[ENGLISH]

Hello Cloud Gurus and welcome to this lecture,

which is going to introduce RDS backups and snapshots.

Now when it comes to backing up your data held in RDS,

you've actually got two options.

And they're similar,

but they have some very important differences.

So firstly, we have database snapshots,

which are manual, ad-hoc, and user initiated.

And this provides a snapshot or a point in time copy

of the storage volume attached to your database instance.

And we also have automated backups,

and these are enabled by default.

And with automated backups,

RDS creates daily backups or snapshots

which run during a backup window that you define.

And in addition to this daily backup,

it also generates transaction logs,

which are used to replay transactions

when you come to restore the database.

So let's take a closer look at each of these options

in a little bit more detail,

beginning with automated backups.

Now with automated backups,

you actually get a lot more bang for your buck,

because this gives you the ability

to perform a point-in-time recovery

and recover your database to any point in time

within a retention period of between one and 35 days.

So this gives you the ability to recover

to any point in time within your defined retention period.

So how does it do that?

Well, it performs a full daily backup or snapshot,

and it also stores transaction logs throughout the day.

And then during the recovery process,

when you perform a recovery,

AWS will first select the most recent daily backup.

It will then apply the transaction logs relevant to that day

up to the recovery point that you select.

So imagine that you have an RDS database,

storing details of your customers online purchases.

You have an automated backup scheduled to complete

within a backup window of between 2:00 AM and 5:00 AM.

So RDS will automatically take a daily snapshot

during that backup window,

and the snapshots are stored in S3.

And it's also creating transaction logs as well.

So let's say that somebody accidentally deleted

some of your data and you need to recover the database back

to the state that it was in at 9:00 AM this morning.

Well to do that,

RDS will restore using the latest snapshot,

and it's then going to use the transaction logs

to replay any changes which happened

since the snapshot was taken.

So any changes that happened up to our recovery point,

which was 9:00 AM this morning.

And it's this combination of the daily snapshot

and the transaction log which enables point-in-time recovery

down to the second within your retention period.

And the retention period is of course user-defined.

And it can be anything between one and 35 days.

So with automated backups,

these are stored in S3,

and the manual snapshots are also stored in S3.

You get free storage space equivalent

to the size of your database.

So if you've got an RDS instance with 10 gigs of data,

then you will get 10 gigs worth of storage

for your automated backups.

And everything happens within a backup window

that you define.

However, during the backup window,

your storage I/O may be suspended for just a few seconds

while the backup process initializes itself.

And during this time, you may experience increased latency.

But this is only during the initialization process.

And after that,

your latency on your performance should go back to normal.

So what about snapshots?

Well, these are not automated.

So database snapshots are done manually,

and they are user-initiated.

There is no retention period when you do a manual snapshot.

So they are not deleted even after you delete

the original RDS instance, including any automated backups.

So the database and its backups can be deleted,

and the snapshots will remain.

And snapshots enable you to back up your database

to a known state.

And you can back up your database instance to a known state

as frequently as you wish,

and then restore to that specific state at any time.

So when would you use this?

Well, imagine you were planning

some significant updates to your data.

You might wish to backup to a known state

before you make any changes to your data,

so that you can always restore back to that state

if anything goes wrong.

Now when you come to restore an RDS database,

whether you restore from an automated backup

or from a manual snapshot,

the restored version of the database

will always be a completely new RDS instance

with a new DNS endpoint.

So it's going to have a different endpoint

to your original RDS instance.

So we've got our original endpoint

and the new endpoint for the restored database.

Moving on to encryption,

and you might be wondering,

how does encryption fit in with all of this?

Well, there is a link,

and there are some important features to be aware of

when it comes to encryption and database snapshots.

Encryption at rest is very easy to enable with RDS,

and you can enable it at creation time

by just selecting the encryption option in the console.

And this is something that we're going to see later on

when we can come to create our own RDS instance.

And RDS is completely integrated with KMS.

So encryption is done using KMS,

and it uses the industry standard, AES-256 bit encryption.

Now when we enable encryption on an RDS database,

then RDS is going to encrypt all of the database storage.

So that includes all of the underlying storage associated

with your RDS database,

including any automated backups,

any manual snapshots, any logs,

and read replicas as well.

And if you haven't heard of read replicas,

we will be covering those later on

in this section of the course.

Now encryption can only be enabled

when you first create the database,

and you cannot later on enable encryption

on an unencrypted RDS database instance.

So what do you do

if you have an existing unencrypted database

and you are suddenly asked to encrypt that data?

Well, snapshots can actually help you with that situation,

to help encrypt your database.

So if you've already created an unencrypted database

and you need to encrypt that data,

you can take a snapshot

and that snapshot will also be unencrypted.

And then from that unencrypted snapshot,

you can create an encrypted snapshot,

and then perform a database restore

using that encrypted snapshot.

And in that way, you will get an encrypted database.

So this will be a copy of your original database,

but with everything encrypted.

And it sounds like a pretty long winded process.

So if possible, to avoid that,

make sure you find out if the data needs to be encrypted

before creating your database.

And then you can just enable encryption in the beginning.

So onto my exam tips for backups and snapshots.

And you'll need to understand

the difference between an automated backup

and a database snapshot or a manual snapshot.

So automated backups are enabled by default

and you define the backup window.

It runs a daily backup consisting

of a point-in-time snapshot or backup plus transaction logs,

allowing you to restore to any point in time

within your retention period.

And you can define a retention period

of anything between one and 35 days,

and automated backups can be used to recover your database

to any point in time down to the second

within that retention period.

Alternatively, with database snapshots,

and you might also see them called manual snapshots.

These are user-initiated and ad-hoc.

So they don't happen automatically.

It's a point-in-time snapshot only,

and there is no retention period.

So your snapshots are stored indefinitely,

even if the database and its automated backups are deleted.

And a database snapshot can be used

to backup your database instance to a known state

and restore to that specific state at any time.

For example before making a change

to your production database,

you might take a snapshot

so that you can easily roll back the changes

if something goes wrong.

When it comes to encryption,

you can only enable encryption

when you first create the database.

So you cannot enable it later.

And when encryption is enabled,

this includes all of the underlying storage

of the RDS database, including your automated backups,

any snapshots, logs, and read replicas.

And when you enable encryption,

it uses the AWS key management service

with the industry standard, AES-256 bit encryption.

And finally if you didn't enable encryption

at creation time,

and then you'd later on need to encrypt the data

in your RDS instance,

then you can use snapshot technology to take a snapshot.

And from that snapshot,

create an encrypted snapshot,

and create a new RDS instance from the encrypted snapshot.

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 Cloud Gurus y bienvenidos a esta conferencia,

que va a introducir copias de seguridad e instantáneas de RDS.

Ahora, cuando se trata de hacer una copia de seguridad de sus datos guardados en RDS,

tienes dos opciones.

Y son similares,

pero tienen algunas diferencias muy importantes.

En primer lugar, tenemos instantáneas de la base de datos,

que son manuales, ad-hoc e iniciados por el usuario.

Y esto proporciona una instantánea o una copia de un punto en el tiempo

del volumen de almacenamiento adjunto a su instancia de base de datos.

Y también tenemos copias de seguridad automatizadas,

y estos están habilitados por defecto.

Y con las copias de seguridad automatizadas,

RDS crea copias de seguridad o instantáneas diarias

que se ejecutan durante una ventana de copia de seguridad que defina.

Y además de esta copia de seguridad diaria,

también genera registros de transacciones,

que se utilizan para reproducir transacciones

cuando vengas a restaurar la base de datos.

Así que echemos un vistazo más de cerca a cada una de estas opciones.

con un poco más de detalle,

comenzando con copias de seguridad automatizadas.

Ahora con copias de seguridad automatizadas,

obtienes mucho más por tu dinero,

porque esto te da la habilidad

para realizar una recuperación puntual

y recupere su base de datos en cualquier momento

dentro de un período de retención de entre uno y 35 días.

Así que esto te da la capacidad de recuperar

a cualquier punto en el tiempo dentro de su período de retención definido.

Entonces, ¿cómo hace eso?

Bueno, realiza una copia de seguridad o instantánea diaria completa,

y también almacena registros de transacciones a lo largo del día.

Y luego, durante el proceso de recuperación,

cuando realiza una recuperación,

AWS seleccionará primero la copia de seguridad diaria más reciente.

Luego aplicará los registros de transacciones relevantes para ese día.

hasta el punto de recuperación que seleccione.

Imagine que tiene una base de datos RDS,

almacenar detalles de las compras en línea de sus clientes.

Tienes una copia de seguridad automatizada programada para completarse

dentro de una ventana de copia de seguridad de entre las 2:00 a. m. y las 5:00 a. m.

Entonces RDS tomará automáticamente una instantánea diaria

durante esa ventana de copia de seguridad,

y las instantáneas se almacenan en S3.

Y también está creando registros de transacciones.

Así que digamos que alguien borró accidentalmente

algunos de sus datos y necesita recuperar la base de datos

al estado en que se encontraba a las 9:00 a. m. de esta mañana.

Bueno, para hacer eso,

RDS restaurará utilizando la última instantánea,

y luego usará los registros de transacciones

para reproducir cualquier cambio que haya ocurrido

desde que se tomó la instantánea.

Entonces, cualquier cambio que haya ocurrido hasta nuestro punto de recuperación,

que fue a las 9:00 a. m. de esta mañana.

Y es esta combinación de la instantánea diaria

y el registro de transacciones que permite la recuperación en un momento dado

hasta el segundo dentro de su período de retención.

Y el período de retención es, por supuesto, definido por el usuario.

Y puede ser cualquier cosa entre uno y 35 días.

Entonces, con las copias de seguridad automatizadas,

estos se almacenan en S3,

y las instantáneas manuales también se almacenan en S3.

Obtienes espacio de almacenamiento gratuito equivalente

al tamaño de su base de datos.

Entonces, si tiene una instancia de RDS con 10 gigas de datos,

entonces obtendrás 10 gigas de almacenamiento

para sus copias de seguridad automatizadas.

Y todo sucede dentro de una ventana de copia de seguridad

que tu definas.

Sin embargo, durante la ventana de copia de seguridad,

su E/S de almacenamiento puede suspenderse por solo unos segundos

mientras el proceso de copia de seguridad se inicializa.

Y durante este tiempo, puede experimentar una mayor latencia.

Pero esto es solo durante el proceso de inicialización.

Y después de eso,

su latencia en su rendimiento debería volver a la normalidad.

Entonces, ¿qué pasa con las instantáneas?

Bueno, estos no están automatizados.

Entonces, las instantáneas de la base de datos se realizan manualmente,

y son iniciados por el usuario.

No hay período de retención cuando realiza una instantánea manual.

Para que no se eliminen incluso después de eliminar

la instancia de RDS original, incluidas las copias de seguridad automatizadas.

Entonces la base de datos y sus copias de seguridad se pueden eliminar,

y las instantáneas permanecerán.

Y las instantáneas le permiten hacer una copia de seguridad de su base de datos

a un estado conocido.

Y puede hacer una copia de seguridad de su instancia de base de datos en un estado conocido

con la frecuencia que desees,

y luego restaurar a ese estado específico en cualquier momento.

Entonces, ¿cuándo usarías esto?

Bueno, imagina que estabas planeando

algunas actualizaciones significativas a sus datos.

Es posible que desee realizar una copia de seguridad en un estado conocido

antes de realizar cualquier cambio en sus datos,

para que siempre pueda restaurar de nuevo a ese estado

si algo sale mal.

Ahora, cuando venga a restaurar una base de datos RDS,

si restaura desde una copia de seguridad automática

o desde una instantánea manual,

la versión restaurada de la base de datos

será una instancia RDS completamente nueva

con un nuevo extremo DNS.

Así que va a tener un punto final diferente

a su instancia original de RDS.

Así que tenemos nuestro punto final original

y el nuevo punto final para la base de datos restaurada.

Pasando al cifrado,

y te estarás preguntando,

¿Cómo encaja el cifrado en todo esto?

Bueno, hay un enlace,

y hay algunas características importantes a tener en cuenta

cuando se trata de instantáneas de cifrado y base de datos.

El cifrado en reposo es muy fácil de habilitar con RDS,

y puede habilitarlo en el momento de la creación

simplemente seleccionando la opción de cifrado en la consola.

Y esto es algo que vamos a ver más adelante.

cuando podemos llegar a crear nuestra propia instancia de RDS.

Y RDS está completamente integrado con KMS.

Entonces, el cifrado se realiza mediante KMS,

y utiliza el estándar de la industria, encriptación AES-256 bit.

Ahora, cuando habilitamos el cifrado en una base de datos RDS,

entonces RDS cifrará todo el almacenamiento de la base de datos.

Eso incluye todo el almacenamiento subyacente asociado

con su base de datos RDS,

incluidas las copias de seguridad automáticas,

cualquier instantánea manual, cualquier registro,

y leer réplicas también.

Y si no ha oído hablar de las réplicas de lectura,

cubriremos más adelante

en esta sección del curso.

Ahora el cifrado solo se puede habilitar

cuando crea la base de datos por primera vez,

y luego no puede habilitar el cifrado

en una instancia de base de datos RDS sin cifrar.

entonces que haces

si tiene una base de datos no cifrada existente

y de repente se le pide que encripte esos datos?

Bueno, las instantáneas pueden ayudarte con esa situación.

para ayudar a cifrar su base de datos.

Entonces, si ya ha creado una base de datos sin cifrar

y necesitas encriptar esos datos,

puedes tomar una instantánea

y esa instantánea también estará sin cifrar.

Y luego, a partir de esa instantánea sin cifrar,

puede crear una instantánea cifrada,

y luego realice una restauración de la base de datos

utilizando esa instantánea cifrada.

Y de esa manera, obtendrá una base de datos encriptada.

Así que esta será una copia de su base de datos original,

pero con todo encriptado.

Y suena como un proceso bastante largo.

Entonces, si es posible, para evitar eso,

asegúrese de averiguar si los datos deben cifrarse

antes de crear su base de datos.

Y luego puede habilitar el cifrado al principio.

Entonces, en mis consejos de examen para copias de seguridad e instantáneas.

Y tendrás que entender

la diferencia entre una copia de seguridad automatizada

y una instantánea de la base de datos o una instantánea manual.

Por lo tanto, las copias de seguridad automáticas están habilitadas de forma predeterminada

y usted define la ventana de copia de seguridad.

Ejecuta una copia de seguridad diaria que consiste

de una instantánea o copia de seguridad de un punto en el tiempo más registros de transacciones,

permite restaurar a cualquier punto en el tiempo

dentro de su período de retención.

Y puede definir un período de retención

de cualquier cosa entre uno y 35 días,

y las copias de seguridad automáticas se pueden usar para recuperar su base de datos

a cualquier punto en el tiempo hasta el segundo

dentro de ese período de retención.

Alternativamente, con las instantáneas de la base de datos,

y también puede verlos llamados instantáneas manuales.

Estos son iniciados por el usuario y ad-hoc.

Así que no suceden automáticamente.

Es solo una instantánea de un punto en el tiempo,

y no hay período de retención.

Entonces sus instantáneas se almacenan indefinidamente,

incluso si se eliminan la base de datos y sus copias de seguridad automáticas.

Y se puede usar una instantánea de la base de datos

a copia de seguridad de su instancia de base de datos a un estado conocido

y restaurar a ese estado específico en cualquier momento.

Por ejemplo antes de hacer un cambio

a su base de datos de producción,

podrías tomar una instantánea

para que pueda revertir fácilmente los cambios

si algo sale mal.

Cuando se trata de encriptación,

puedes habilitar el cifrado

cuando crea la base de datos por primera vez.

Por lo tanto, no puede habilitarlo más tarde.

Y cuando el cifrado está habilitado,

esto incluye todo el almacenamiento subyacente

de la base de datos RDS, incluidas sus copias de seguridad automatizadas,

instantáneas , registros y réplicas de lectura.

Y cuando habilita el cifrado,

utiliza el servicio de administración de claves de AWS

con el estándar de la industria, cifrado AES-256 bit.

Y finalmente, si no habilitó el cifrado

en el momento de la creación,

y luego necesitaría cifrar los datos

en su instancia de RDS,

entonces puede usar la tecnología de instantáneas para tomar una instantánea.

Y de esa instantánea,

crear una instantánea cifrada,

y cree una nueva instancia de RDS a partir de la instantánea cifrada.

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.