[ENGLISH]

Hello Cloud Gurus and welcome to this lesson,

which is a summary of the S3 section.

Remember that S3 is object-based storage,

so it allows you to upload files and store them in AWS.

And it's a great place to store things

like images, videos, code, text files and documents,

et cetera.

However, it's not suitable to run an operating system

or a database.

Files can be up to five terabytes in size

and you get unlimited storage.

Files are stored in buckets

and S3 has a universal name space.

So all bucket names must be unique.

This is what an S3 URL looks like.

So we've got the bucket name, followed by the region,

followed by the key name,

which is the object name or file name.

And in my example,

I've got a bucket named Faye Cloud Guru

located in US-East-1,

and I've got a file in there called ralphie.jpeg.

And if you're using the CLI or the API,

then successful uploads

are gonna generate an HTTP 200 status code.

S3 objects consist of a key, which is the object name,

the value, which is the data itself,

made up of a sequence of bytes.

There's a version ID,

allowing you to store multiple versions

of the same object.

And also metadata,

which is data about the data you're storing,

like content type or the date it was last modified.

Remember the differences between the various storage classes

or tiers.

S3 Standard is suitable for most workloads

and it's great for frequently accessed data.

S3 Standard-Infrequent Access

is long-term storage for infrequently accessed

critical data,

like backups or disaster recovery files.

S3 One Zone-Infrequent Access,

is for long-term, infrequently accessed noncritical data,

and the data is stored redundantly

in one single availability zone,

so it's not suitable for critical data like backups.

Glacier Instant Retrieval

is used for archiving long-lived data

that needs millisecond retrieval times.

And Glacier is of course,

a cost effective way to store your data,

but you do pay a fee every time you access the data.

Glacier Flexible Retrieval is for archiving data

that needs to be accessed within a few hours or minutes.

And Glacier Deep Archive is for rarely accessed data,

with default retrieval times of 12 hours.

And then there's also S3 Intelligent-Tiering,

designed for unpredictable access patterns

and it will automatically move infrequently accessed data

to a more cost effective storage class to save you money.

Onto security, and S3 is secured by default.

So by default, all newly created buckets are private.

You can control access to your buckets

using bucket policies,

which apply permissions at a bucket level.

And S3 buckets can be configured to produce access logs,

which log all requests to the S3 bucket.

And these logs get written to another bucket.

Onto encryption.

And S3 supports encryption in transit using SSL or TLS,

which is all about encrypting your data

as it travels over the network.

And we can also use HTTPS to encrypt our connections

to S3.

It also supports three different types

of encryption at rest, also known as server-side encryption.

By default, all new buckets and new objects that you upload

are configured with SSE-S3,

which uses the Advanced Encryption Standard

256 bit encryption.

And this uses encryption keys that are managed within S3.

Alternatively, you can use SSE-KMS,

which uses encryption keys that are managed within

the AWS KMS service, or Key Management Service.

And there's also SSE-C,

which uses encryption keys managed by you.

Now, we can also use client-side encryption as well

and this is where you encrypt the files yourself

before uploading them into S3.

Now you might be asked in the exam

about how to enforce encryption using a bucket policy.

So just remember,

that it's possible to use a bucket policy

to deny all put requests that do not include this

x-amz server-side encryption parameter

in the request header.

And you can also use a bucket policy

to deny requests that do not use AWS Secure Transport,

in order to enforce the use of HTTPS or SSL.

Onto cross-origin resource sharing or CORS.

And we can use CORS to enable the code in one bucket

to access code located in another S3 bucket.

And if you remember, we configured one S3 bucket

containing index.html and another containing loadpage.html.

Then, we configured CORS to allow the file

in our first bucket to read the file in our second bucket.

And then when we accessed the website,

index.html is referencing loadpage.html

and the website will display the contents of both files.

CloudFront is a service that allows you to improve

the performance of your website

by caching webpages at a local edge location.

And an edge location is the location

where the content is going to be cached,

and it's separate to an AWS Region or Availability Zone.

The origin is the origin of all the files

that CloudFront Is going to serve.

This could be an S3 bucket, an EC2 instance,

or Elastic Load Balancer, et cetera.

And the CloudFront distribution

represents the origin and configuration settings

for the content that you wish to distribute

using CloudFront.

So here is my edge location,

which is the location where the content is gonna be cached.

The origin is the origin of all the files

that CloudFront is going to serve,

and the CloudFront distribution

represents the origin and the configuration settings.

Edge locations are not just read only,

you can write to them as well.

S3 Transfer Acceleration utilizes

CloudFront edge locations to reduce latency for S3 uploads,

and objects within CloudFront are cached

for the time to live, and by default that is one day.

However, if your website is changing more frequently

than once a day, then you can clear the cached objects.

However, when you do that,

you will be charged.

CloudFront AllowedMethods,

defines the HTTP methods that your CloudFront distribution

is going to allow.

And there are three different options to choose from.

Now the first two, GET, HEAD,

and GET, HEAD, OPTIONS, are read only.

And then the third choice,

which includes PUT, POST, PATCH, and DELETE,

will allow your users to write data.

So when you are configuring CloudFront,

you need to consider what the users will need to do

on your website.

So for websites that are gonna be interactive,

allowing users to do more than read,

for example, if they need to complete forms

or upload data, et cetera,

then you will need to enable the third option

in your AllowedMethods.

Otherwise, your website is not gonna work.

When it comes to certificate management.

AWS Certificate Manager is used to create and manage

SSL/TLS certificates for securing your website.

And this is gonna allow secure connections using HTTPS.

But just remember,

that when you are using AWS Certificate Manager

with CloudFront,

the certificate must be created in the US-East-1 region

and no other region is supported.

Athena is an interactive query service,

and it allows you to query data that's stored in S3

using standard SQL queries.

And the great thing about it is that it's serverless,

so you don't need to configure any infrastructure

to use Athena.

So if you see anything in the exam

about querying your S3 data using standard SQL,

I want you to think Athena.

Well, that's it for this lesson.

Any questions, please let me know.

Otherwise, please join me in the next section.

Thank you.

[SPANISH]

Hola Cloud Gurus y bienvenidos a esta lección,

que es un resumen de la sección S3.

Recuerde que S3 es almacenamiento basado en objetos,

por lo que le permite cargar archivos y almacenarlos en AWS.

Y es un gran lugar para guardar cosas.

como imágenes, videos, código, archivos de texto y documentos,

etcétera .

Sin embargo, no es adecuado para ejecutar un sistema operativo

o una base de datos.

Los archivos pueden tener un tamaño de hasta cinco terabytes

y obtienes almacenamiento ilimitado.

Los archivos se almacenan en cubos

y S3 tiene un espacio de nombres universal.

Por lo tanto, todos los nombres de depósito deben ser únicos.

Así es como se ve una URL de S3.

Así que tenemos el nombre del depósito, seguido de la región,

seguido del nombre de la clave,

que es el nombre del objeto o nombre del archivo.

Y en mi ejemplo,

Tengo un cubo llamado Faye Cloud Guru

ubicado en US-East-1,

y tengo un archivo allí llamado ralphie.jpeg.

Y si está utilizando la CLI o la API,

luego cargas exitosas

son va a generar un código de estado HTTP 200.

Los objetos de S3 constan de una clave, que es el nombre del objeto,

el valor, que es el propio dato,

formado por una secuencia de bytes.

Hay una ID de versión,

permite almacenar múltiples versiones

del mismo objeto.

Y también metadatos,

que son datos sobre los datos que está almacenando,

como el tipo de contenido o la fecha en que se modificó por última vez.

Recuerde las diferencias entre las distintas clases de almacenamiento

o niveles.

S3 Standard es adecuado para la mayoría de las cargas de trabajo

y es ideal para datos de acceso frecuente.

S3 Estándar-Acceso infrecuente

es el almacenamiento a largo plazo para acceso poco frecuente

críticos ,

como copias de seguridad o archivos de recuperación de desastres.

S3 One Zone-Acceso poco frecuente,

es para datos no críticos a largo plazo, a los que se accede con poca frecuencia,

y los datos se almacenan de forma redundante

en una sola zona de disponibilidad,

por lo que no es adecuado para datos críticos como copias de seguridad.

Recuperación instantánea de glaciares

se utiliza para archivar datos de larga duración

que necesita tiempos de recuperación de milisegundos.

Y Glacier es, por supuesto,

una forma rentable de almacenar sus datos,

pero paga una tarifa cada vez que accede a los datos.

Glacier Flexible Retrieval es para archivar datos

que necesita ser accedido dentro de unas pocas horas o minutos.

Y Glacier Deep Archive es para datos a los que rara vez se accede,

con tiempos de recuperación predeterminados de 12 horas.

Y luego también está S3 Intelligent- Tiering ,

diseñado para patrones de acceso impredecibles

y moverá automáticamente los datos a los que se accede con poca frecuencia

a una clase de almacenamiento más rentable para ahorrarle dinero.

En cuanto a la seguridad, y S3 está protegido de forma predeterminada.

Entonces, de forma predeterminada, todos los cubos recién creados son privados.

Puedes controlar el acceso a tus cubos

usando políticas de depósito,

que aplican permisos a nivel de depósito.

Y los cubos S3 se pueden configurar para producir registros de acceso,

que registran todas las solicitudes en el depósito S3.

Y estos registros se escriben en otro depósito.

Sobre el cifrado.

Y S3 admite el cifrado en tránsito mediante SSL o TLS,

que se trata de cifrar sus datos

mientras viaja por la red.

Y también podemos usar HTTPS para cifrar nuestras conexiones

a S3.

También es compatible con tres tipos diferentes.

de cifrado en reposo, también conocido como cifrado del lado del servidor.

De forma predeterminada, todos los cubos nuevos y los objetos nuevos que cargue

están configurados con SSE-S3,

que utiliza el estándar de cifrado avanzado

Cifrado de 256 bits.

Y esto usa claves de cifrado que se administran dentro de S3.

Alternativamente, puede usar SSE-KMS,

que utiliza claves de cifrado que se gestionan dentro

el servicio AWS KMS o el servicio de administración de claves.

Y también está SSE-C,

que utiliza claves de cifrado administradas por usted.

Ahora, también podemos usar el cifrado del lado del cliente

y aquí es donde usted mismo encripta los archivos

antes de cargarlos en S3.

Ahora es posible que te pregunten en el examen

sobre cómo hacer cumplir el cifrado mediante una política de depósito.

Así que recuerda,

que es posible usar una política de depósito

para denegar todas las solicitudes de colocación que no incluyan esto

parámetro de cifrado del lado del servidor x- amz

en el encabezado de la solicitud.

Y también puede usar una política de depósito

para denegar solicitudes que no utilizan AWS Secure Transport,

para hacer cumplir el uso de HTTPS o SSL.

En el intercambio de recursos de origen cruzado o CORS.

Y podemos usar CORS para habilitar el código en un cubo

para acceder al código ubicado en otro depósito S3.

Y si recuerdas, configuramos un depósito S3

que contiene index.html y otro que contiene loadpage.html.

Luego, configuramos CORS para permitir que el archivo

en nuestro primer cubo para leer el archivo en nuestro segundo cubo.

Y luego, cuando accedimos al sitio web,

index.html hace referencia a loadpage.html

y el sitio web mostrará el contenido de ambos archivos.

CloudFront es un servicio que le permite mejorar

el rendimiento de su sitio web

en caché las páginas web en una ubicación de borde local.

Y una ubicación de borde es la ubicación

dónde se almacenará en caché el contenido,

y está separado de una región o zona de disponibilidad de AWS.

El origen es el origen de todos los archivos.

eso CloudFront va a servir.

Esto podría ser un depósito S3, una instancia EC2,

o Elastic Load Balancer, etcétera.

Y la distribución de CloudFront

representa el origen y los ajustes de configuración

por el contenido que deseas distribuir

usando frente a la nube .

Así que aquí está mi ubicación de borde,

que es la ubicación donde se almacenará en caché el contenido .

El origen es el origen de todos los archivos.

eso CloudFront va a servir,

y la distribución de CloudFront

representa el origen y los ajustes de configuración.

Las ubicaciones de borde no son solo de lectura,

puedes escribirles.

S3 Transfer Acceleration utiliza

de CloudFront para reducir la latencia para las cargas de S3,

y los objetos dentro de CloudFront se almacenan en caché

para el tiempo de vida, y por defecto es un día.

Sin embargo, si su sitio web cambia con más frecuencia

de una vez al día, puede borrar los objetos almacenados en caché.

Sin embargo, cuando haces eso,

se le cobrará.

frente a la nube métodos permitidos ,

define los métodos HTTP que su distribución de CloudFront

va a permitir.

Y hay tres opciones diferentes para elegir.

Ahora los dos primeros, GET, HEAD,

y GET, HEAD, OPTIONS, son de solo lectura.

Y luego la tercera opción,

que incluye PUT, POST, PATCH y DELETE,

permitirá a sus usuarios escribir datos.

Entonces, cuando esté configurando CloudFront ,

debe considerar lo que los usuarios deberán hacer

en su sitio web

Entonces, para los sitios web que van a ser interactivos,

permitiendo a los usuarios hacer más que leer,

por ejemplo, si necesitan completar formularios

o subir datos, etcétera,

entonces deberá habilitar la tercera opción

en sus métodos permitidos .

De lo contrario, su sitio web no funcionará .

Cuando se trata de la gestión de certificados.

AWS Certificate Manager se utiliza para crear y administrar

Certificados SSL/TLS para asegurar su sitio web.

Y esto permitirá conexiones seguras usando HTTPS.

Pero recuerda,

que cuando utiliza AWS Certificate Manager

con frente a la nube ,

el certificado debe crearse en la región US-East-1

y ninguna otra región es compatible.

Athena es un servicio de consulta interactivo,

y le permite consultar los datos almacenados en S3

mediante consultas SQL estándar.

Y lo mejor de esto es que no tiene servidor ,

por lo que no necesita configurar ninguna infraestructura

usar Atenea.

Así que si ves algo en el examen

sobre consultar sus datos S3 usando SQL estándar,

Quiero que pienses en Atenea.

Bueno, eso es todo por esta lección.

Para cualquier duda, por favor hágamelo saber.

De lo contrario, únase a mí en la siguiente sección.

Gracias.