[ENGLISH]

Hello, Cloud Gurus, and welcome

to this lesson, where we're going to take a look

at how to configure cross-account access.

We'll begin with an overview of cross-account access.

We'll take a look at an example use case,

run through a quick demo, and finish off with my exam tips.

So what is cross-account access,

and why would we ever need it?

Well, it's all about delegating access

to resources in different AWS accounts that you own,

and it allows you to share resources

in 1 AWS account with users in a different AWS account.

And the way that we set it up

is by using Identity And Access Management roles.

So we create a role in 1 account to allow the access

and then grant permission to users

in a different account so that they can assume that role.

And the really cool thing is that you can switch roles

within the AWS Management Console itself.

So you can switch to a role

that grants you the permissions you need

in a different account and no password is required. Now

you might be wondering, "when would I actually use this?"

Well, imagine you've got a development account

and a production account,

and you want to give your developers access

to the management console

and a single S3 bucket in your production account.

So maybe your development team

are doing some development and testing

and they need some historical production data to work with.

And this is quite a common use case for a lot of companies.

Well, it's actually really easy

to set this up, and I'm going to show you how to do it.

So first of all,

you'll need to have your 2 accounts set up.

So we've got our development account

and production account. In the development account,

we need to create an Identity And Access Management group.

Next in the production account,

we'll create our S3 bucket, and this is the bucket

that we're going to give access to our developers.

Then still in our production account,

we'll need an Identity And Access Management policy

with permissions for the S3 bucket.

Now this policy is going to be attached to an IAM role,

and it's this role which is the most important thing here.

So this role defines a kind

of trust relationship between these 2 accounts. And

it's going to reference the account ID of our development

account to allow our group to assume the role.

And then finally, the last piece

of the puzzle is an Identity And Access Management policy

in the development account.

And this is going to allow our group to assume the role

that we created in the production account.

So hopefully all of that makes sense,

but it's going to be much clearer when you see it all

in action, so if you'd like to

join me the AWS console, we can have a go

at setting up cross-account access together.

Now you will not be able to do this using our AWS Sandbox,

and you can only set this

up using 2 accounts that you own.

But don't worry, in the exam, they're not going to test you

on all the technicalities of the process.

You just need to understand it at a very high level.

So here I am in the AWS console,

and I've got 2 accounts here.

And these are both accounts that I own.

So I've got my production account here,

and I've got a development account over here.

This one is using a regular Chrome browser window,

and then this one is using Chrome in incognito mode.

So that means that I can be logged

into both accounts concurrently without getting kicked off.

So if you are using Chrome, you can just use incognito mode

for one of the windows, and that will just allow you

to log into 2 different accounts at the same time.

And as I said before, we can't do this using the AWS

Sandbox. It's got to be your own personal account.

Now before I do anything else,

I'm going to make a note of my account IDs

because we're going to need them later on.

So if you head to the name of your account up

here,and select Account,

it's going to take you to a screen like this,

and you'll find your account ID up here.

So just make a note of each account number

so that it's easier to find later on.

And here's the account number for my development account.

So I'm just going to make a note of both of these numbers.

So now in my development account,

we're going to create an IAM group.

So search for IAM,

select User Groups, Create Group,

and I'm going to call my group Developers. Scroll down,

and then under permissions, I'll give them

AdministratorAccess for this account

and Create Group.

Next we're going to add a user.

So select Users, Add Users,

my user's name is Anna.

We'll give our user AWS Management Console access

with a custom password.

Uncheck the password reset option just to make it easier,

hit Next, and we'll add our user to the developers group.

Hit Next, Next, and Create User.

So that is our user created, and she can log in

to the AWS Management Console using this link.

So now, the next step is within our production account.

So head over to your production account,

and we are going to come to S3, select S3,

and we're going to create a new bucket.

So select Create Bucket.

I'm going to call it my-prod-share-data,

scroll down to the bottom, and Create Bucket.

Now the next thing we'll do is create

an Identity And Access Management policy.

And once again,

we're are doing that in our production account.

So search for IAM, select Policies,

Create Policy, select the JSON option.

I'm going to remove the sample code.

And I've already prepared the policy code

that we are going to use, and you'll find this

in the resources section for this course.

And if we take a look at this policy,

this permission here allows the user

to list all the buckets that exist in the account.

This one allows you to list the contents of the bucket.

This one allows you to get the location.

And then these 3 here allow you

to get, put, and delete objects from the bucket.

But there's a couple of things

that we need to update in here.

So we need to provide the ARN of our bucket.

So we're going to replace this bucket name here

with the name that we used for our own bucket.

And mine was called my-prod-share-data,

so you want to replace it in both of these resource ARNs,

and just make sure that you don't delete this section

by mistake because the asterisk here is a wildcard,

and having it here just means that these permissions apply

to everything that's inside the bucket,

so all the files within the bucket.

So once you're happy with that, select Next, Review,

and we need to give our policy a name.

And I'm just going to call it developer-read-write-bucket,

scroll down, and Create Policy.

So that is our policy created in our production account.

And the next thing we need to do

is attach this policy to a role.

So let's go ahead and create our role.

So select Roles, Create Role.

Now we are creating this role for another AWS account,

so make sure you select this option.

And this is where we need to provide the account ID

for our development account.

Down here, select another AWS account,

and hopefully you made a note of your development account.

So paste the account ID of your development account in here.

It should be the 12-digit number.

Then scrolling down, we'll ignore these 2 options

because it's not going to be an external idea or a third

party. We're not going to use MFA either.

So then hit Next, and this is where

we can attach the policy that we just created to this role.

And I'm going to filter by type,

and the type is going to be customer-managed policies.

And that should bring up the policy that we just created.

And there it is, developer-read-write-bucket.

So just select that, hit Next. We'll give our role a name.

I'm going to call it MyDeveloperAccess.

Scroll down and Create Role.

So now let's head back to our development account.

I'm going to search for IAM,

User Groups, and select my Developers group,

go to Permissions.

And we need to add a new policy

allowing our developers to assume

the production role that we just created.

So select Add Permissions, and select Create Inline Policy.

And this is going to be a custom policy

that we're going to create ourselves, so select JSON.

I'm going to remove the sample code,

and you'll find this code

in the resources section of the course.

So just copy everything and paste it in here.

Now this policy basically allows anyone in the developers

group to assume the role in the production account,

and it uses this sts:AssumeRole API.

And there's one thing that we need to change here.

So first of all, we need to add our production account ID

into the ARN.

So paste in your production account ID,

and we just need to double-check the name

of my role because the names are case sensitive.

And if we get this wrong then it's not going to work.

But that looks pretty good to me.

As long as it matches the name of our role,

MyDeveloperAccess, then you will be good to go.

So if you're happy with your policy, select Review Policy.

We'll give our policy a name.

I'm going to call it AllowAssumeS3RoleInProd

and then Create Policy.

So that is our policy created,

and it's been added to our developers group.

So now, if we select Dashboard

on the right-hand side, over here on the right,

you'll find the sign-in URL for IAM users in this account.

So just copy that, I'm going to open it

in a new browser tab, and

we'll sign in as Anna.

Use the password that you set up earlier.

So now we are logged in as Anna.

And you can see the username up here.

But if we select the dropdown and then select Switch Role,

this is how we assume the role

that we set up in the production account.

So over here, we need to provide the account ID

for our production accounts.

So add the production ID in there.

Our role is MyDeveloperAccess.

You can set a display name, and you can select a color

so it will hopefully indicate

that you're operating under a different role.

And Anna's favorite color is blue.

So we're going to set it to blue and Switch Role.

And there we go.

And if that's all worked correctly, it should indicate

up here that I'm logged in as Anna from the dev team.

If you select the dropdown,

here's the role I've assumed in this account,

but I'm signed in as Anna from a different account.

So now let's head to S3 and see what Anna has access to.

Select S3.

And we can actually see 2 buckets here.

So here's the one that's been shared

with us, my-prod-share-data.

So select that one, and let's see if we can upload a file.

And I'm just going to upload

an image file and see if I'm allowed to do that.

And there we go.

We've successfully been able to upload a file, but

what about if we want to try and access a different bucket?

Head back to Buckets.

And I've got a different bucket in here.

This one hasn't been shared with Anna.

And there we go,

we're getting insufficient permission to list objects.

What if we try to upload a file, or we don't have access

for anything--we can't download and we can't upload?

And the reason for that is we only gave access

for that 1 single bucket, and our policy only

gives us access to the bucket that we specified.

So now let's switch back over to our developer account.

If you select the dropdown and select switch back,

we're back in our development account.

And if we head over to S3,

select buckets from the left-hand menu,

you will see the buckets

we were able to view earlier are no longer there

because we are back in our development account.

So that is cross-account access.

And don't worry, for the exam,

you don't need to remember all of the details.

You only need to know how it works at a very high level.

So let's review all of the steps that we did.

So we started off with a development account

and a production account.

We created our developer's

Identity And Access Management group

and we also created our user called Anna,

and she was a member of the developers group.

Next, in our production account,

we created an S3 bucket, and we created

an Identity And Access Management policy with permissions

to list, put, and delete items from the bucket.

We attached that policy to an IAM role,

and the role that we created specified the account ID

of our development account.

And then finally, we created another IAM policy,

this time in the development account,

which allowed our developers group

to assume the role that we created in production.

So that is everything that you should need

to know about cross-account access.

[SPANISH]

Hola, Cloud Gurus, y bienvenidos

a esta lección, donde vamos a echar un vistazo

en cómo configurar el acceso entre cuentas.

Comenzaremos con una descripción general del acceso entre cuentas.

Echaremos un vistazo a un ejemplo de caso de uso,

ejecute una demostración rápida y termine con mis consejos para el examen.

Entonces, ¿qué es el acceso entre cuentas ,

y ¿ por qué lo necesitaríamos?

Bueno, se trata de delegar el acceso

a recursos en diferentes cuentas de AWS de su propiedad,

y te permite compartir recursos

en 1 cuenta de AWS con usuarios en una cuenta de AWS diferente.

Y la forma en que lo configuramos

es mediante el uso de roles de gestión de acceso e identidad.

Entonces creamos un rol en 1 cuenta para permitir el acceso

y luego otorgar permiso a los usuarios

en una cuenta diferente para que puedan asumir ese rol.

Y lo realmente genial es que puedes cambiar de rol

dentro de la propia consola de administración de AWS.

Entonces puedes cambiar a un rol

que te otorga los permisos que necesitas

en una cuenta diferente y no se requiere contraseña. Ahora

es posible que se pregunte, "¿cuándo usaría esto realmente?"

Bueno, imagina que tienes una cuenta de desarrollo

y una cuenta de producción,

y desea dar acceso a sus desarrolladores

a la consola de administración

y un solo depósito S3 en su cuenta de producción.

Así que tal vez su equipo de desarrollo

están haciendo algo de desarrollo y pruebas

y necesitan algunos datos históricos de producción para trabajar.

Y este es un caso de uso bastante común para muchas empresas.

Bueno, en realidad es muy fácil.

para configurar esto, y le mostraré cómo hacerlo.

Entonces, en primer lugar,

necesitará tener sus 2 cuentas configuradas.

Así que tenemos nuestra cuenta de desarrollo

y cuenta de producción. En la cuenta de desarrollo,

Necesitamos crear un grupo de administración de identidad y acceso.

A continuación en la cuenta de producción,

crearemos nuestro depósito S3, y este es el depósito

que vamos a dar acceso a nuestros desarrolladores.

Entonces todavía en nuestra cuenta de producción,

necesitaremos una política de administración de identidad y acceso

con permisos para el depósito S3.

Ahora esta política se adjuntará a un rol de IAM,

y es este papel que es lo más importante aquí.

Así que este rol define un tipo

de relación de confianza entre estas 2 cuentas. Y

va a hacer referencia al ID de cuenta de nuestro desarrollo

cuenta para permitir que nuestro grupo asumiera el papel.

Y finalmente, la última pieza.

del rompecabezas es una política de gestión de identidad y acceso

en la cuenta de desarrollo.

Y esto va a permitir que nuestro grupo asuma el papel

que creamos en la cuenta de producción.

Así que espero que todo eso tenga sentido,

pero va a ser mucho más claro cuando lo veas todo

en acción, así que si quieres

únete a la consola de AWS, podemos intentarlo

en la configuración conjunta del acceso entre cuentas.

Ahora no podrá hacer esto usando nuestro AWS Sandbox,

y solo puedes configurar esto

usando 2 cuentas de tu propiedad.

Pero no te preocupes, en el examen no te van a poner a prueba.

sobre todos los tecnicismos del proceso.

Solo necesitas entenderlo a un nivel muy alto.

Así que aquí estoy en la consola de AWS,

y tengo 2 cuentas aquí.

Y estas son las dos cuentas que tengo.

Así que tengo mi cuenta de producción aquí,

y tengo una cuenta de desarrollo aquí.

Este está usando una ventana normal del navegador Chrome,

y luego este está usando Chrome en modo de incógnito.

Entonces eso significa que puedo estar registrado

en ambas cuentas al mismo tiempo sin ser expulsado.

Entonces, si está usando Chrome, puede usar el modo de incógnito

para una de las ventanas, y eso solo le permitirá

para iniciar sesión en 2 cuentas diferentes al mismo tiempo.

Y como dije antes, no podemos hacer esto usando AWS

Salvadera. Tiene que ser su propia cuenta personal.

Ahora, antes de hacer nada más,

Voy a tomar nota de mis ID de cuenta

porque los vamos a necesitar más adelante.

Entonces, si se dirige al nombre de su cuenta hacia arriba

aquí, y seleccione Cuenta,

va a llevar a una pantalla como esta,

y encontrará su ID de cuenta aquí.

Así que solo tome nota de cada número de cuenta

para que sea más fácil de encontrar más adelante.

Y aquí está el número de cuenta de mi cuenta de desarrollo.

Así que voy a tomar nota de estos dos números.

Así que ahora en mi cuenta de desarrollo,

vamos a crear un grupo de IAM.

Así que busca IAM,

seleccione Grupos de usuarios, Crear grupo,

y voy a llamar a mi grupo Desarrolladores. Desplácese hacia abajo,

y luego bajo permisos, les daré

AdministradorAcceso para esta cuenta

y Crear grupo.

A continuación vamos a agregar un usuario.

Así que seleccione Usuarios, Agregar usuarios,

mi nombre de usuario es Anna.

Le daremos a nuestro usuario acceso a la consola de administración de AWS

con una contraseña personalizada.

Desmarque la opción de restablecimiento de contraseña solo para que sea más fácil,

presione Siguiente y agregaremos nuestro usuario al grupo de desarrolladores.

Pulse Siguiente, Siguiente y Crear usuario.

Entonces ese es nuestro usuario creado, y ella puede iniciar sesión

a la Consola de administración de AWS usando este enlace.

Así que ahora, el siguiente paso está dentro de nuestra cuenta de producción.

Así que dirígete a tu cuenta de producción,

y vamos a llegar a S3, seleccione S3,

y vamos a crear un nuevo depósito.

Así que seleccione Crear cubo.

Voy a llamarlo my-prod-share-data,

desplácese hacia abajo hasta la parte inferior y Crear depósito.

Ahora lo siguiente que haremos es crear

una política de Gestión de Identidad y Acceso.

Una vez mas,

estamos haciendo eso en nuestra cuenta de producción.

Así que busque IAM, seleccione Políticas,

Crear política, seleccione la opción JSON.

Voy a eliminar el código de ejemplo.

Y ya he preparado el código de política

que vamos a usar, y encontrarás esto

en la sección de recursos de este curso.

Y si echamos un vistazo a esta política,

este permiso aquí permite al usuario

para enumerar todos los cubos que existen en la cuenta.

Este le permite enumerar el contenido del depósito.

Éste le permite obtener la ubicación.

Y luego estos 3 aquí te permiten

para obtener, colocar y eliminar objetos del depósito.

Pero hay un par de cosas

que tenemos que actualizar aquí.

Por lo tanto, debemos proporcionar el ARN de nuestro depósito.

Así que vamos a reemplazar este nombre de depósito aquí

con el nombre que usamos para nuestro propio balde.

Y el mío se llamaba my-prod-share-data,

por lo que desea reemplazarlo en ambos ARN de recursos,

y solo asegúrese de no eliminar esta sección

por error porque el asterisco aquí es un comodín,

y tenerlo aquí solo significa que se aplican estos permisos

a todo lo que hay dentro del balde,

por lo que todos los archivos dentro del cubo.

Entonces, una vez que esté satisfecho con eso, seleccione Siguiente, Revisar,

y necesitamos darle un nombre a nuestra política.

Y voy a llamarlo desarrollador-read-write-bucket,

desplácese hacia abajo y Crear política.

Así que esa es nuestra política creada en nuestra cuenta de producción.

Y lo siguiente que tenemos que hacer

es adjuntar esta política a un rol.

Así que sigamos adelante y creemos nuestro rol.

Así que seleccione Funciones, Crear función.

Ahora estamos creando este rol para otra cuenta de AWS,

así que asegúrese de seleccionar esta opción.

Y aquí es donde necesitamos proporcionar la identificación de la cuenta.

para nuestra cuenta de desarrollo.

Aquí abajo, seleccione otra cuenta de AWS,

y es de esperar que haya tomado nota de su cuenta de desarrollo.

Así que pegue el ID de cuenta de su cuenta de desarrollo aquí.

Debe ser el número de 12 dígitos.

Luego, desplazándonos hacia abajo, ignoraremos estas 2 opciones

porque no va a ser una idea externa o una tercera

fiesta \_ Tampoco vamos a usar MFA.

Entonces presione Siguiente , y aquí es donde

podemos adjuntar la política que acabamos de crear a este rol.

Y voy a filtrar por tipo,

y el tipo va a ser políticas administradas por el cliente.

Y eso debería mostrar la política que acabamos de crear.

Y ahí está, desarrollador-lectura-escritura-cubo.

Así que simplemente seleccione eso, presione Siguiente . Le daremos un nombre a nuestro rol.

Voy a llamarlo MyDeveloperAccess .

Desplácese hacia abajo y Crear rol.

Así que ahora volvamos a nuestra cuenta de desarrollo.

Voy a buscar IAM,

Grupos de usuarios y seleccione mi grupo de desarrolladores,

vaya a Permisos.

Y necesitamos agregar una nueva política

permitiendo que nuestros desarrolladores asuman

el rol de producción que acabamos de crear.

Así que seleccione Agregar permisos y seleccione Crear política en línea.

Y esto va a ser una política personalizada.

que vamos a crear nosotros mismos, así que seleccione JSON.

Voy a eliminar el código de muestra,

y encontrarás este código

en la sección de recursos del curso.

Así que copia todo y pégalo aquí.

Ahora bien, esta política básicamente permite que cualquiera de los desarrolladores

grupo para asumir el papel en la cuenta de producción,

y utiliza esta API sts:AssumeRole .

Y hay una cosa que tenemos que cambiar aquí.

Entonces, antes que nada, debemos agregar nuestra ID de cuenta de producción

en el ARN.

Así que pega tu ID de cuenta de producción,

y solo tenemos que verificar dos veces el nombre

de mi función porque los nombres distinguen entre mayúsculas y minúsculas.

Y si lo hacemos mal, entonces no va a funcionar.

Pero eso me parece bastante bien.

Siempre que coincida con el nombre de nuestro rol,

MyDeveloperAccess , entonces estará listo para comenzar.

Entonces, si está satisfecho con su política, seleccione Revisar política.

Le daremos un nombre a nuestra política.

Voy a llamarlo AllowAssumeS3RoleInProd

y luego Crear política.

Así que esa es nuestra política creada,

y se ha agregado a nuestro grupo de desarrolladores.

Así que ahora, si seleccionamos Dashboard

en el lado derecho, aquí a la derecha,

encontrará la URL de inicio de sesión para los usuarios de IAM en esta cuenta.

Así que copia eso, lo voy a abrir.

en una nueva pestaña del navegador, y

iniciaremos sesión como Anna.

Utilice la contraseña que configuró anteriormente.

Así que ahora estamos registrados como Anna.

Y puedes ver el nombre de usuario aquí.

Pero si seleccionamos el menú desplegable y luego seleccionamos Cambiar rol,

así es como asumimos el rol

que configuramos en la cuenta de producción.

Así que aquí, tenemos que proporcionar el ID de la cuenta.

para nuestras cuentas de producción.

Así que agregue la ID de producción allí.

Nuestro rol es MyDeveloperAccess .

Puede establecer un nombre para mostrar y puede seleccionar un color

por lo que con suerte indicará

que está operando bajo un rol diferente.

Y el color favorito de Anna es el azul.

Así que vamos a configurarlo en azul y cambiar de rol.

Y ahí vamos.

Y si todo ha funcionado correctamente, debería indicar

aquí que he iniciado sesión como Anna del equipo de desarrollo .

Si selecciona el menú desplegable,

aquí está el papel que he asumido en esta cuenta,

pero he iniciado sesión como Anna desde una cuenta diferente.

Así que ahora vayamos a S3 y veamos a qué tiene acceso Anna.

Seleccione S3.

Y en realidad podemos ver 2 baldes aquí.

Así que aquí está el que se ha compartido.

con nosotros, my-prod-share-data.

Seleccione ese y veamos si podemos cargar un archivo.

y solo voy a subir

un archivo de imagen y ver si puedo hacerlo.

Y ahí vamos.

Hemos podido subir un archivo con éxito, pero

Qué pasa si queremos probar y acceder a un depósito diferente?

Regresa a Baldes.

Y tengo un balde diferente aquí.

Este no ha sido compartido con Anna.

Y ahí vamos,

estamos obteniendo permisos insuficientes para listar objetos.

¿Qué sucede si intentamos cargar un archivo o no tenemos acceso?

para cualquier cosa--no podemos descargar y no podemos cargar?

Y la razón de eso es que solo dimos acceso

para ese 1 solo cubo, y nuestra política solo

da acceso al depósito que especificamos.

Así que ahora volvamos a nuestra cuenta de desarrollador.

Si selecciona el menú desplegable y selecciona volver atrás,

estamos de vuelta en nuestra cuenta de desarrollo.

Y si nos dirigimos a S3,

seleccione cubos en el menú de la izquierda,

verás los cubos

pudimos ver antes ya no están allí

porque estamos de vuelta en nuestra cuenta de desarrollo.

Eso es acceso entre cuentas.

Y no te preocupes, para el examen,

es necesario recordar todos los detalles.

Solo necesita saber cómo funciona a un nivel muy alto.

Entonces, repasemos todos los pasos que hicimos.

Así que empezamos con una cuenta de desarrollo

y una cuenta de producción.

Creamos nuestro desarrollador

Grupo de gestión de acceso e identidad

y también creamos nuestro usuario llamado Anna,

y ella era miembro del grupo de desarrolladores.

A continuación, en nuestra cuenta de producción,

creamos un depósito S3 y creamos

una política de gestión de acceso e identidad con permisos

para enumerar, colocar y eliminar elementos del cubo.

Adjuntamos esa política a un rol de IAM,

y el rol que creamos especificó el ID de la cuenta

de nuestra cuenta de desarrollo.

Y finalmente, creamos otra política de IAM,

esta vez en la cuenta de desarrollo,

lo que permitió a nuestro grupo de desarrolladores

para asumir el papel que creamos en la producción.

Así que eso es todo lo que deberías necesitar.

saber sobre el acceso entre cuentas.