[ENGLISH]

Hello, Cloud Gurus,

and welcome to this lesson

where we'll take a look at S3 bucket policies.

And first of all,

we are gonna create an S3 bucket

and we'll review all of the options available with S3.

Next, we're gonna upload a file from our local machine

and we'll use a bucket policy

to enable public access to our file.

So if you'd like to get started,

please join me in the AWS console.

So from the console,

search for S3

and select create bucket.

And the first thing we need to do when we create a bucket,

is give it a DNS-compliant bucket name,

so this needs to be globally unique.

And I'm gonna call mine acloudguru-faye

and then, add a load of random numbers on the end,

and that should give me a globally-unique name.

I'll create it in the us-east-1 region.

Then, scroll down to public access settings.

And these are the default access settings

which block public access,

so they prevent public access to the data in your buckets.

So by default, everything is completely private.

Then, scroll down to bucket versioning.

And if you enable versioning,

then S3 is going to keep all the different versions

of the same object within the same bucket,

so if you accidentally delete an object or modify it,

then the previous version will still be there.

So, it's a really good way to protect your data

against accidentally deleting or modifying your files.

The next section is tags

and you can use tags to track your project

or team costs, for example,

and they're completely defined by you.

So, I could add the tag of project name

and I'm gonna call my project the Phoenix project.

And if you're on the lookout for something great to read,

there's actually a really good novel

called "The Phoenix Project,"

and it's a novel all about IT and DevOps.

It tells a story of a really dysfunctional company.

They're having loads of problems delivering a new IT project

until they finally see the light

and move towards a DevOps approach.

And they start using continuous integration

and continuous deployment,

which we're gonna be covering later on in this course.

And it's actually a really, really good read,

believe it or not,

and I've read it a couple of times

and I really like it.

So, that is highly recommended.

Scrolling down, the next option is encryption.

And by default,

they apply server-side encryption to all new buckets

and all new objects that are stored in your bucket.

And by default,

they use SSE-S3 which encrypts your data

using an encryption key that S3 manages for you.

And don't worry, because we're gonna go through

all the different types of encryption

in a lot more detail later in the course.

Now, you've also got the option of SSE-KMS,

and this uses KMS or the Key Management Service

to manage your encryption keys instead.

And we'll be going through KMS

in a lot more detail later on.

So now, let's just scroll down to the bottom

and create bucket.

So, that is our bucket created.

So next, I want you to select the bucket

and we're gonna upload a file.

So, select upload,

add files,

and I'm gonna select an image file from my local machine.

And I've included an image file that you can use

in the resources for this lesson.

Once you've selected the file, select upload,

and that is our file uploaded.

So now, we can try and access the file.

If you select the file name,

there are actually two different ways

that we can access the file from here.

Now, first of all,

we can select open,

and there is our file.

It's just an image of me and Ryan

at the AWS New York Summit.

Then, if I head back to the console,

the second way we can access the file

is as an unauthenticated user over the internet

using this object URL.

So if I select this link,

I'm gonna right-click and open in a new tab,

select the tab,

and we're actually gonna get this access denied message.

And the reason that we get access denied

is of course,

when we try to access the files from the browser

using this URL,

it's really exactly the same

as an anonymous access request.

And by default,

all S3 buckets are created without public access enabled.

So to access the object in this way,

we will need to enable public access

and that's exactly what we're gonna do next.

So, how do we make this file publicly available?

Well, let's head back to our bucket,

select our bucket name,

and select permissions.

And there are two things we'll need to do.

So first of all,

we need to edit these block public access settings.

So, select edit,

and I'm gonna remove these block public access settings

and save changes.

We'll need to confirm.

And now, you should see

that your block public access settings are set to off.

But at the top here,

it's still saying that the bucket and objects

are not public,

so the second thing that we need to do

is create a bucket policy.

So, scroll down to bucket policy,

select edit,

and we can use the policy generator to create our policy.

The type of policy is an S3 bucket policy.

The effect is allow.

The principle is gonna be star

because we're allowing public access.

The AWS service is S3.

And the action is going to be GetObject.

So, scroll down until you find GetObject,

and there it is.

So, make sure you've selected that.

The ARN is going to be the ARN of our S3 bucket

and you'll find that on the S3 screen.

And here it is.

So, select that

and paste it down here.

And then, after you've pasted the ARN,

you'll need to add forward slash

and the star character again,

so that it looks like that.

So, that means that this policy is going to apply

to everything inside the bucket.

After you've done that,

select add statement, here's our policy statement,

and generate policy.

And when you're done, this is what it should look like.

So we're gonna copy that policy,

head back to S3,

paste in the policy,

and just make sure that it looks like this

and make sure that you have added

this trailing forward slash and star character.

Once you're done, scroll down,

we can ignore this message,

and hit save changes.

I'm now gonna refresh my screen,

so refresh using the browser button.

And then, after you've done that,

your bucket should show as publicly accessible

and under permissions,

it should say that public access is allowed.

So now, if we come back to our object,

select objects,

select our object,

and click on the object URL,

there we go, you should see the image appear

because we have enabled public access

for the contents of this bucket.

So for the exam,

just remember that by default,

all newly-created S3 buckets are private

and public access is disabled by default.

And we can control access to everything

using bucket policies.

And you will also need to remember

to disable the block public access settings.

So, that is it for this lesson.

Any questions, please let me know.

Otherwise, I will see you in the next one.

Thank you.

[SPANISH]

Hola, gurús de la nube,

y bienvenidos a esta lección

donde veremos las políticas de depósito de S3.

Y en primer lugar,

vamos a crear un depósito S3

y revisaremos todas las opciones disponibles con S3.

A continuación, vamos a cargar un archivo desde nuestra máquina local.

y usaremos una política de depósito

para habilitar el acceso público a nuestro archivo.

Entonces, si desea comenzar,

Únase a mí en la consola de AWS.

Así que desde la consola,

buscar S3

y seleccione crear depósito.

Y lo primero que debemos hacer cuando creamos un cubo,

es darle un nombre de depósito compatible con DNS,

así que esto debe ser globalmente único.

Y voy a llamar al mío acloudguru-faye

y luego, agregue una carga de números aleatorios al final,

y eso debería darme un nombre único a nivel mundial.

Lo crearé en la región us -east-1.

Luego, desplácese hacia abajo hasta la configuración de acceso público.

Y estas son las configuraciones de acceso por defecto

que bloquean el acceso público,

por lo que impiden el acceso público a los datos en sus cubos.

Entonces, por defecto, todo es completamente privado.

Luego, desplácese hacia abajo hasta el control de versiones del depósito.

Y si habilita el control de versiones,

entonces S3 mantendrá todas las diferentes versiones

del mismo objeto dentro del mismo balde,

así que si accidentalmente elimina un objeto o lo modifica,

entonces la versión anterior seguirá estando allí.

Por lo tanto, es una muy buena manera de proteger sus datos

contra la eliminación o modificación accidental de sus archivos.

La siguiente sección son las etiquetas.

y puedes usar etiquetas para rastrear tu proyecto

o costes de equipo, por ejemplo,

y están completamente definidos por usted.

Entonces, podría agregar la etiqueta del nombre del proyecto

y voy a llamar a mi proyecto el proyecto Phoenix.

Y si está buscando algo bueno para leer,

hay una muy buena novela

llamado "El Proyecto Fénix",

y es una novela sobre TI y DevOps .

Cuenta la historia de una empresa realmente disfuncional.

Están teniendo muchos problemas para entregar un nuevo proyecto de TI

hasta que por fin ven la luz

y avanzar hacia un enfoque DevOps .

Y empiezan a utilizar la integración continua

y despliegue continuo,

que cubriremos más adelante en este curso.

Y en realidad es una muy, muy buena lectura,

creas o no,

y lo he leido un par de veces

y realmente me gusta

Entonces, eso es muy recomendable.

Desplazándose hacia abajo, la siguiente opción es el cifrado.

Y por defecto,

aplican encriptación del lado del servidor a todos los cubos nuevos

y todos los objetos nuevos que se almacenan en su cubo.

Y por defecto,

utilizan SSE-S3 que cifra sus datos

utilizando una clave de cifrado que S3 administra por usted.

Y no te preocupes, porque vamos a pasar

todos los diferentes tipos de encriptación

con mucho más detalle más adelante en el curso.

Ahora, también tiene la opción de SSE-KMS,

y esto usa KMS o el Servicio de administración de claves

para administrar sus claves de cifrado en su lugar.

Y estaremos pasando por KMS

con mucho más detalle más adelante.

Así que ahora, desplacémonos hacia abajo hasta el final

y crear cubo.

Entonces, ese es nuestro cubo creado.

A continuación, quiero que seleccione el cubo

y vamos a subir un archivo.

Por lo tanto, seleccione cargar,

agregar archivos,

y voy a seleccionar un archivo de imagen de mi máquina local.

Y he incluido un archivo de imagen que puedes usar

en los recursos para esta lección.

Una vez que haya seleccionado el archivo, seleccione cargar,

y ese es nuestro archivo subido.

Así que ahora, podemos intentar acceder al archivo.

Si selecciona el nombre del archivo,

hay dos maneras diferentes

que podemos acceder al archivo desde aquí.

Ahora, en primer lugar,

podemos seleccionar abierto,

y ahí está nuestro archivo.

Es solo una imagen mía y de Ryan.

en la Cumbre de Nueva York de AWS.

Luego, si vuelvo a la consola,

la segunda forma en que podemos acceder al archivo

es como un usuario no autenticado a través de Internet

utilizando esta URL de objeto.

Así que si selecciono este enlace,

Voy a hacer clic derecho y abrir en una nueva pestaña,

seleccione la pestaña,

y de hecho vamos a recibir este mensaje de acceso denegado.

Y la razón por la que se nos niega el acceso

es por supuesto,

cuando intentamos acceder a los archivos desde el navegador

utilizando esta URL,

es exactamente lo mismo

como una solicitud de acceso anónimo.

Y por defecto,

todos los depósitos de S3 se crean sin el acceso público habilitado.

Entonces, para acceder al objeto de esta manera,

tendremos que habilitar el acceso público

y eso es exactamente lo que haremos a continuación.

Entonces, ¿cómo hacemos que este archivo esté disponible públicamente?

Bueno, volvamos a nuestro balde,

seleccione nuestro nombre de cubo,

y seleccione los permisos.

Y hay dos cosas que tendremos que hacer.

Entonces, en primer lugar,

necesitamos editar estas configuraciones de bloqueo de acceso público.

Por lo tanto, seleccione editar,

y voy a eliminar estos bloqueos de configuración de acceso público

y guardar los cambios.

Tendremos que confirmar.

Y ahora, deberías ver

que su configuración de bloqueo de acceso público está desactivada.

Pero en la parte superior aquí,

sigue diciendo que el balde y los objetos

son publicos,

entonces lo segundo que tenemos que hacer

es crear una política de depósito.

Por lo tanto, desplácese hacia abajo hasta la política de depósito,

seleccione editar,

y podemos usar el generador de políticas para crear nuestra política.

El tipo de política es una política de depósito S3.

El efecto es permitir.

El principio va a ser estrella

porque estamos permitiendo el acceso público.

El servicio de AWS es S3.

Y la acción será GetObject .

Por lo tanto, desplácese hacia abajo hasta que encuentre GetObject ,

y ahí está

Por lo tanto, asegúrese de haber seleccionado eso.

El ARN va a ser el ARN de nuestro depósito S3

y lo encontrará en la pantalla del S3.

Y aquí está.

Entonces, selecciona eso

y pégalo aquí abajo.

Y luego, después de haber pegado el ARN,

deberás agregar una barra inclinada

y el personaje estrella de nuevo,

para que se vea así.

Entonces, eso significa que esta política se va a aplicar

a todo lo que hay dentro del balde.

Después de que hayas hecho eso,

seleccione agregar declaración, aquí está nuestra declaración de política,

y generar política.

Y cuando haya terminado, este es el aspecto que debería tener.

Así que vamos a copiar esa política,

regresa a S3,

pegar en la política,

y solo asegúrate de que se vea así

y asegúrese de haber agregado

esta barra inclinada hacia adelante y el carácter de estrella.

Una vez que haya terminado, desplácese hacia abajo,

podemos ignorar este mensaje,

y pulsa guardar cambios.

Ahora voy a actualizar mi pantalla,

así que actualice usando el botón del navegador.

Y luego, después de haber hecho eso,

su depósito debe mostrarse como de acceso público

y bajo permisos,

debe decir que el acceso público está permitido.

Así que ahora, si volvemos a nuestro objeto,

seleccionar objetos,

seleccione nuestro objeto,

y haga clic en la URL del objeto,

ahí vamos, deberías ver aparecer la imagen

porque hemos habilitado el acceso público

por el contenido de este balde.

Así que para el examen,

solo recuerda que por defecto,

todos los depósitos S3 recién creados son privados

y el acceso público está deshabilitado de forma predeterminada.

Y podemos controlar el acceso a todo

utilizando políticas de depósito.

Y también tendrás que recordar

para deshabilitar la configuración de bloqueo de acceso público.

Entonces, eso es todo por esta lección.

Para cualquier duda, por favor hágamelo saber.

De lo contrario, te veré en la próxima.

Gracias.