[ENGLISH]

Hello Cloud Gurus and welcome to this lecture.

And this lecture

is all about Inline, Managed and Custom policies

within identity access management.

So let's get started.

Now identity access management is used

to define user access permissions within AWS

and we've used IAM a lot throughout this course.

Now there are three different types

of IAM policies available.

Firstly managed policies,

then customer managed policies and finally Inline policies.

So let's take a look at those three different policies

in a little bit more detail.

Now a managed policy is an IAM policy

which is created and administered by AWS.

And they provide managed policies

for really common use cases based on job function.

So for example DynamoDBFullAccess,

CodeCommitPowerUser, EC2ReadOnlyAccess, et cetera.

And we've used AWS managed policies like this

many times throughout this course.

So for example

when we've created an EC2 instance

that needs to create or query a DynamoDB table,

we've used that DynamoDBFullAccess managed policy

in combination with a service role

to give our EC2 instance access to the DynamoDB tables.

And these AWS provided policies allow you

to assign appropriate permissions

to your users, groups and roles

without having to write the policy yourself.

On the policies are all written in Jason

they're all fairly complex and comprehensive

so it just takes away that heavy lifting

of creating a policy yourself.

And a single managed policy can be attached

to multiple users, groups or roles

within the same AWS account

and across different accounts.

But there's one important thing to know

about the managed policies is that you cannot change

the permissions defined in an AWS managed policy.

Moving on to customer managed policies.

And a customer managed policy

is a standalone policy that you create

and administer inside your own AWS account.

You can attach this policy

to multiple users, groups and roles

but only within your own account.

And to create a customer managed policy,

you can take a copy of an existing AWS managed policy

just copy the Jason code and customize it

to fit the requirements of your organization.

And this is recommended for use cases

where existing AWS managed policies

don't quite meet the needs of your environment.

Finally we have Inline policies.

And an Inline policy is an identity access management policy

which is actually embedded

within the user, group or role to which it applies.

And there's a strict one-to-one relationship

between the entity and the policy.

That means you cannot attach an Inline policy

to multiple users, groups, or roles

and when you delete the user, group or role

in which the Inline policy is embedded,

the policy will also be deleted.

Now, in most cases

AWS recommends using managed policies over Inline policies.

However they are useful

when you want to be sure that the permissions in a policy

are not inadvertently assigned

to another user, group or role

than the one for which they are intended.

For example, if you're creating a policy

which must only ever be attached

to a single user, group or role for security

or technical reasons.

And if you come into the AWS console

you can take a look at the different types of policy

that are available.

So scroll down to identity access management,

click on policies and you can filter based on policy type.

And it's showing me either customer managed or AWS managed.

So first let's take a look at my customer managed policies

and these are all the different policies

that I have created myself.

And if you go into these policies

you can actually edit the policy

and you can actually change the Jason code

that makes up the policy.

So I'm just gonna click cancel,

go back to my policies and click on AWS managed.

And you can see

they provide lots of different managed policies

for various different types of access.

So depending on whether you need a read only or full access

or down to administrative access

and they give you lots of different policies

for all different types of services.

And the interesting thing about these policies

is if I select one it's not going to let me edit it.

So I cannot change this Jason code

and that's the important thing to remember about

a managed policy.

It does not give you the option to edit.

And in fact it says down here on the bottom right-hand side

it says read only.

So let's go back to my dashboard

and I don't actually have any Inline policies at the moment

but let's go ahead and create one.

So if I go to my user

and because it's an Inline policy

and it is associated with either a user, group or role

you have to be in the user, group or role

in order to actually create the policy.

So if you go into a user

you will see this option here to add an Inline policy.

So I'm just gonna choose a service

and I'm gonna add a policy for Athena

and I'm gonna to add right access for Athena

click on review, give it a name

and click on create policy.

And there is my Inline policy

and it will show here as being an Inline policy.

And if I wanted to for example create a new user

and I'm gonna call my user Rob,

I'm gonna give Rob programmatic access, next

and I'm gonna try and add that Inline policy.

And if I try to search for that policy, it doesn't come up.

Only my customer managed policies come up.

I can't filter based on Inline policies.

I've only have the choice of either the customer managed

or the AWS managed.

So let's take a look at our exam tips

for the three different types of IAM policy.

Just remember the AWS managed policy

is the AWS default policy

like DynamoDBFullAccess, et cetera.

The customer managed policy is one managed by you,

created by you and managed by you

and you can apply it to multiple users, groups, or roles.

And the Inline policy is managed by you

but it's embedded in a single user, group or role.

And there is a one-to-one relationship

between the Inline policy and the user, group or role

to which they are embedded.

And finally in most cases

AWS recommends using managed policies over Inline policies.

Well, that's the end of this lecture.

If you have any questions, please let me know.

If not, feel free to move on to the next lecture.

Thank you.

[SPANISH]

Hola Cloud Gurus y bienvenidos a esta conferencia.

Y esta conferencia

se trata de políticas en línea, administradas y personalizadas

dentro de la gestión de acceso a la identidad.

Entonces empecemos.

Ahora se utiliza la gestión de acceso de identidad

para definir los permisos de acceso de los usuarios dentro de AWS

y hemos usado mucho IAM a lo largo de este curso.

Ahora hay tres tipos diferentes.

de políticas de IAM disponibles.

Políticas gestionadas en primer lugar,

luego las políticas administradas por el cliente y finalmente las políticas en línea.

Así que echemos un vistazo a esas tres políticas diferentes.

con un poco más de detalle.

Ahora una política administrada es una política de IAM

que es creado y administrado por AWS.

Y proporcionan políticas administradas

para casos de uso muy comunes basados en la función del trabajo.

Entonces, por ejemplo , DynamoDBFullAccess ,

CodeCommitPowerUser , EC2ReadOnlyAccess, etcétera.

Y hemos usado políticas administradas por AWS como esta

muchas veces a lo largo de este curso.

Así por ejemplo

cuando hemos creado una instancia EC2

que necesita crear o consultar una tabla de DynamoDB ,

hemos usado esa política administrada de DynamoDBFullAccess

en combinación con un rol de servicio

para dar acceso a nuestra instancia EC2 a las tablas de DynamoDB .

Y estas políticas proporcionadas por AWS le permiten

para asignar los permisos apropiados

a sus usuarios, grupos y roles

sin tener que redactar la póliza usted mismo.

En las políticas están todas escritas en Jason

son bastante complejos y completos

así que solo quita ese trabajo pesado

de crear una póliza usted mismo.

Y se puede adjuntar una sola política administrada

a múltiples usuarios, grupos o roles

dentro de la misma cuenta de AWS

y a través de diferentes cuentas.

Pero hay una cosa importante que debes saber

sobre las políticas administradas es que no puede cambiar

los permisos definidos en una política administrada por AWS.

Pasando a las políticas administradas por el cliente.

Y una póliza administrada por el cliente

es una política independiente que usted crea

y administre dentro de su propia cuenta de AWS.

Puede adjuntar esta política

a múltiples usuarios, grupos y roles

pero sólo dentro de su propia cuenta.

Y para crear una política administrada por el cliente,

puede tomar una copia de una política administrada por AWS existente

simplemente copie el código de Jason y personalícelo

para adaptarse a los requisitos de su organización.

Y esto se recomienda para casos de uso.

donde las políticas administradas por AWS existentes

no satisfacen del todo las necesidades de su entorno.

Finalmente tenemos políticas en línea.

Y una política en línea es una política de gestión de acceso a la identidad.

que en realidad está incrustado

dentro del usuario, grupo o rol al que se aplica.

Y hay una estricta relación de uno a uno

entre la entidad y la póliza.

Eso significa que no puede adjuntar una política en línea

a múltiples usuarios, grupos o roles

y cuando elimina el usuario, grupo o rol

en el que está incrustada la política Inline,

la política también se eliminará.

Ahora, en la mayoría de los casos

AWS recomienda utilizar políticas administradas en lugar de políticas en línea.

Sin embargo, son útiles

cuando quiere estar seguro de que los permisos en una política

se asignan inadvertidamente

a otro usuario, grupo o rol

que aquél para el que están destinados.

Por ejemplo, si está creando una política

que sólo debe adjuntarse

a un solo usuario, grupo o rol por seguridad

o razones técnicas.

Y si entras en la consola de AWS

puedes echar un vistazo a los diferentes tipos de póliza

que están disponibles.

Desplácese hacia abajo hasta la gestión de acceso a la identidad,

haga clic en políticas y puede filtrar según el tipo de política.

Y me muestra administrado por el cliente o administrado por AWS.

Entonces, primero echemos un vistazo a mis políticas administradas por el cliente

y estas son todas las diferentes políticas

que yo mismo he creado.

Y si entras en estas políticas

puedes editar la política

y puedes cambiar el código de Jason

que compone la política.

Así que voy a hacer clic en cancelar,

regrese a mis políticas y haga clic en AWS administrado.

y puedes ver

proporcionan muchas políticas administradas diferentes

para diferentes tipos de acceso.

Entonces, dependiendo de si necesita un acceso de solo lectura o completo

o hacia abajo para el acceso administrativo

y te dan muchas políticas diferentes

para todo tipo de servicios.

Y lo interesante de estas políticas

es que si selecciono uno no me va a dejar editarlo.

Entonces no puedo cambiar este código de Jason

y eso es lo importante a recordar acerca de

una política administrada.

No te da la opción de editar.

Y de hecho dice aquí abajo en la parte inferior derecha

dice solo lectura.

Así que volvamos a mi tablero

y en realidad no tengo ninguna política en línea en este momento

pero sigamos adelante y creemos uno.

Así que si voy a mi usuario

y porque es una política en línea

y está asociado con un usuario, grupo o rol

tienes que estar en el usuario, grupo o rol

para crear realmente la política.

Así que si entras en un usuario

verá esta opción aquí para agregar una política en línea.

Así que voy a elegir un servicio

y voy a agregar una política para Athena

y voy a agregar acceso correcto para Athena

haz clic en revisar, dale un nombre

y haga clic en crear política.

Y ahí está mi política en línea

y se mostrará aquí como una política en línea.

Y si quisiera por ejemplo crear un nuevo usuario

y voy a llamar a mi usuario Rob,

Voy a darle a Rob acceso programático, a continuación

y voy a tratar de agregar esa política en línea.

Y si trato de buscar esa política, no aparece.

Solo aparecen mis políticas administradas por el cliente.

No puedo filtrar según las políticas en línea.

Solo tengo la opción de administrar el cliente

o el administrado por AWS.

Así que echemos un vistazo a nuestros consejos para el examen

para los tres tipos diferentes de políticas de IAM.

Solo recuerde la política administrada por AWS

es la política predeterminada de AWS

como DynamoDBFullAccess , etcétera.

La política gestionada por el cliente es una gestionada por usted,

creado por usted y administrado por usted

y puede aplicarlo a múltiples usuarios, grupos o roles.

Y la póliza Inline la administra usted

pero está incrustado en un solo usuario, grupo o rol.

Y hay una relación de uno a uno.

entre la política en línea y el usuario, grupo o rol

al que están incrustados.

Y finalmente en la mayoría de los casos

AWS recomienda utilizar políticas administradas en lugar de políticas en línea.

Bueno, ese es el final de esta conferencia.

Si tiene alguna pregunta, por favor hágamelo saber.

Si no, siéntase libre de pasar a la siguiente lección.

Gracias.