[ENGLISH]

Hello, Cloud Gurus and welcome to this lecture.

And this lecture is called identity access management 101.

And IAM is the best place to start with AWS because it's all

about setting up your users and granting those users access to the

AWS console. So what is IAM? Well,

essentially,

IAM allows you to manage users and also manage their level of

access to the AWS console.

And it's really important to understand IAM and how it works,

both for the exam and for administrating a company's AWS account in

real life. So what does IAM give you?

It gives you centralized control over your AWS account.

It also gives you shared access to your AWS account.

It gives you granular permissions.

So this means you can enable different levels of access to different users

within your organization. It enables identity federation.

So this means that it can enable users to log in using credentials stored in

active directory, Facebook, or LinkedIn.

It allows multifactor authentication.

And this is where a user is granted access only after successfully completing

multiple independent authentication mechanisms.

So for example,

providing a username and password as one authentication mechanism,

and then providing a software token.

So that could be via a token generator like Google authenticator as

the second authentication mechanism.

It also provides temporary access for users or devices and services

as necessary. So for example,

if you developed a web or mobile phone application,

you can configure identity access management to enable users to have temporary

access to AWS resources within your account.

For example,

to enable access to store or retrieve data located in an S3

bucket or within a DynamoDB database.

It allows you to set up your own password rotation policy.

It integrates with many different AWS services and it

supports PCI DSS compliance for any applications

associated with the payment card industry.

So there are some core concepts that you need to understand before going into

the exam. So first of all, we have users,

so this is the end users and just think people.

So these are the people logging in to the AWS console and also

interacting with AWS by running API commands.

We then have groups which are collections of users grouped together with a

common set of permissions. So for example,

your marketing team might need access to read and write certain files

stored in an S3 bucket, and that might be logos or images,

et cetera.

And they're going to need a specific set of permissions to allow them to do

this.

So it makes sense to create a group with the required permissions.

And then all you need to do is add the relevant users into that group.

And they will all have permissions to read your S3 bucket. And similarly,

you might have a database administrations team and they need to create DynamoDB

tables and run queries on the database. So in that case,

you can create a group with the relevant permissions for DynamoDB,

and then add all of your database admins into that group.

And we also have roles.

Now you can create roles and then assign them to AWS resources.

So a role is used to define a set of permissions, for example,

S3 bucket access.

And then that role can be assumed by either users or AWS services

such as EC2.

So you might have an EC2 instance which needs to query a database or access

files in S3, and you can configure that using a role. And finally,

we have policies and a policy is a document that defines either one or

more permissions. And a policy can be attached to either a user,

a group, or a role. And when we attach a policy, the user, group,

or role will then have the permissions defined within that policy.

And it's possible for a user, group, and role to all share the same policy.

So the quickest way to learn identity access management is actually to start

using it. And that's what we're going to do right now. So if you've got time,

please join me in the next lecture, which is an identity access management lab.

Thank you.

[SPANISH]

Hola, Cloud Gurus y bienvenidos a esta conferencia.

Y esta conferencia se llama administración de acceso a la identidad 101.

Y IAM es el mejor lugar para comenzar con AWS porque es todo

sobre la configuración de sus usuarios y la concesión de acceso a esos usuarios a la

Consola AWS. Entonces, ¿qué es IAM? Bien,

esencialmente ,

IAM le permite administrar usuarios y también administrar su nivel de

acceso a la consola de AWS.

Y es muy importante entender IAM y cómo funciona,

tanto para el examen como para administrar la cuenta de AWS de una empresa en

la vida real Entonces, ¿qué te da IAM?

Le brinda control centralizado sobre su cuenta de AWS.

También le brinda acceso compartido a su cuenta de AWS.

Te da permisos granulares.

Entonces, esto significa que puede habilitar diferentes niveles de acceso para diferentes usuarios

dentro de su organización. Habilita la federación de identidades.

Esto significa que puede permitir que los usuarios inicien sesión con las credenciales almacenadas en

activo , Facebook o LinkedIn.

Permite autenticación multifactor.

Y aquí es donde se otorga acceso a un usuario solo después de completar con éxito

Múltiples mecanismos de autenticación independientes.

Así por ejemplo,

proporcionar un nombre de usuario y una contraseña como un mecanismo de autenticación,

y luego proporcionar un token de software.

Entonces eso podría ser a través de un generador de tokens como el autenticador de Google como

el segundo mecanismo de autenticación.

También proporciona acceso temporal para usuarios o dispositivos y servicios.

según sea necesario Así por ejemplo,

si desarrollaste una aplicación web o de teléfono móvil,

puede configurar la administración de acceso de identidad para permitir que los usuarios tengan acceso temporal

acceso a los recursos de AWS dentro de su cuenta.

Por ejemplo,

para habilitar el acceso para almacenar o recuperar datos ubicados en un S3

depósito o dentro de una base de datos de DynamoDB .

Le permite configurar su propia política de rotación de contraseñas.

Se integra con muchos servicios diferentes de AWS y

admite el cumplimiento de PCI DSS para cualquier aplicación

relacionados con la industria de las tarjetas de pago.

Entonces, hay algunos conceptos básicos que debe comprender antes de entrar en

el examen En primer lugar, tenemos usuarios,

así que estos son los usuarios finales y solo piensan en personas.

Estas son las personas que inician sesión en la consola de AWS y también

interactuando con AWS mediante la ejecución de comandos API.

Entonces tenemos grupos que son colecciones de usuarios agrupados junto con un

común de permisos. Así por ejemplo,

su equipo de marketing podría necesitar acceso para leer y escribir ciertos archivos

almacenados en un cubo S3, y que pueden ser logotipos o imágenes,

etcétera .

Y van a necesitar un conjunto específico de permisos para permitirles hacer

esto \_

Por lo tanto, tiene sentido crear un grupo con los permisos necesarios.

Y luego todo lo que necesita hacer es agregar los usuarios relevantes a ese grupo.

Y todos tendrán permisos para leer su depósito S3. Y de manera similar,

tenga un equipo de administradores de bases de datos y necesiten crear DynamoDB

tablas y ejecutar consultas en la base de datos. Así que en ese caso,

puede crear un grupo con los permisos pertinentes para DynamoDB ,

y luego agregue todos los administradores de su base de datos a ese grupo.

Y también tenemos papeles.

Ahora puede crear roles y luego asignarlos a los recursos de AWS.

Entonces, un rol se usa para definir un conjunto de permisos, por ejemplo,

Acceso al depósito S3.

Y luego ese rol puede ser asumido por los usuarios o los servicios de AWS.

como EC2.

Por lo tanto, es posible que tenga una instancia EC2 que necesite consultar una base de datos o acceder

archivos en S3, y puede configurar eso usando un rol. Y finalmente,

tenemos políticas y una política es un documento que define uno o

más permisos. Y una política se puede adjuntar a un usuario,

un grupo o un rol. Y cuando adjuntamos una política, el usuario, grupo,

o el rol tendrá los permisos definidos dentro de esa política.

Y es posible que un usuario, grupo y rol compartan la misma política.

Entonces, la forma más rápida de aprender a administrar el acceso a la identidad es comenzar

usándolo \_ Y eso es lo que vamos a hacer ahora mismo. Así que si tienes tiempo,

Únase a mí en la próxima conferencia, que es un laboratorio de administración de acceso de identidad.

Gracias.