[ENGLISH]

Hello, Cloud Gurus,

and welcome to this lecture.

And this lecture is all about STS,

and the AssumeRoleWithWebIdentity API.

So let's get started.

So what is assume-role-with-web-identity?

Well, it's an API, which is provided by STS,

which is the Security Token Service,

and it returns temporary security credentials

for users which have been authenticated by either a mobile

or web application using a web identity provider

like Amazon, Facebook, or Google.

And of course for mobile phone applications,

they recommend Cognito, and underneath Cognito

is actually making the STS assume-role-with-web-identity

calls on your behalf.

So when you use Cognito you don't explicitly

need to use this API.

However, for regular web applications,

where you're not using Cognito

you can use this STS assume-role-with-web-identity-API.

So let's take a look at an example workflow.

And we have our user on the left-hand side here.

And she's going to authenticate using Facebook, Google,

or Amazon.

And once she's successfully authenticated,

the web ID provider passes back a JWT token

to the application.

The application then makes

the assume-role-with-web-identity API call to STS.

And as part of that API call, it provides the JWT token.

STS then exchanges the JWT token for temporary credentials.

So an access key and secret access key.

Finally, the application can use those temporary credentials

to access AWS resources.

For example DynamoDB tables,

or the contents of an S3 bucket.

So let's take a look at a sample response

that you might see when your application makes a call

to assume-role-with-web-identity.

Now, the main two things that you need to know

about the sample response, are that firstly it responds

with this assumed-role user ARN,

and the assumed-role ID.

On both of these are simply ARN

or Amazon Resource Name identifiers,

and these can be used if you want to refer programmatically

to the temporary credentials.

So, if your application code needs to later on refer

to the temporary credentials, these are the identifiers

that it's going to use.

And it can be a little bit confusing

because it's referring to roles and IDs.

It's nothing to do with identity access management roles.

Just remember it's the specific ARN identifier

that you can use to programmatically refer

to the temporary credentials.

And then the next section that I've highlighted,

is the credentials themselves.

So you get a session token,

and then you get a secret access key and access key.

And these are temporary.

And by default, they're only going to last

for one hour before they expire.

There's an expiration timestamp included as well.

So let's take a look at some of our exam tips

for assume-role-with-web-identity.

Just remember it's part of the Security Token Service.

It allows users who have authenticated

with a web identity provider like Facebook, Google

or Amazon, to access AWS resources temporarily.

Once the user has authenticated with the web ID provider

the application then makes the assume role-with-web-identity

API call.

And if it's successful,

STS will return temporary credentials,

enabling access to AWS resources.

And just remember this assumed-role user ARN

and the assumed-role ID.

Those are used to programmatically reference

the temporary credentials, they're not related

to an identity management role or user.

They are simply ARNs used to programmatically reference

the credentials.

So that is everything that you should need to know

for the exam about assume-role-with-web-identity.

If you have any questions, please let me know.

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

Thank you.

[SPANISH]

Hola, gurús de la nube,

y bienvenidos a esta conferencia.

Y esta conferencia es todo sobre STS,

y la API AssumeRoleWithWebIdentity .

Entonces empecemos.

Entonces, ¿qué es asumir un rol con identidad web?

Bueno, es una API proporcionada por STS,

que es el servicio de token de seguridad,

y devuelve credenciales de seguridad temporales

para usuarios que han sido autenticados por un dispositivo móvil

o aplicación web usando un proveedor de identidad web

como Amazon, Facebook o Google.

Y por supuesto para aplicaciones de teléfonos móviles,

recomiendan Cognito , y debajo de Cognito

está haciendo que el STS asuma un rol con identidad web

llama en su nombre.

Entonces, cuando usas Cognito , no explícitamente

necesita usar esta API.

Sin embargo, para las aplicaciones web normales,

donde no estás usando Cognito

puede usar este STS asumir-role-con-web-identity-API.

Así que echemos un vistazo a un flujo de trabajo de ejemplo.

Y aquí tenemos a nuestro usuario en el lado izquierdo.

Y se va a autenticar usando Facebook, Google,

o Amazon.

Y una vez que se haya autenticado con éxito,

el proveedor de ID web devuelve un token JWT

a la aplicación

La aplicación entonces hace

la llamada API de asumir rol con identidad web a STS.

Y como parte de esa llamada a la API, proporciona el token JWT.

STS luego intercambia el token JWT por credenciales temporales.

Entonces, una clave de acceso y una clave de acceso secreta.

Finalmente, la aplicación puede usar esas credenciales temporales

para acceder a los recursos de AWS.

Por ejemplo , tablas de DynamoDB ,

o el contenido de un depósito S3.

Así que echemos un vistazo a una respuesta de muestra

que podrías ver cuando tu aplicación hace una llamada

para asumir-rol-con-identidad-web.

Ahora, las dos cosas principales que necesitas saber

sobre la respuesta de la muestra, son que en primer lugar responde

con este ARN de usuario de rol asumido,

y el ID del rol asumido.

En ambos son simplemente ARN

o identificadores de nombres de recursos de Amazon,

y estos se pueden usar si desea hacer referencia mediante programación

a las credenciales temporales.

Entonces, si el código de su aplicación necesita consultar más adelante

a las credenciales temporales, estos son los identificadores

que va a usar.

Y puede ser un poco confuso

porque se refiere a roles e ID.

No tiene nada que ver con los roles de administración de acceso a la identidad.

Solo recuerda que es el identificador de ARN específico

que puede usar para hacer referencia programáticamente

a las credenciales temporales.

Y luego la siguiente sección que he resaltado,

son las propias credenciales.

Entonces obtienes un token de sesión,

y luego obtienes una clave de acceso secreta y una clave de acceso.

Y estos son temporales.

Y por defecto, solo van a durar

durante una hora antes de que caduquen.

También se incluye una marca de tiempo de caducidad.

Así que echemos un vistazo a algunos de nuestros consejos para el examen.

para asumir-rol-con-identidad-web.

Solo recuerde que es parte del Servicio de token de seguridad.

Permite a los usuarios que se han autenticado

con un proveedor de identidad web como Facebook, Google

o Amazon, para acceder a los recursos de AWS temporalmente.

Una vez que el usuario se haya autenticado con el proveedor de identificación web

la aplicación luego asume el rol con identidad web

llamada API.

Y si tiene éxito,

STS devolverá credenciales temporales,

permitir el acceso a los recursos de AWS.

Y solo recuerde este ARN de usuario de rol asumido

y el ID del rol asumido.

Se utilizan para hacer referencia programáticamente

las credenciales temporales, no están relacionadas

a un rol o usuario de administración de identidad.

Son simplemente ARN que se utilizan para hacer referencia mediante programación

las credenciales

Así que eso es todo lo que deberías saber

para el examen sobre asumir-rol-con-identidad-web.

Si tiene alguna pregunta, por favor hágamelo saber.

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

Gracias.