[ENGLISH]

Hello, Cloud Gurus!

And welcome to this section of the course,

which is going to cover

Advanced Identity and Access Management

beginning with web identity federation,

and web identity federation simplifies authentication

and authorization for web applications.

And it gives users access to AWS resources

after successfully authenticating

with a web-based identity provider

like Facebook, Amazon, or Google.

Following successful authentication,

users will receive an authentication code

from the web identity provider,

and they can trade this authentication code

for temporary AWS security credentials,

authorizing access to AWS resources.

And there's a service called Amazon Cognito,

which provides web identity federation,

including sign-up and sign-in functionality

for your applications and access for guest users as well.

So Cognito acts as an identity broker,

and this means that it manages the authentication

between your application and the web identity provider

like Facebook, for example.

So you don't need to write any additional code

to allow your users to sign up or sign in to your

application using their Facebook account.

And Cognito supports multiple devices,

and it will even synchronize user data

across multiple different devices,

for example, a tablet, mobile phone, and laptop.

And web identity federation with Cognito

is the recommended approach

for all mobile phone applications which call AWS services.

So let's take a look at a common use case for Cognito.

So just imagine a mobile shopping application

using S3 for product data and DynamoDB for customer data,

and you want your customers

to be able to access the product data

and their own customer data within the DynamoDB table.

And we can use Cognito

to configure web identity federation

using a social media account like Facebook.

And the way it works is that first

the user authenticates using Facebook,

and once the user has successfully authenticated

to Facebook, Cognito will provide temporary AWS credentials

allowing access to the AWS resources.

So Cognito provides temporary credentials,

and it brokers between the application

and Facebook, Amazon, or Google

to provide these temporary credentials,

and the temporary credentials map

to an Identity Access Management role

allowing access to the required resources.

And Cognito is secure and seamless.

So there's no need for the application

to embed or store AWS credentials locally on the device.

And Cognito also gives users a seamless experience

across all devices.

So your user data will be completely up to date,

no matter what device you're using.

Now, Cognito has some terminology

that you will need to understand.

And firstly, we have user pools,

and these are user directories

used to manage the sign-up and sign-in functionality

for mobile and web applications.

And users can sign-in directly to the user pool

or by using a web identity provider

like Facebook, Amazon, or Google.

And then we have identity pools,

and identity pools enable you

to provide the temporary AWS credentials

enabling access to AWS services, like S3 or DynamoDB.

So try it to remember the distinction.

User pools are for sign-up and sign-in functionality,

whereas identity pools

are all about providing temporary AWS credentials,

allowing users to access AWS services.

So let's take a look at a Cognito workflow

in a little bit more detail.

Here's our user,

and she's using a mobile application on her tablet,

and she wants to authenticate using Facebook.

So first of all, she logs into Facebook,

and a Cognito user pool will broker the sign-up

and sign-in functionality with Facebook.

And after successfully logging in,

then Facebook will return a JWT token, or a JSON web token.

And it's this JWT token,

which is exchanged for AWS credentials

by the Cognito identity pool.

And then these credentials

map to an Identity Access Management role

which gives the user access to AWS resources.

Now Cognito can also manage synchronization

of the user experience across multiple devices.

So it tracks the association between a user identity

and the various different devices that they sign in from.

And it uses a technology called push synchronization

to push updates and synchronize user data

across multiple devices,

and under the hood, it's using SNS notifications.

So it sends an SNS notification to all the devices

associated with a given user identity

whenever data stored in the cloud changes.

So here is our user,

and imagine he's made an update to his account details,

and maybe he's changed his address

while logged in on his mobile phone.

Cognito will then send an SNS silent push notification

to each of the devices that are associated with this user.

And then next time our user logs in

using one of these other devices,

it should show the new address.

So onto my exam tips,

and remember web identity federation is all about

allowing users to authenticate to your application,

using a web identity provider

and following a successful authentication.

An authentication token, or JWT token,

is exchanged for temporary AWS credentials,

allowing users to assume an Identity Access Management role

with permission to access AWS resources.

And we can use Cognito to act as an identity broker

handling all the interaction

with the web identity providers.

It provides sign up and sign in,

as well as guest user access.

And Cognito is the AWS recommended approach

for web identity federation for mobile applications.

So if you see anything in the exam

relating to web identity federation

for a mobile application,

then I want you to remember Cognito.

It's important to remember the differences

between user pools and identity pools,

and user pools are user directories

used to manage sign-up and sign-in functionality

for mobile and web applications,

whereas identity pools enable you

to provide a temporary AWS credentials

enabling access to AWS services, like S3 or DynamoDB.

So user pools are all about

sign-up and sign-in functionality,

whereas identity pools are all about

providing the temporary AWS credentials.

And finally, Cognito push synchronization uses SNS

to send a silent push notification of user data updates

to multiple devices associated with a single user ID.

And just think about our user

updating his address on his mobile phone.

When he logs in to the same application using his tablet,

he wants to see the new address reflected.

So that's it for 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 sección del curso,

que va a cubrir

Gestión avanzada de identidades y accesos

comenzando con la federación de identidad web,

y la federación de identidad web simplifica la autenticación

y autorización para aplicaciones web.

Y les da a los usuarios acceso a los recursos de AWS

después de autenticarse con éxito

con un proveedor de identidad basado en la web

como Facebook, Amazon o Google.

Después de una autenticación exitosa,

los usuarios recibirán un código de autenticación

del proveedor de identidad web,

y pueden intercambiar este código de autenticación

para credenciales de seguridad temporales de AWS,

autorizando el acceso a los recursos de AWS.

Y hay un servicio llamado Amazon Cognito ,

que proporciona federación de identidad web,

incluida la función de registro e inicio de sesión

para sus aplicaciones y acceso para usuarios invitados también.

Entonces, Cognito actúa como un agente de identidad,

y esto significa que gestiona la autenticación

entre su aplicación y el proveedor de identidad web

como Facebook, por ejemplo.

Así que no necesitas escribir ningún código adicional

para permitir que sus usuarios se registren o inicien sesión en su

aplicación utilizando su cuenta de Facebook.

Y Cognito es compatible con múltiples dispositivos,

e incluso sincronizará los datos del usuario

a través de múltiples dispositivos diferentes,

por ejemplo, una tableta, un teléfono móvil y una computadora portátil.

Y federación de identidad web con Cognito

es el enfoque recomendado

para todas las aplicaciones de teléfonos móviles que llaman a los servicios de AWS.

Así que echemos un vistazo a un caso de uso común para Cognito .

Así que imagina una aplicación de compras móvil

usando S3 para datos de productos y DynamoDB para datos de clientes,

y quieres que tus clientes

para poder acceder a los datos del producto

y sus propios datos de clientes dentro de la tabla de DynamoDB .

Y podemos usar Cognito

para configurar la federación de identidad web

utilizando una cuenta de redes sociales como Facebook.

Y la forma en que funciona es que primero

el usuario se autentica usando Facebook,

y una vez que el usuario se haya autenticado con éxito

a Facebook, Cognito proporcionará credenciales temporales de AWS

permitiendo el acceso a los recursos de AWS.

Entonces, Cognito proporciona credenciales temporales,

y actúa como intermediario entre la aplicación

y Facebook, Amazon o Google

para proporcionar estas credenciales temporales,

y el mapa de credenciales temporales

a un rol de administración de acceso a la identidad

permitiendo el acceso a los recursos requeridos.

Y Cognito es seguro y fluido.

Así que no hay necesidad de la aplicación.

para incrustar o almacenar credenciales de AWS localmente en el dispositivo.

Y Cognito también brinda a los usuarios una experiencia perfecta

en todos los dispositivos.

Así tus datos de usuario estarán completamente actualizados,

no importa qué dispositivo estés usando.

Ahora, Cognito tiene algo de terminología.

que tendrás que entender.

Y en primer lugar, tenemos grupos de usuarios,

y estos son directorios de usuarios

se utiliza para administrar la funcionalidad de registro e inicio de sesión

para aplicaciones móviles y web.

Y los usuarios pueden iniciar sesión directamente en el grupo de usuarios

o mediante el uso de un proveedor de identidad web

como Facebook, Amazon o Google.

Y luego tenemos grupos de identidad,

y los grupos de identidades le permiten

para proporcionar las credenciales temporales de AWS

permitiendo el acceso a los servicios de AWS, como S3 o DynamoDB .

Así que pruébalo para recordar la distinción.

Los grupos de usuarios son para la funcionalidad de registro e inicio de sesión,

mientras que los grupos de identidad

se trata de proporcionar credenciales temporales de AWS,

permitiendo a los usuarios acceder a los servicios de AWS.

Así que echemos un vistazo a un flujo de trabajo de Cognito

con un poco más de detalle.

Aquí está nuestro usuario,

y ella está usando una aplicación móvil en su tableta,

y quiere autenticarse usando Facebook.

En primer lugar, inicia sesión en Facebook,

y un grupo de usuarios de Cognito negociará el registro

y funcionalidad de inicio de sesión con Facebook.

Y después de iniciar sesión con éxito,

luego , Facebook devolverá un token JWT o un token web JSON.

Y es este token JWT,

que se intercambia por credenciales de AWS

por el grupo de identidades de Cognito .

Y luego estas credenciales

asignar a un rol de administración de acceso a la identidad

que le da al usuario acceso a los recursos de AWS.

Ahora Cognito también puede gestionar la sincronización

de la experiencia del usuario en múltiples dispositivos.

Entonces rastrea la asociación entre una identidad de usuario

y los distintos dispositivos desde los que inician sesión.

Y utiliza una tecnología llamada sincronización push

para enviar actualizaciones y sincronizar datos de usuario

a través de múltiples dispositivos,

y bajo el capó, está usando notificaciones SNS.

Entonces envía una notificación SNS a todos los dispositivos

asociado con una identidad de usuario dada

siempre que cambien los datos almacenados en la nube.

Así que aquí está nuestro usuario,

e imagina que ha actualizado los detalles de su cuenta,

y tal vez ha cambiado su dirección

mientras estaba conectado en su teléfono móvil.

Cognito luego enviará una notificación push silenciosa SNS

a cada uno de los dispositivos que están asociados a este usuario.

Y luego, la próxima vez que nuestro usuario inicie sesión

utilizando uno de estos otros dispositivos,

debe mostrar la nueva dirección.

Entonces, en mis consejos para el examen,

y recuerde que la federación de identidad web se trata de

permitir a los usuarios autenticarse en su aplicación,

utilizando un proveedor de identidad web

y después de una autenticación exitosa.

Un token de autenticación, o token JWT,

se cambia por credenciales temporales de AWS,

permitir que los usuarios asuman un rol de gestión de acceso a la identidad

con permiso para acceder a los recursos de AWS.

Y podemos usar Cognito para actuar como intermediario de identidad.

manejar toda la interacción

con los proveedores de identidad web.

Proporciona registrarse e iniciar sesión,

así como acceso de usuario invitado.

Y Cognito es el enfoque recomendado por AWS

para la federación de identidad web para aplicaciones móviles.

Así que si ves algo en el examen

relacionado con la federación de identidad web

para una aplicación móvil,

entonces quiero que recuerdes a Cognito .

Es importante recordar las diferencias.

entre grupos de usuarios y grupos de identidades,

y los grupos de usuarios son directorios de usuarios

se utiliza para administrar la funcionalidad de registro e inicio de sesión

para aplicaciones móviles y web,

mientras que los grupos de identidades le permiten

para proporcionar unas credenciales temporales de AWS

permitiendo el acceso a los servicios de AWS, como S3 o DynamoDB .

Así que los grupos de usuarios se tratan de

de registro e inicio de sesión,

mientras que los grupos de identidad tienen que ver con

proporcionando las credenciales temporales de AWS.

Y finalmente, la sincronización push de Cognito usa SNS

para enviar una notificación push silenciosa de actualizaciones de datos de usuario

a múltiples dispositivos asociados con una sola ID de usuario.

Y solo piensa en nuestro usuario

actualizando su dirección en su teléfono móvil.

Cuando inicia sesión en la misma aplicación usando su tableta,

quiere ver reflejada la nueva dirección.

Así que eso es todo por esta conferencia.

Si tiene alguna pregunta, por favor hágamelo saber.

De lo contrario, te veré en la próxima lección. Gracias.