[ENGLISH]

Hello Cloud Gurus and welcome to this lecture.

And this lecture is going to be a summary

of identity access management 101.

So we're going to cover off everything that we've learnt

and also are going to be telling you some of the

exam tips that we have for this section as well

so let's get started.

So what have we learned so far,

identity access management

consists of users, groups, and roles.

And if you remember the lab,

we created a couple of users,

we also created a couple of groups,

and we use those groups to apply

permissions policies to those users.

And we also applied policies directly to the users.

And we have an example of a

policy document here written in JSON.

And the document is written as a series of key value pairs.

So under the version we then have the statement,

the effect is allow,

and the action is to allow all actions across all resources.

So this policy document would give full access

to everything within AWS.

And then finally, in our lab we also created a role,

and we created a role which can be

used by an EC2 instance to allow access

to read and write files within S3.

Identity access management is universal.

It doesn't apply to regions at this time.

So what does that mean?

It just means that identity access management is global.

And anything you set up within IAM

can be viewed and utilized by any region.

The root account is simply the account you

created when you first set up your AWS account.

So that's the email address that you used

when you first registered your account with AWS.

And it has complete admin access.

So of course for day-to-day activities

we shouldn't be using the root account,

instead we should be creating

identity access management users,

and making sure those users

have the permissions and privileges

they need to do their jobs.

New users have no permissions at all

when they're first created.

So we need to explicitly add the permissions

they needed to do their role.

For example, in the lab

we added permissions for S3 and Glacier

for our HR user, to enable them to

access those AWS services.

New users are assigned the access key ID

and secret access key when they're very first created.

And these are not the same as a username and password,

you can't use the access key

and secret access key to log in to the AWS console

but you can use it to access AWS via the API

and command line interface from your local desktop.

And you only get to view

and download the file containing your access key

and secret access key one time

when you initially create them.

And after that, you can still view the access key

but you cannot view the secret access key again.

So if you lose your secret access key,

you are going to need to regenerate new Keys.

So do make sure that you save your secret access key

in a safe location.

Always set up Multi-factor Authentication or MFA

on your root account.

And that's another thing that we did in the lab.

And finally you can create and customize your own

password rotation policies.

So that's the end of this section.

Well done for completing the section.

If you have any questions please let me know,

otherwise please join us in the next lecture.

Thank you.

[SPANISH]

Hola Cloud Gurus y bienvenidos a esta conferencia.

Y esta conferencia va a ser un resumen.

de gestión de acceso a la identidad 101.

Así que vamos a cubrir todo lo que hemos aprendido.

y también les estaré contando algunas de las

de examen que tenemos para esta sección también

así que empecemos.

Entonces, ¿qué hemos aprendido hasta ahora?

gestión de acceso de identidad

consta de usuarios, grupos y roles.

Y si recuerdas el laboratorio,

creamos un par de usuarios,

creamos un par de grupos,

y usamos esos grupos para aplicar

de permisos a esos usuarios.

Y también aplicamos políticas directamente a los usuarios.

Y tenemos un ejemplo de un

de política aquí escrito en JSON.

Y el documento está escrito como una serie de pares de valores clave.

Entonces, bajo la versión, tenemos la declaración,

el efecto es permitir,

y la acción es permitir todas las acciones en todos los recursos.

Así que este documento de política daría acceso completo

a todo dentro de AWS.

Y finalmente, en nuestro laboratorio también creamos un rol,

y creamos un rol que puede ser

utilizado por una instancia EC2 para permitir el acceso

para leer y escribir archivos dentro de S3.

La gestión del acceso a la identidad es universal.

No se aplica a las regiones en este momento.

¿Entonces que significa eso?

Simplemente significa que la gestión del acceso a la identidad es global.

Y cualquier cosa que configure dentro de IAM

puede ser visto y utilizado por cualquier región.

La cuenta raíz es simplemente la cuenta que

creado cuando configuró su cuenta de AWS por primera vez.

Esa es la dirección de correo electrónico que usaste.

cuando registró por primera vez su cuenta con AWS.

Y tiene acceso de administrador completo.

Así que, por supuesto, para las actividades del día a día.

deberíamos estar usando la cuenta raíz,

en su lugar, deberíamos estar creando

usuarios de administración de acceso de identidad ,

y asegurarse de que esos usuarios

tener los permisos y privilegios

necesitan hacer su trabajo.

Los nuevos usuarios no tienen ningún permiso

cuando se crean por primera vez.

Entonces necesitamos agregar explícitamente los permisos

necesitaban hacer su papel.

Por ejemplo, en el laboratorio.

agregamos permisos para S3 y Glacier

para nuestro usuario de recursos humanos, para permitirles

acceder a esos servicios de AWS.

A los nuevos usuarios se les asigna el ID de clave de acceso

y clave de acceso secreta cuando se crean por primera vez.

Y estos no son lo mismo que un nombre de usuario y contraseña,

puedes usar la clave de acceso

y clave de acceso secreta para iniciar sesión en la consola de AWS

pero puede usarlo para acceder a AWS a través de la API

y la interfaz de línea de comandos desde su escritorio local.

Y solo puedes ver

y descargue el archivo que contiene su clave de acceso

y clave de acceso secreta una vez

cuando los crea inicialmente.

Y después de eso, aún puede ver la clave de acceso

pero no puede volver a ver la clave de acceso secreta.

Entonces, si pierde su clave de acceso secreta,

vas a necesitar regenerar nuevas claves.

Así que asegúrese de guardar su clave de acceso secreta

en un lugar seguro.

Configure siempre la autenticación multifactor o MFA

en su cuenta raíz.

Y esa es otra cosa que hicimos en el laboratorio.

Y finalmente puedes crear y personalizar tu propio

de contraseñas .

Así que ese es el final de esta sección.

Bien hecho por completar la sección.

Si tiene alguna pregunta, por favor hágamelo saber,

de lo contrario , únase a nosotros en la próxima conferencia.

Gracias.