[ENGLISH]

Hello Cloud Gurus and welcome to this lecture.

We're going to have a look at a couple of mechanisms

that you can use to secure your S3 buckets.

Now, S3 is extremely secure by default

and by default, all newly created buckets

are completely private.

So by default, only the bucket owner

can upload new files,

read files and delete files, et cetera.

Nobody else has permission

and there is no public access by default.

So there's no anonymous access

and no access to users

who are not the bucket owner by default.

However, you might wish to allow other AWS users

or even anonymous users

to have read access

or even read and write access

to an S3 bucket that you own.

For example, if you're collaborating with other users

or providing data to other users or applications.

So how do we enable other users

to read and write the objects within our S3 buckets?

Well, one of the ways that we can do that

is using bucket policies.

So you can set up access control to your buckets

using bucket policies.

Now, bucket policies are applied at a bucket level,

so the clue is in the name.

And permissions granted by the policy

are going to apply to all of the objects

within the bucket.

So we're not applying permissions

to individual objects

and you cannot attach a bucket policy

to an individual object.

So it's not fine-grained access control.

It's a blanket control

for everything within your bucket.

However, bucket policies, they are really useful.

If you have a group of files in the same bucket

and they need to be accessed by the same people.

Say, for example, you would like to enable

another team member

to be able to read all of the files

within your bucket.

That would be a really good use case

for bucket policies.

Now, bucket policies are written in JSON,

which of course, stands for

JavaScript object notation language

and it's basically, a list of key-value pairs.

And here is an example of a bucket policy

and I've highlighted an example of a key-value pair.

So action would be the key

and S3 get objects would be the value.

So this bucket policing is allowing get object

or read access

to the contents of our bucket.

And here is the name of our bucket

and these permissions are being provided to all users

represented by this wild card.

And if this bucket policy looks familiar to you

then it should do

because the format of a bucket policy

is fairly similar to the format

of an Identity Access Management policy

that we have seen in the previous section.

And don't worry, you don't have to be a whiz

at writing JavaScript or writing JSON

in order to create these policies

because AWS provides a policy generator tool

to build out the policies

that you need within your AWS account.

And this is something that we're going to be looking at

in the next lecture.

Now, moving on to Bucket Access Control Lists

and they usually known as Bucket ACLs.

Now, Access Control Lists are applied at an object level.

So this means that we can apply different permissions

for different objects within the same bucket.

So using Access Control Lists,

we can grant different types of access

to different objects within our bucket.

And we can define which accounts and groups

are granted access

and also the type of access.

For example, read, write or full control.

And it's bucket ACLs

which give you the fine-grained access control

for objects within your S3 buckets.

So you can grant a different type of access

to different objects within the same bucket.

For example, you can apply different permissions

for different objects

for different users and groups.

So you could set some objects

within your bucket as publicly readable

and others as only readable by your own team

and you can do that using bucket Access Control Lists.

Now, S3 also provides access logs

and these are not enabled by default

but you can go in and enable S3 access logs.

And this will log all of the requests

made to your S3 buckets.

For example, every time a user makes a request

to upload a file,

read a file or delete a file.

This is going to be recorded in the S3 access log.

And when you enable S3 access logs,

you can have your logs written

to another S3 bucket.

So moving on to my exam tips

for securing S3.

Just remember that S3 is very secure by default

and by default, all newly created buckets

are completely private.

To control access to your S3 buckets,

we use bucket policies

which are applied at a bucket level

and you've also got bucket Access Control Lists

which are applied at an object level.

And it's the Access Control Lists

which give you fine-grained access

at an object level.

And then finally, we have access logs.

So, S3 buckets can be configured

to create access logs.

Which log all the requests made to the S3 bucket

and these logs can be written

to another S3 bucket.

And access logs are not configured by default.

So you need to go in and enable them yourself.

So that covers the main mechanisms for access control

to objects and buckets within S3.

And if it doesn't make an awful lot of sense right now,

don't worry because we're going to jump straight into a demo

in the next lecture,

to give you an opportunity

to get your hands dirty with S3.

So that's it for this lecture.

If you have any questions, please let me know.

Otherwise, feel free to move on to the next lecture.

Thank you.

[SPANISH]

Hola Cloud Gurus y bienvenidos a esta conferencia.

Vamos a echar un vistazo a un par de mecanismos.

que puede usar para asegurar sus cubos S3.

Ahora, S3 es extremadamente seguro por defecto

y por defecto, todos los cubos recién creados

son completamente privados.

Entonces, de forma predeterminada, solo el propietario del depósito

puede cargar nuevos archivos,

leer archivos y eliminar archivos, etcétera.

Nadie más tiene permiso

y no hay acceso público por defecto.

Así que no hay acceso anónimo.

y sin acceso a los usuarios

que no son los propietarios del depósito de forma predeterminada.

Sin embargo, es posible que desee permitir que otros usuarios de AWS

o incluso usuarios anónimos

tener acceso de lectura

o incluso acceso de lectura y escritura

a un depósito S3 de su propiedad.

Por ejemplo, si está colaborando con otros usuarios

o proporcionar datos a otros usuarios o aplicaciones.

Entonces, ¿cómo habilitamos a otros usuarios

para leer y escribir los objetos dentro de nuestros cubos S3?

Bueno, una de las maneras en que podemos hacer eso

está utilizando políticas de depósito.

Para que pueda configurar el control de acceso a sus cubos

utilizando políticas de depósito.

Ahora, las políticas de depósito se aplican a nivel de depósito,

así que la pista está en el nombre.

Y permisos otorgados por la política

se van a aplicar a todos los objetos

dentro del balde.

Así que no estamos aplicando permisos.

a objetos individuales

y no puede adjuntar una política de depósito

a un objeto individual.

Por lo tanto, no es un control de acceso detallado.

Es un control general

para todo dentro de su balde.

Sin embargo, las políticas de depósito son realmente útiles.

Si tiene un grupo de archivos en el mismo cubo

y necesitan ser accedidos por las mismas personas.

Digamos, por ejemplo, que le gustaría habilitar

otro miembro del equipo

para poder leer todos los archivos

dentro de tu balde.

Ese sería un muy buen caso de uso.

para políticas de depósitos.

Ahora, las políticas de depósito están escritas en JSON,

que por supuesto, significa

Lenguaje de notación de objetos JavaScript

y es básicamente una lista de pares clave-valor.

Y aquí hay un ejemplo de una política de depósito

y he resaltado un ejemplo de un par clave-valor.

Así que la acción sería la clave.

y S3 obtener objetos sería el valor.

Entonces, esta vigilancia de depósito permite obtener objetos

o acceso de lectura

al contenido de nuestro balde.

Y aquí está el nombre de nuestro balde.

y estos permisos se otorgan a todos los usuarios

representado por este comodín.

Y si esta política de depósitos le resulta familiar

entonces debería hacer

porque el formato de una política de depósito

es bastante similar al formato

de una política de gestión de acceso a la identidad

que hemos visto en el apartado anterior.

Y no te preocupes, no tienes que ser un genio

al escribir JavaScript o escribir JSON

para crear estas políticas

porque AWS proporciona una herramienta generadora de políticas

para construir las políticas

que necesita dentro de su cuenta de AWS.

Y esto es algo que vamos a estar viendo

en la próxima conferencia.

Ahora, pasemos a las Listas de control de acceso al depósito

y generalmente se conocen como ACL de depósito.

Ahora, las listas de control de acceso se aplican a nivel de objeto.

Entonces esto significa que podemos aplicar diferentes permisos

para diferentes objetos dentro del mismo cubo.

Entonces, usando listas de control de acceso,

podemos otorgar diferentes tipos de acceso

a diferentes objetos dentro de nuestro balde.

Y podemos definir qué cuentas y grupos

se les concede acceso

y también el tipo de acceso.

Por ejemplo, lectura, escritura o control total.

Y son las ACL del depósito

que le dan el control de acceso detallado

para objetos dentro de sus cubos S3.

Para que pueda otorgar un tipo diferente de acceso

a diferentes objetos dentro del mismo cubo.

Por ejemplo, puede aplicar diferentes permisos

para diferentes objetos

para diferentes usuarios y grupos.

Por lo que podría establecer algunos objetos

dentro de su cubo como legible públicamente

y otros como solo legibles por su propio equipo

y puede hacerlo usando listas de control de acceso de depósito.

Ahora, S3 también proporciona registros de acceso

y estos no están habilitados por defecto

pero puede ingresar y habilitar los registros de acceso de S3.

Y esto registrará todas las solicitudes.

hecho a sus cubos S3.

Por ejemplo, cada vez que un usuario realiza una solicitud

para subir un archivo,

leer un archivo o eliminar un archivo.

Esto se registrará en el registro de acceso de S3.

Y cuando habilita los registros de acceso de S3,

puedes tener tus registros escritos

a otro cubo S3.

Así que pasando a mis consejos para el examen

para asegurar S3.

Solo recuerda que S3 es muy seguro por defecto

y por defecto, todos los cubos recién creados

son completamente privados.

Para controlar el acceso a sus cubos S3,

usamos políticas de depósito

que se aplican a nivel de cubeta

y también tiene Listas de control de acceso de depósito

que se aplican a nivel de objeto.

Y son las Listas de Control de Acceso

que le dan acceso detallado

a nivel de objeto.

Y finalmente, tenemos registros de acceso.

Entonces, los cubos S3 se pueden configurar

para crear registros de acceso.

Que registra todas las solicitudes realizadas al depósito S3

y estos registros se pueden escribir

a otro cubo S3.

Y los registros de acceso no están configurados de forma predeterminada.

Por lo tanto, debe ingresar y habilitarlos usted mismo.

De modo que cubre los principales mecanismos para el control de acceso.

a objetos y cubos dentro de S3.

Y si no tiene mucho sentido en este momento,

no se preocupe porque vamos a saltar directamente a una demostración

en la próxima conferencia,

para darte una oportunidad

para ensuciarse las manos con S3.

Así que eso es todo por esta conferencia.

Si tiene alguna pregunta, por favor hágamelo saber.

De lo contrario, siéntase libre de pasar a la siguiente lección.

Gracias.