?

Well, it's a service that allows you to create

and manage public and private SSL TLS certificates.

And it can be used with lots

of other AWS services, including Elastic Load Balancer

CloudFront, API Gateway, and web applications.

But you might be wondering, what are SSL TLS certificates?

Well, they're digital certificates that are used

to verify the authenticity of a website,

enabling a secure connection between the visitors

to the website and the website itself.

They're used during the encryption process

to encrypt data in transits.

So that means data that's traveling across the network so

that websites can provide a secure experience for customers.

So think of an online banking website

or an e-commerce website where you don't want your passwords

or other sensitive data traveling

across the network without being encrypted.

And an example use case could be, a company's website hosted

on EC2 instances and served

by CloudFront, that needs to host content securely

and protect user data using SSL TLS encryption.

So when the users access the website

they are using HTTPS.

Now CloudFront does have its own default certificate

that it uses, but you may have a requirement

to manage your own certificates instead

of using the default one.

For instance,

if you have your own domain name that you want to use

with CloudFront, only need to provide a certificate

to prove the authenticity of the website.

While the AWS recommended way of doing that is

to create a certificate using AWS Certificate Manager.

However, when working with CloudFront,

you will need to create that certificate

in the US East one region

if you are using AWS Certificate Manager

because that is the only supported region

if you want to use the certificate with CloudFront.

So in the CloudFront settings

you can optionally associate a custom

SSL certificate using AWS Certificate Manager,

but the certificate can only be in the US East one region

and it actually tells you this in the console.

So for the exam, just be aware

that we can use AWS Certificate Manager to create

and manage SSL TLS certificates for securing our websites.

This enables secure connections, so connections

to your website using HTTPS.

However, one thing to be aware

of if you are using AWS Certificate Manager with CloudFront

then you must create the certificate

in the US East one region

because no other regions are supported.

Well, that's it for this lesson.

If you've got any questions, please 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 la gestión de certificados en AWS.

Cubriremos qué es AWS Certificate Manager o ACM.

Qué son los certificados SSL TLS, ACM y CloudFront .

Y terminar con mis consejos de examen.

Entonces, ¿qué es AWS Certificate Manager?

Bueno, es un servicio que te permite crear

y administrar certificados SSL TLS públicos y privados.

Y se puede usar con muchos

de otros servicios de AWS, incluido Elastic Load Balancer

CloudFront , API Gateway y aplicaciones web.

Pero quizás se pregunte, ¿qué son los certificados SSL TLS?

Pues son certificados digitales que se utilizan

para verificar la autenticidad de un sitio web,

permitiendo una conexión segura entre los visitantes

al sitio web y al sitio web en sí.

Se utilizan durante el proceso de encriptación.

para cifrar datos en tránsitos.

Eso significa que los datos viajan a través de la red, por lo que

que los sitios web pueden proporcionar una experiencia segura para los clientes.

Así que piense en un sitio web de banca en línea

o un sitio web de comercio electrónico donde no desea sus contraseñas

u otros datos confidenciales que viajan

a través de la red sin ser encriptado.

Y un ejemplo de caso de uso podría ser el sitio web de una empresa alojado

en instancias EC2 y servido

por CloudFront , que necesita alojar contenido de forma segura

y proteger los datos de los usuarios mediante el cifrado SSL TLS.

Entonces, cuando los usuarios acceden al sitio web

están usando HTTPS.

Ahora CloudFront tiene su propio certificado predeterminado

que utiliza, pero es posible que tenga un requisito

para administrar sus propios certificados en su lugar

de usar el predeterminado.

Por ejemplo,

si tiene su propio nombre de dominio que desea usar

con CloudFront , solo necesita proporcionar un certificado

para probar la autenticidad del sitio web.

Si bien la forma recomendada por AWS de hacerlo es

para crear un certificado con AWS Certificate Manager.

Sin embargo, cuando se trabaja con CloudFront ,

tendrá que crear ese certificado

en la región este de EE. UU.

si está utilizando AWS Certificate Manager

porque esa es la única región admitida

si desea utilizar el certificado con CloudFront .

Así que en la configuración de CloudFront

puede asociar un personalizado

Certificado SSL usando AWS Certificate Manager,

pero el certificado solo puede estar en la región este de EE. UU.

y en realidad te dice esto en la consola.

Entonces, para el examen, solo tenga en cuenta

que podemos usar AWS Certificate Manager para crear

y administrar certificados SSL TLS para asegurar nuestros sitios web.

Esto permite conexiones seguras, por lo que las conexiones

a su sitio web usando HTTPS.

Sin embargo, una cosa a tener en cuenta

de si está utilizando AWS Certificate Manager con CloudFront

entonces debes crear el certificado

en la región este de EE. UU.

porque no se admiten otras regiones.

Bueno, eso es todo por esta lección.

Si tiene alguna pregunta, por favor hágamelo saber.

De lo contrario, te veré en la próxima.

Gracias.