[ENGLISH]

Hello, Cloud Gurus, and welcome to this lesson,

where we'll be launching an EC2 instance with an S3 role.

So let's take a look at the objectives for this lesson.

First of all, we're going to create an Identity

and Access Management role with S3 access.

Next, we'll create an EC2 instance,

and we'll attach the role that we just created.

And then finally, we're going to try

and access S3 from our EC2 instance.

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

we'll get started.

So here I am in the console,

and the first thing I'm going to do is search for IAM.

Select IAM, and we'll head over to Roles.

Now, IAM roles are, of course,

a secure way to grant permission

to entities that you trust.

For instance, an IAM user in another account,

application code running on an EC2 instance,

or an AWS service that needs to perform an action

on resources in your account.

So basically, you use a role

to grant permission to entities within AWS,

and that's exactly what we'll do now.

So select Create Role, and then you need to select

which type of trusted entity we are creating the role for.

And it can either be an AWS service, like EC2 or Lambda;

another AWS account; a web identity;

for instance, Cognito, which we'll be learning about

later on in this course;

another identity provider, for instance,

a SAML 2.0 compliant identity provider,

like Facebook or Google; or even federation

with a corporate directory, like Active Directory.

And you can also create a custom trust policy,

enabling an IAM user from another account

to perform actions in this account.

But we are going to be creating a role

for an EC2 instance.

So just make sure that AWS Service is selected.

Then down here, under common use cases,

select EC2, and then hit Next.

And this is where we add a permissions policy to our role.

And this is going to be for S3 access.

So in the search box, just search for S3.

And we're going to give S3 full access

because we want our EC2 instance

to be able to create buckets, delete them,

add files, and read files as well.

And then if we click on this policy name,

it's going to open the policy up in a new tab.

Make sure that JSON is selected.

And then this is our policy document.

So in the policy statement here,

these are the permissions defined by the policy.

So the effect is allow and then it's allowing these actions.

And with this wildcard,

it's basically allowing all S3 actions.

And this is going to apply to all resources within S3.

So basically, this role is allowed to do anything inside S3

but it doesn't have any other permissions.

So our EC2 instance won't be allowed

to read DynamoDB tables, for example,

or launch another EC2 instance.

It only has permissions for S3.

So now I'm going to close that tab,

come back to my role, and scroll down to the bottom.

Hit Next, we need to give our role a name,

and I'm going to call it MyS3Role.

We can optionally add a tag, and I'm going to add a tag of

Team. And the team name is going to be Developers.

So now hit Create Role.

And that is our role created.

And if you search in the search box for "My",

there is our role.

So now, we need to attach our role to an EC2 instance.

So in the search box at the top, search for EC2.

I'm going to right-click and open in a new tab.

Then select Launch Instance.

I'm going to call it My S3 Instance.

Use the Amazon Linux AMI.

Instance type will be t3\_micro.

Scroll down to key pair.

I'm going to create a new key pair.

Give it a name and Create Key Pair.

Under network settings,

make sure that auto-assign public IP is set to enable.

And then scroll down to advanced details.

And it's here under IAM instance profile

that you need to select the role that you just created.

So make sure that your role has been selected.

And then you can go ahead and launch your instance.

And while it's initializing,

just select the instance ID here.

It might take a few moments to complete,

but as soon as it's finished initializing,

then you will be good to go.

And you can refresh this view using this button.

Once your instance has finished initializing

and it's past its status check, we are ready to log in.

And we're going to log in using EC2 Instance Connect.

And to do that, just select your instance on the left

and then select Connect at the top.

We'll use EC2 Instance Connect, hit Connect.

And it might just take a few seconds to connect.

And this method is not going to be covered in the exam--

it's just a quick and easy way

for you to connect your EC2 instance using SSH

from inside the AWS console.

So there we are, we are on our EC2 instance.

I'm going to clear the screen.

And now, let's test if we can access S3.

So type aws s3 ls.

There's no error message so that's a good sign.

And if you did have any S3 buckets in this account,

then they would show up here.

But let's see if we can create a new S3 bucket.

So type aws s3 mb, for make bucket.

Then s3:// and your bucket name.

And I'm just going to add some random numbers on the end

to make a unique bucket name.

And there we go.

We've successfully created an S3 bucket.

So now if we type aws s3 ls,

it's showing us the bucket name in our account.

So now, let's create a new file.

So we're just going to create a simple text file.

So type echo "This is a new file"

And then redirect that &gt; to a new file.

And the name of our file is file.txt and hit Enter.

There's our file.

And now we can just run aws s3 cp, for copy,

and then the name of our file.

And then I'm just going to copy and paste

the name of my S3 bucket and hit Enter.

So that has uploaded my file.

And then we can check that it's in there

by running aws s3 ls and the name of our bucket.

And hit Enter.

And there we go, it's found our file in our bucket.

So now we've verified that our EC2 instance

is able to read and write to S3.

And if we run aws configure list and hit Enter,

we can see that it's actually provided

an access key and secret access key.

And these are provided by the IAM role

that we associated with our EC2 instance

when we launched it.

And this is what is allowing our EC2 instance to access S3.

So what do you think would happen

if I go in and detach this role?

Well, let's try it and see.

Head back to the console, select your instance--

make sure it's selected on the left-hand side here--

select Actions, Security, and Modify IAM Role.

Here's the role that we attached.

And from the dropdown, select No IAM Role,

Update, and we need to confirm.

So we need to confirm that we want to detach this role.

Hit Detach, and then if we come back

to our Instance Connect console,

and sometimes when you leave it and come back,

you've lost your session.

So if that does happen, then just go back to your instance,

select your instance, and Connect again.

So from Instance Connect,

we'll run aws configure list again and hit Enter.

And there we go.

We can see that we've lost

our access key and secret access key.

So the credentials have gone,

and our permission has been taken away.

So if we run aws s3 ls

and our bucket name and hit Enter,

it's saying it's unable to locate our credentials,

and we need to run AWS Configure.

So that's pretty cool, right?

And we can actually go back in and reattach that role.

So let's come back to our instance.

Select Actions, Security,

we'll modify the IAM role again.

Select your S3 role and Update.

Come back to our Instance Connect session,

and we're going to run AWS configure list again,

and we'll see that our credentials have come back.

And you'll notice that they're actually different this time.

If you look at the last 4 characters of your access key

and secret access key, they're actually different

to the credentials that we had previously.

And that is because these are only temporary credentials.

And when you get credentials that are provided

by the IAM role, they are always temporary.

But if we go ahead and run aws s3 ls and our bucket name

and hit Enter, we've got the same access that we had before.

So what are my exam tips?

Well just remember that roles

are the preferred option from a security perspective.

And if you do see any questions in the exam

where they're asking you about how to enable

your application or your EC2 instance

to access AWS resources,

then the best practice is to use roles.

You should always avoid hard coding security credentials

in your application or on your EC2 instances.

And roles allow you to provide the access that you need

without you having to configure any access keys

and secret access keys--it's all done for you.

Policies are used to control the roles permissions.

So if you remember, we attached the S3

full access policy to our role,

and you can update a policy attached to a role,

and it's going to take immediate effect.

And as we saw earlier, you can attach

and detach roles from running EC2 instances

without having to stop or terminate the instance.

And when you do, it will take immediate effect.

So that is it for this lesson.

If you have any questions, please let me know.

Otherwise, I will see you in the next lesson.

Thank you.

[SPANISH]

Hola, Cloud Gurus, y bienvenidos a esta lección.

donde lanzaremos una instancia EC2 con un rol S3.

Así que echemos un vistazo a los objetivos de esta lección.

En primer lugar, vamos a crear una Identidad

y función de administración de acceso con acceso S3.

A continuación, crearemos una instancia EC2,

y adjuntaremos el rol que acabamos de crear.

Y finalmente, vamos a intentar

y acceda a S3 desde nuestra instancia EC2.

Entonces, si desea unirse a mí en la consola de AWS,

vamos a empezar

Así que aquí estoy en la consola,

y lo primero que voy a hacer es buscar IAM.

Seleccione IAM y nos dirigiremos a Roles.

Ahora, los roles de IAM son, por supuesto,

una forma segura de otorgar permiso

a las entidades en las que confía.

Por ejemplo, un usuario de IAM en otra cuenta,

de aplicación que se ejecuta en una instancia EC2,

o un servicio de AWS que necesita realizar una acción

en los recursos de su cuenta.

Entonces, básicamente, usas un rol

para otorgar permiso a entidades dentro de AWS,

y eso es exactamente lo que haremos ahora.

Así que seleccione Create Role, y luego debe seleccionar

qué tipo de entidad de confianza estamos creando el rol.

Y puede ser un servicio de AWS, como EC2 o Lambda;

otra cuenta de AWS; una identidad web;

por ejemplo, Cognito , sobre el que aprenderemos

más adelante en este curso;

otro proveedor de identidad, por ejemplo,

un proveedor de identidad compatible con SAML 2.0,

como Facebook o Google; o incluso federación

con un directorio corporativo, como Active Directory.

Y también puede crear una política de confianza personalizada,

habilitar un usuario de IAM desde otra cuenta

para realizar acciones en esta cuenta.

Pero vamos a estar creando un rol.

para una instancia EC2.

Así que solo asegúrese de que el Servicio de AWS esté seleccionado.

Luego, aquí abajo, en casos de uso común,

seleccione EC2 y luego presione Siguiente.

Y aquí es donde agregamos una política de permisos a nuestro rol.

Y esto va a ser para el acceso S3.

Entonces, en el cuadro de búsqueda, solo busque S3.

Y le daremos acceso total a S3

porque queremos nuestra instancia EC2

para poder crear cubos, eliminarlos,

agregar archivos y leer archivos también.

Y luego, si hacemos clic en el nombre de esta política,

va a abrir la política en una nueva pestaña.

Asegúrese de que JSON esté seleccionado.

Y luego este es nuestro documento de política.

Así que en la declaración de política aquí,

estos son los permisos definidos por la política.

Entonces, el efecto es permitir y luego está permitiendo estas acciones.

Y con este comodín,

está permitiendo todas las acciones de S3.

Y esto se aplicará a todos los recursos dentro de S3.

Básicamente, este rol puede hacer cualquier cosa dentro de S3

pero no tiene otros permisos.

Entonces nuestra instancia EC2 no estará permitida

para leer tablas de DynamoDB , por ejemplo,

o inicie otra instancia EC2.

Solo tiene permisos para S3.

Así que ahora voy a cerrar esa pestaña,

Vuelva a mi rol y desplácese hasta el final.

Presiona Siguiente , necesitamos darle un nombre a nuestro rol,

y lo llamaré MyS3Role.

Opcionalmente, podemos agregar una etiqueta, y voy a agregar una etiqueta de

Equipo. Y el nombre del equipo será Desarrolladores.

Así que ahora presiona Crear rol.

Y ese es nuestro papel creado.

Y si busca en el cuadro de búsqueda "Mi",

ahí está nuestro papel.

Entonces, ahora debemos adjuntar nuestro rol a una instancia EC2.

Entonces, en el cuadro de búsqueda en la parte superior, busque EC2.

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

Luego seleccione Iniciar instancia.

Lo llamaré Mi instancia S3.

Utilice la AMI de Amazon Linux.

El tipo de instancia será t3\_micro.

Desplácese hacia abajo hasta el par de claves.

Voy a crear un nuevo par de claves.

Dale un nombre y crea un par de claves.

En la configuración de red,

asegúrese de que la asignación automática de IP pública esté configurada para habilitar.

Y luego desplácese hacia abajo hasta los detalles avanzados.

Y está aquí en el perfil de instancia de IAM.

que necesita para seleccionar el rol que acaba de crear.

Así que asegúrese de que su rol haya sido seleccionado.

Y luego puede continuar y lanzar su instancia.

Y mientras se está inicializando,

simplemente seleccione el ID de la instancia aquí.

Puede tardar unos minutos en completarse,

pero tan pronto como termine de inicializarse,

entonces estarás listo para irte.

Y puede actualizar esta vista usando este botón.

Una vez que su instancia haya terminado de inicializarse

y ha pasado su verificación de estado, estamos listos para iniciar sesión.

Y vamos a iniciar sesión usando EC2 Instance Connect.

Y para hacer eso, simplemente seleccione su instancia a la izquierda

y luego seleccione Conectar en la parte superior.

Usaremos EC2 Instance Connect, presione Connect.

Y puede que solo tarde unos segundos en conectarse.

Y este método no va a ser cubierto en el examen--

es solo una manera rápida y fácil

para que conecte su instancia EC2 mediante SSH

desde el interior de la consola de AWS.

Ahí estamos, estamos en nuestra instancia EC2.

Voy a limpiar la pantalla.

Y ahora, probemos si podemos acceder a S3.

Así que escriba aws s3 ls .

No hay ningún mensaje de error, por lo que es una buena señal.

Y si tenía depósitos de S3 en esta cuenta,

entonces aparecerían aquí.

Pero veamos si podemos crear un nuevo depósito S3.

Así que escriba aws s3 mb , para hacer cubo.

Luego s3:// y el nombre de su depósito.

Y solo voy a agregar algunos números aleatorios al final

para hacer un nombre de cubo único.

Y ahí vamos.

Hemos creado con éxito un depósito S3.

Ahora, si escribimos aws s3 ls ,

nos muestra el nombre del cubo en nuestra cuenta.

Así que ahora, vamos a crear un nuevo archivo.

Así que solo vamos a crear un archivo de texto simple.

Así que escribe echo "Este es un archivo nuevo"

Y luego redirigir ese & gt ; a un archivo nuevo.

Y el nombre de nuestro archivo es file.txt y presiona Enter.

Ahí está nuestro archivo.

Y ahora podemos simplemente ejecutar aws s3 cp , para copiar,

y luego el nombre de nuestro archivo.

Y luego solo voy a copiar y pegar

el nombre de mi depósito S3 y presione Entrar.

Así que ha subido mi archivo.

Y luego podemos comprobar que está ahí

ejecutando aws s3 ls y el nombre de nuestro depósito .

Y presiona Entrar.

Y ahí vamos, encontró nuestro archivo en nuestro balde.

Así que ahora hemos verificado que nuestra instancia EC2

es capaz de leer y escribir en S3.

Y si ejecutamos aws configure list y presionamos Enter,

podemos ver que en realidad se proporciona

una clave de acceso y una clave de acceso secreta.

Y estos son proporcionados por el rol de IAM.

que asociamos con nuestra instancia EC2

cuando lo lanzamos.

Y esto es lo que permite que nuestra instancia EC2 acceda a S3.

Entonces, ¿qué crees que pasaría ?

si entro y me desprendo de este papel?

Bueno, probemos y veremos.

Regrese a la consola, seleccione su instancia--

asegúrese de que esté seleccionado en el lado izquierdo aquí--

seleccione Acciones, Seguridad y Modificar rol de IAM.

Aquí está el papel que adjuntamos.

Y en el menú desplegable, seleccione Sin rol de IAM,

Actualizar, y tenemos que confirmar.

Por lo tanto, debemos confirmar que queremos separar este rol.

Presiona Separar, y luego si volvemos

a nuestra consola Instance Connect,

y a veces cuando lo dejas y vuelves,

has perdido tu sesión.

Entonces, si eso sucede, simplemente regrese a su instancia,

seleccione su instancia y vuelva a conectarse.

Entonces, desde Instance Connect,

ejecutaremos aws configure list nuevamente y presionaremos Enter.

Y ahí vamos.

Podemos ver que hemos perdido

nuestra clave de acceso y clave de acceso secreta.

Así que las credenciales se han ido,

y nuestro permiso ha sido quitado.

Entonces, si ejecutamos aws s3 ls

y el nombre de nuestro cubo y presiona Enter,

dice que no puede localizar nuestras credenciales,

y necesitamos ejecutar AWS Configure.

Así que eso es genial, ¿verdad?

Y podemos regresar y volver a adjuntar ese rol.

Así que volvamos a nuestro ejemplo.

Seleccione Acciones, Seguridad,

modificaremos el rol de IAM nuevamente.

Seleccione su función S3 y actualice.

Vuelva a nuestra sesión de Instance Connect,

y vamos a ejecutar la lista de configuración de AWS nuevamente,

y veremos que nuestras credenciales han regresado.

Y notarás que en realidad son diferentes esta vez.

Si observa los últimos 4 caracteres de su clave de acceso

y clave de acceso secreta, en realidad son diferentes

a las credenciales que teníamos anteriormente.

Y eso es porque estas son solo credenciales temporales.

Y cuando obtiene las credenciales que se proporcionan

por el rol de IAM, siempre son temporales.

Pero si seguimos adelante y ejecutamos aws s3 ls y nuestro nombre de depósito

y presiona Enter, tenemos el mismo acceso que teníamos antes.

Entonces, ¿cuáles son mis consejos para el examen?

Bueno, solo recuerda esos roles

son la opción preferida desde una perspectiva de seguridad.

Y si ves alguna pregunta en el examen

donde te preguntan cómo habilitar

su aplicación o su instancia EC2

para acceder a los recursos de AWS,

entonces la mejor práctica es usar roles.

Siempre debe evitar las credenciales de seguridad codificadas

en su aplicación o en sus instancias EC2.

Y los roles le permiten proporcionar el acceso que necesita

sin tener que configurar ninguna clave de acceso

y claves de acceso secretas: todo está hecho para usted.

Las políticas se utilizan para controlar los permisos de los roles.

Entonces, si recuerdas, adjuntamos el S3

completo a nuestro rol,

y puede actualizar una política adjunta a un rol,

y va a tener efecto inmediato.

Y como vimos anteriormente, puede adjuntar

y separar roles de ejecutar instancias EC2

sin tener que detener o terminar la instancia.

Y cuando lo haga, tendrá efecto inmediato.

Eso es todo por esta lección.

Si tiene alguna pregunta, por favor hágamelo saber.

De lo contrario, te veré en la próxima lección.

Gracias.