[ENGLISH]

Hello, Cloud Gurus,

and welcome to this lecture.

Where we're going to be talking about

DynamoDB Access Control.

So how do we control access to DynamoDB tables?

Well, as you've probably guessed,

we use identity and access management.

So authentication and access control

is managed using AWS IAM.

And you can create identity and access management users

within your AWS account with specific permissions

to access, and read, and write,

and create DynamoDB tables.

And you can also create

identity access management roles,

enabling temporary access to DynamoDB.

But what about restricting user access?

Well, you can also use a special

identity access management condition

to restrict user access to only their own records.

So only the data which relates to them,

rather than the entire table.

So how do we do that?

Well, imagine a mobile gaming application

with millions of players,

and the users need to access their own top score

for each game that they're playing,

but access must be restricted to ensure

that they cannot view anyone else's data.

Well, this can be done by adding a condition

to an identity access management policy

to allow access only to items

where the partition key value matches the user ID.

So let's take a look at an example,

identity access management policy,

which does exactly that.

So here is our example policy,

and at the top here,

we've got our statement identifier.

Under actions, this defines the actions

which the policy is going to allow.

And then it's this condition section,

which is the important bit.

So this section is what allows the users to access

only the items where the partition key value

matches their own user ID.

And it's this DynamoDB leading keys condition parameter,

which is the important bit.

And this means that the partition key value

must match the user's ID,

so that the user can only access the data

which belongs to them, and they won't be able

to access anyone else's data.

And then onto the DynamoDB attributes section.

This defines the attributes which the policy applies to.

So onto our exam tips.

Just for you remember, you can configure

fine-grained access control using

identity and access management.

And we use this IAM condition parameter

called DynamoDB leading keys

to allow users to access only the items

where the partition key value matches their user ID.

And when we use this in a condition statement

within an identity access management policy,

we can restrict user access to only the items

which relate to a user ID.

And it means they won't be able to see

anybody else's data within that table.

So that is the end of this lecture.

If you have any questions, please let me know.

Otherwise, I'll see you in the next lecture.

Thank you.

[SPANISH]

Hola, gurús de la nube,

y bienvenidos a esta conferencia.

de donde vamos a estar hablando

Control de acceso de DynamoDB .

Entonces, ¿cómo controlamos el acceso a las tablas de DynamoDB ?

Bueno, como probablemente habrás adivinado,

utilizamos gestión de identidad y acceso.

Entonces autenticación y control de acceso

se administra mediante AWS IAM.

Y puede crear usuarios de administración de acceso e identidad

dentro de su cuenta de AWS con permisos específicos

para acceder, leer y escribir,

y crear tablas de DynamoDB .

Y también puedes crear

funciones de gestión de acceso a la identidad ,

habilitando el acceso temporal a DynamoDB .

Pero, ¿qué hay de restringir el acceso de los usuarios?

Bueno, también puedes usar un especial

condición de gestión de acceso de identidad

para restringir el acceso de los usuarios solo a sus propios registros.

Entonces, solo los datos que se relacionan con ellos,

en lugar de toda la tabla.

¿Entonces cómo hacemos eso?

Pues imagina una aplicación de juegos para móvil

con millones de jugadores,

y los usuarios necesitan acceder a su propia puntuación máxima

para cada juego que están jugando,

pero el acceso debe ser restringido para asegurar

que no pueden ver los datos de nadie más.

Bueno, esto se puede hacer agregando una condición.

a una política de gestión de acceso a la identidad

para permitir el acceso solo a los elementos

donde el valor de la clave de partición coincide con el ID de usuario.

Así que echemos un vistazo a un ejemplo,

a la identidad ,

que hace exactamente eso.

Así que aquí está nuestra política de ejemplo,

y en la parte superior aquí,

tenemos nuestro identificador de declaración.

En acciones, esto define las acciones

que la política va a permitir.

Y luego está esta sección de condiciones,

que es lo importante.

Así que esta sección es lo que permite a los usuarios acceder

solo los elementos donde el valor de la clave de partición

coincide con su propia ID de usuario.

Y es este parámetro de condición de claves principales de DynamoDB ,

que es lo importante.

Y esto significa que el valor de la clave de partición

debe coincidir con el ID del usuario,

para que el usuario solo pueda acceder a los datos

que les pertenece, y no podrán

para acceder a los datos de otra persona.

Y luego en la sección de atributos de DynamoDB .

Esto define los atributos a los que se aplica la política.

Así que en nuestros consejos de examen.

Solo para que recuerdes, puedes configurar

detallado utilizando

de identidades y accesos.

Y usamos este parámetro de condición de IAM

llamado Claves principales de DynamoDB

para permitir que los usuarios accedan solo a los elementos

donde el valor de la clave de partición coincide con su ID de usuario.

Y cuando usamos esto en una declaración de condición

dentro de una política de gestión de acceso a la identidad,

podemos restringir el acceso de los usuarios solo a los elementos

que se relacionan con una identificación de usuario.

Y significa que no podrán ver

cualquier otra persona dentro de esa tabla.

Así que ese es el final de esta conferencia.

Si tiene alguna pregunta, por favor hágamelo saber.

De lo contrario, te veré en la próxima lección.

Gracias.