[ENGLISH]

Hello, Cloud Gurus,

and welcome to this lesson where we'll get our hands dirty

with identity and access management.

And first of all,

we're going to set up multi-factor authentication

on our account.

Next, we'll create our first user,

then we'll create a group.

And finally, we're gonna create a role as well,

and then we'll finish off with my exam tips.

Now, you will need to use your own AWS account

to complete this lesson

because multifactor authentication cannot be performed

using the A Cloud Guru cloud playground

or sandbox environment.

So please join me in your own AWS account.

From the AWS console,

search for IAM,

and you should see a dashboard that is similar to this.

And remember, we're doing this in our own AWS account.

Now, as you can see,

I've got some security recommendations here,

because I haven't yet configured

multi-factor authentication.

So I'm getting this security alert.

So let's go ahead and set up multi-factor authentication.

Select add MFA,

and we need to assign a new MFA device.

So select assign MFA.

I'll give it a name,

my-MFA,

and scroll down to select your MFA device.

And I'm gonna use a virtual MFA device

installed on my smartphone.

So select the first option,

then come down to the bottom and hit next.

And this is where we're gonna set up our device.

First of all, you need to install a compatible application,

like Google Authenticator.

And if you select this link,

it will give you a list of supported applications.

And if you scroll down,

here are the virtual authenticator apps that are supported,

and there are some for Android and some for iOS.

But I like using Google Authenticator,

so that's the one that I'm gonna show you.

Back in the IAM console, scroll down to step two,

and we're gonna create a QR code.

So select show QR code,

then the next thing we do is

open up our authenticator app on our smartphone,

select the add button, select scan a QR code,

scan your code.

And after you scan the QR code on your phone,

Google Authenticator will start generating some MFA codes,

and you will need to fill in two consecutive codes

that are generated by the MFA device.

So here's my first one.

Then I'm gonna wait for that code to expire,

and it's gonna provide me with the next code.

And I'll enter that second code and click add MFA.

And it is as simple as that.

So now, if we head back to our dashboard,

I'm gonna refresh using this button.

And you should see

that the security recommendation relating to MFA

has now disappeared.

So the next time you sign into your Root account,

it's going to ask you to type in the latest code

that's generated by your MFA device.

So now, the next thing we're going to do

is create some identity and access management users.

So select users from the left hand side, add users,

and I'm gonna create a user called Faye.

There are two different ways to access AWS.

The first way is programmatically.

Optionally, we can provide the user access

to the AWS management console,

and we can also enable programmatic access.

And this enables access using the AWS API,

the command line interface,

and development of toolkits as well.

And this is how applications can access AWS,

and it's also how you, as an IAM user,

can access the AWS command line interface.

So I'm gonna select, I want to create an IAM user.

I'll stick with the default auto-generated password,

and users need to create a new password at next sign in.

So select next,

and now it's asking us to set permissions for our new user.

So we've got a choice of how we can actually

add these permissions.

So firstly, we can add a user to a group.

We can copy permissions from an existing user,

or we can attach permission policies directly.

But for now,

we're just gonna go ahead and create a new group.

So select create group.

My group name is Sysadmin,

and we're going to provide administrator access.

And this is gonna give full access to AWS services.

And if we select the plus sign here,

you can actually view the permissions policy.

So within this policy, the effect is to allow,

the action is any action,

and the resource is any resource within our AWS account.

So this is basically full access to AWS,

so make sure that that policy is selected

and create user group.

So now, we can add our user to this group.

So if you select the group here,

hit next,

we can review our selections,

scroll down, and create user.

After the user is created,

it's generated a console sign-in URL

that the user can use to sign into the console,

and here is the password.

And if you wanna see the auto-generated password,

you can just show it there.

So now, let's return to our user list,

and we're gonna create another user.

So select add users.

Our username is Robbie.

We'll give him console access,

create him as an IAM user.

Hit next,

we can add him to the existing group.

Hit next and create user.

Return to your user's list,

select continue, and select your user, Robbie.

And if we select groups,

we can see that Robbie is a member of the sysadmin group.

But let's say he moves to a different role.

So let's say he's moved to the development team,

and he's no longer a systems administrator.

Well, let's create a new group.

Select user groups,

create group.

Our new group is called Dev.

We can add Robbie to that group

and add some permissions.

Now the dev team is going to have access

to read files in S3.

So under policy,

I'm gonna search for S3,

and select S3 read only access,

create group.

Then I'm gonna select the group,

and we'll see that Robbie is a member of the dev group.

Now if we go back to Robbie,

we can see that he's a member of both groups,

but we wanna remove him from the sysadmin group.

So select that group and select remove.

And then still under Robbie, if you select permissions,

you can actually add permissions directly to our user.

So let's say that Robbie also needs DynamoDB access.

So let's select add permissions

and attach policies directly.

Under permission policies,

search for DynamoDB,

and select DynamoDB read only access,

then hit next and add permissions.

So now, under our user, Robbie,

we should see

that he's got DynamoDB read only access attached directly

and S3 read only access,

which is attached through the group that he's a member of,

so through the dev group.

And then, he's also got access to change his own password.

So now, using the menu on the left,

select account settings,

and under password policy,

this is where you can customize your password policy.

If you select edit,

you can see the default password policy.

And then, if you select custom,

this is where you can customize everything.

So you can change your minimum password length,

for instance, you could change it to 12 characters.

And then select some options around the password strength,

so you can require at least one uppercase, one lowercase,

one number, and one alphanumeric character.

You can also turn on password expiring,

so you can have your passwords by default

expiring within 90 days.

So whatever password policy

you have within your own organization,

you should be able to reflect that here within AWS as well.

Then once you're ready, you can save the changes.

Now, the last thing we're gonna do here

is we're gonna create a role.

So select roles from the left hand menu,

and IAM roles are a secure way

to grant permissions to entities that you trust.

So select create role and select your trusted entity,

and this could be an AWS service, like EC2 or Lambda.

So this would allow application code

running on an EC2 instance

to perform actions on AWS resources.

It could also be entities

in other AWS accounts that belong to you,

or even users that have been authenticated

by an external directory or using federation with SAML.

But right now, we're gonna create a role

allowing an EC2 instance to write files to S3.

So select AWS service, scroll down, and select EC2.

Click next, and then from the default policies,

we're gonna search for S3.

And we'll select S3 full access,

and this is gonna give

any EC2 instance with this role attached

full access to S3.

So now, I'm gonna go ahead and hit next.

We'll give our role a name,

scroll down,

and create role.

After we've created that role,

we'll be able to associate that role

with any EC2 instance in our account.

Well, that is all we're gonna do with IAM at the moment.

But you are going to be using it

quite a bit throughout the course,

so you will become very, very familiar

with using identity access management

and configuring users and roles.

So for the exam, when it comes to users,

I want you to think of end users,

so think about the people who are actually using

your AWS account and resources.

Groups are a collection of users

under one set of permissions,

and they're usually organized

by the kind of role that the users are doing,

like developers or sysadmins, et cetera.

We can also create roles,

and we can assign them to users, applications, and services,

to give them access to AWS resources.

Well, that's it for this lesson.

Any questions, please let me know.

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

Thank you.

[SPANISH]

Hola, gurús de la nube,

y bienvenidos a esta lección donde nos ensuciamos las manos

con gestión de identidad y acceso.

Y en primer lugar,

vamos a configurar la autenticación multifactor

en nuestra cuenta.

A continuación, crearemos nuestro primer usuario,

entonces vamos a crear un grupo.

Y finalmente, vamos a crear un rol también,

y luego terminaremos con mis consejos para el examen.

Ahora, necesitará usar su propia cuenta de AWS

para completar esta lección

porque no se puede realizar la autenticación multifactor

usando el patio de juegos en la nube A Cloud Guru

o entorno de caja de arena.

Únase a mí en su propia cuenta de AWS.

Desde la consola de AWS,

buscar IAM,

y debería ver un tablero similar a este.

Y recuerde, estamos haciendo esto en nuestra propia cuenta de AWS.

Ahora, como puedes ver,

Tengo algunas recomendaciones de seguridad aquí,

porque aún no he configurado

autenticación multifactor.

Así que estoy recibiendo esta alerta de seguridad.

Así que sigamos adelante y configuremos la autenticación multifactor.

Seleccione agregar MFA,

y necesitamos asignar un nuevo dispositivo MFA.

Así que seleccione asignar MFA.

le daré un nombre,

mi-MFA,

y desplácese hacia abajo para seleccionar su dispositivo MFA.

Y voy a usar un dispositivo MFA virtual

instalado en mi teléfono inteligente.

Así que seleccione la primera opción,

luego baja al fondo y presiona siguiente.

Y aquí es donde vamos a configurar nuestro dispositivo.

En primer lugar, debe instalar una aplicación compatible,

como Google Authenticator.

Y si seleccionas este enlace,

le dará una lista de aplicaciones compatibles.

Y si te desplazas hacia abajo,

aquí están las aplicaciones de autenticación virtual que son compatibles,

y hay algunos para Android y otros para iOS.

Pero me gusta usar Google Authenticator,

así que ese es el que les voy a mostrar.

De vuelta en la consola de IAM, desplácese hacia abajo hasta el paso dos,

y vamos a crear un código QR.

Así que selecciona mostrar código QR,

entonces lo siguiente que hacemos es

abra nuestra aplicación de autenticación en nuestro teléfono inteligente,

seleccione el botón Agregar, seleccione escanear un código QR,

escanea tu código.

Y después de escanear el código QR en su teléfono,

Google Authenticator comenzará a generar algunos códigos MFA,

y deberá completar dos códigos consecutivos

que son generados por el dispositivo MFA.

Así que aquí está mi primera.

Entonces voy a esperar a que caduque ese código,

y me va a proporcionar el siguiente código.

E ingresaré ese segundo código y haré clic en agregar MFA.

Y es tan simple como eso.

Ahora, si volvemos a nuestro tablero,

Voy a actualizar usando este botón.

y deberías ver

que la recomendación de seguridad relativa a MFA

ahora ha desaparecido.

Entonces, la próxima vez que inicie sesión en su cuenta raíz,

le pedirá que escriba el último código

que es generado por su dispositivo MFA.

Así que ahora, lo siguiente que vamos a hacer

es crear algunos usuarios de administración de identidad y acceso.

Seleccione usuarios del lado izquierdo, agregue usuarios,

y voy a crear un usuario llamado Faye.

Hay dos formas diferentes de acceder a AWS.

La primera forma es programáticamente.

Opcionalmente, podemos proporcionar al usuario acceso

a la consola de administración de AWS,

y también podemos habilitar el acceso programático.

Y esto permite el acceso usando la API de AWS,

la interfaz de línea de comandos,

y el desarrollo de juegos de herramientas también.

Y así es como las aplicaciones pueden acceder a AWS,

y también es cómo usted, como usuario de IAM,

puede acceder a la interfaz de línea de comandos de AWS.

Voy a seleccionar, quiero crear un usuario de IAM.

Me quedaré con la contraseña predeterminada generada automáticamente,

y los usuarios deben crear una nueva contraseña la próxima vez que inicien sesión.

Así que seleccione siguiente,

y ahora nos pide que establezcamos permisos para nuestro nuevo usuario.

Así que tenemos la opción de cómo podemos realmente

agregar estos permisos.

Entonces, en primer lugar, podemos agregar un usuario a un grupo.

Podemos copiar permisos de un usuario existente,

o podemos adjuntar políticas de permisos directamente.

Pero por ahora,

vamos a seguir adelante y crear un nuevo grupo.

Así que seleccione crear grupo.

El nombre de mi grupo es Sysadmin,

y vamos a proporcionar acceso de administrador.

Y esto dará acceso completo a los servicios de AWS.

Y si seleccionamos el signo más aquí,

en realidad puede ver la política de permisos.

Entonces, dentro de esta política, el efecto es permitir,

la acción es cualquier acción,

y el recurso es cualquier recurso dentro de nuestra cuenta de AWS.

Así que esto es básicamente acceso total a AWS,

así que asegúrese de que esa política esté seleccionada

y crear un grupo de usuarios.

Ahora, podemos agregar nuestro usuario a este grupo.

Entonces, si selecciona el grupo aquí,

golpear siguiente,

podemos revisar nuestras selecciones,

desplácese hacia abajo y cree un usuario.

Una vez creado el usuario,

ha generado una URL de inicio de sesión en la consola

que el usuario puede usar para iniciar sesión en la consola,

y aquí está la contraseña.

Y si quieres ver la contraseña generada automáticamente,

Puedes mostrarlo allí.

Así que ahora, volvamos a nuestra lista de usuarios,

y vamos a crear otro usuario.

Así que seleccione agregar usuarios.

Nuestro nombre de usuario es Robbie.

Le daremos acceso a la consola,

créelo como usuario de IAM.

Pulse siguiente,

podemos agregarlo al grupo existente.

Presiona siguiente y crea un usuario.

Regresa a tu lista de usuarios,

seleccione continuar y seleccione su usuario, Robbie.

Y si seleccionamos grupos,

podemos ver que Robbie es miembro del grupo sysadmin.

Pero digamos que cambia de rol.

Entonces, digamos que se mudó al equipo de desarrollo,

y ya no es administrador de sistemas.

Bueno, vamos a crear un nuevo grupo.

Seleccionar grupos de usuarios,

crea un grupo.

Nuestro nuevo grupo se llama Dev.

Podemos agregar a Robbie a ese grupo.

y agregar algunos permisos.

Ahora el equipo de desarrollo tendrá acceso

para leer archivos en S3.

Así que bajo la política,

Voy a buscar S3,

y seleccione S3 acceso de solo lectura,

crea un grupo.

Luego voy a seleccionar el grupo,

y veremos que Robbie es miembro del grupo de desarrollo.

Ahora, si volvemos a Robbie,

podemos ver que es miembro de ambos grupos,

pero queremos eliminarlo del grupo de administradores de sistemas.

Así que seleccione ese grupo y seleccione eliminar.

Y aún bajo Robbie, si selecciona permisos,

en realidad puede agregar permisos directamente a nuestro usuario.

Entonces, digamos que Robbie también necesita acceso a DynamoDB.

Así que seleccionemos agregar permisos

y adjunte políticas directamente.

Bajo las políticas de permisos,

buscar DynamoDB,

y seleccione el acceso de solo lectura de DynamoDB,

luego presione siguiente y agregue permisos.

Así que ahora, bajo nuestro usuario, Robbie,

deberíamos ver

que tiene acceso de solo lectura de DynamoDB adjunto directamente

y S3 acceso de solo lectura,

que está unido a través del grupo del que es miembro,

así que a través del grupo de desarrollo.

Y luego, también tiene acceso para cambiar su propia contraseña.

Así que ahora, usando el menú de la izquierda,

seleccione la configuración de la cuenta,

y bajo la política de contraseñas,

aquí es donde puede personalizar su política de contraseñas.

Si selecciona editar,

puede ver la política de contraseña predeterminada.

Y luego, si selecciona personalizado,

aquí es donde puedes personalizar todo.

Para que pueda cambiar la longitud mínima de su contraseña,

por ejemplo, podría cambiarlo a 12 caracteres.

Y luego seleccione algunas opciones en torno a la seguridad de la contraseña,

por lo que puede requerir al menos una mayúscula, una minúscula,

un número y un carácter alfanumérico.

También puede activar la caducidad de la contraseña,

para que puedas tener tus contraseñas por defecto

con vencimiento a los 90 días.

Sea cual sea la política de contraseñas

usted tiene dentro de su propia organización,

debería poder reflejar eso aquí dentro de AWS también.

Luego, una vez que esté listo, puede guardar los cambios.

Ahora, lo último que haremos aquí

es que vamos a crear un papel.

Así que selecciona roles en el menú de la izquierda,

y los roles de IAM son una forma segura

para conceder permisos a las entidades en las que confía.

Así que seleccione crear rol y seleccione su entidad de confianza,

y este podría ser un servicio de AWS, como EC2 o Lambda.

Esto permitiría que el código de la aplicación

ejecutándose en una instancia EC2

para realizar acciones en los recursos de AWS.

También pueden ser entidades

en otras cuentas de AWS que le pertenecen,

o incluso usuarios que han sido autenticados

por un directorio externo o mediante federación con SAML.

Pero ahora mismo, vamos a crear un rol

permitiendo que una instancia EC2 escriba archivos en S3.

Así que seleccione el servicio de AWS, desplácese hacia abajo y seleccione EC2.

Haga clic en siguiente y luego en las políticas predeterminadas,

vamos a buscar S3.

Y seleccionaremos S3 full access,

y esto va a dar

cualquier instancia EC2 con este rol adjunto

acceso completo a S3.

Así que ahora, voy a seguir adelante y pulsar siguiente.

Le daremos un nombre a nuestro rol,

desplazarse hacia abajo,

y crear rol.

Después de haber creado ese rol,

podremos asociar ese rol

con cualquier instancia EC2 en nuestra cuenta.

Bueno, eso es todo lo que haremos con IAM por el momento.

Pero lo vas a usar

bastante a lo largo del curso,

así te volverás muy, muy familiar

con el uso de la gestión de acceso de identidad

y configuración de usuarios y roles.

Entonces, para el examen, cuando se trata de usuarios,

Quiero que piense en los usuarios finales,

así que piensa en las personas que realmente están usando

su cuenta y recursos de AWS.

Los grupos son una colección de usuarios.

bajo un conjunto de permisos,

y por lo general están organizados

por el tipo de rol que los usuarios están haciendo,

como desarrolladores o administradores de sistemas, etcétera.

También podemos crear roles,

y podemos asignarlos a usuarios, aplicaciones y servicios,

para darles acceso a los recursos de AWS.

Bueno, eso es todo por esta lección.

Para cualquier duda, por favor hágamelo saber.

De lo contrario, siéntete libre de pasar al siguiente.

Gracias.