Protección de cargas de trabajo en AWS / VMC

NetApp Solutions

NetApp
April 26, 2024

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions/ehc/aws-guest-dr-solution-overview.html on April 26, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Protección de cargas de trabajo en AWS / VMC 1
TR-4931: Recuperación ante desastres con VMware Cloud en Amazon Web Services y Guest Connect . . . 1
Backup y restauración de Veeam en VMware Cloud, con Amazon FSx para ONTAP 71
TR-4955: Recuperación ante desastres con FSX para ONTAP y VMC (cloud VMware de AWS) 104
Usar la replicación de Veeam y FSx para ONTAP para la recuperación ante desastres en VMware Cloud on AWS 117

Protección de cargas de trabajo en AWS / VMC

TR-4931: Recuperación ante desastres con VMware Cloud en Amazon Web Services y Guest Connect

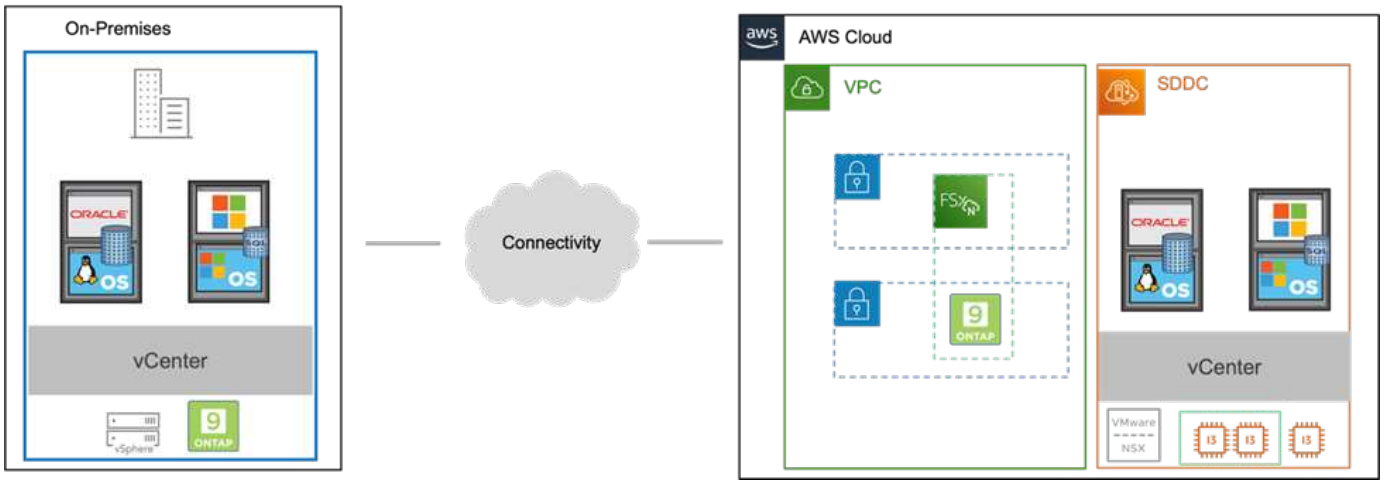
Autores: Chris Reno, Josh Powell y Suresh Toppay - Ingeniería de soluciones de NetApp

Descripción general

Un entorno y un plan de recuperación ante desastres contrastados es críticos para que las organizaciones puedan garantizar que las aplicaciones críticas se restauren rápidamente en caso de interrupción grave del servicio. Esta solución se centra en la demostración de casos prácticos de recuperación ante desastres centrándose en las tecnologías de VMware y NetApp, tanto en las instalaciones como con VMware Cloud en AWS.

NetApp tiene un largo historial de integración con VMware, tal y como muestran las decenas de miles de clientes que han elegido a NetApp como partner de almacenamiento para su entorno virtualizado. Esta integración continúa con las opciones conectadas a invitados en el cloud y las integraciones recientes también con almacenes de datos NFS. Esta solución se centra en el caso práctico conocido como almacenamiento conectado a invitados.

En el almacenamiento de conexión «guest», el VMDK invitado se pone en marcha en un almacén de datos con aprovisionamiento de VMware, y los datos de aplicaciones se alojan en iSCSI o NFS y se asignan directamente al equipo virtual. Las aplicaciones Oracle y MS SQL se utilizan para demostrar una situación de recuperación ante desastres, como se muestra en la siguiente figura.



Supuestos, requisitos previos y descripción general de los componentes

Antes de poner en marcha esta solución, revise la descripción general de los componentes, los requisitos previos necesarios para poner en marcha la solución y los supuestos que se realizan al documentar esta solución.

"Requisitos de la solución DR, requisitos previos y planificación"

Realizar una recuperación ante desastres con SnapCenter

En esta solución, SnapCenter ofrece copias Snapshot coherentes con las aplicaciones para los datos de aplicaciones de SQL Server y Oracle. Esta configuración, junto con la tecnología SnapMirror, proporciona replicación de datos de alta velocidad entre nuestro AFF local y el clúster ONTAP FSX. Además, Veeam Backup & Replication proporciona funcionalidades de backup y restauración para nuestras máquinas virtuales.

En esta sección trataremos la configuración de SnapCenter, SnapMirror y Veeam tanto para backup como para restaurar.

Las siguientes secciones tratan la configuración y los pasos necesarios para completar una conmutación por error en el sitio secundario:

Configurar las relaciones de SnapMirror y los programas de retención

SnapCenter puede actualizar las relaciones de SnapMirror en el sistema de almacenamiento primario (primario > reflejo) y en los sistemas de almacenamiento secundario (primario > almacén) con la finalidad de archivarlas y retenerlos a largo plazo. Para ello, debe establecer e inicializar una relación de replicación de datos entre un volumen de destino y un volumen de origen mediante SnapMirror.

Los sistemas ONTAP de origen y de destino deben estar en redes con una relación entre iguales mediante Amazon VPC, una puerta de enlace de tránsito, AWS Direct Connect o una VPN de AWS.

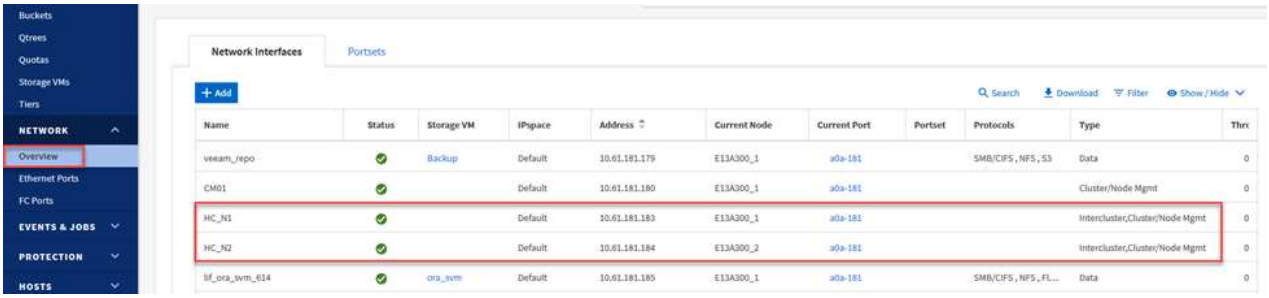
Se requieren los siguientes pasos para configurar las relaciones de SnapMirror entre un sistema ONTAP en las instalaciones y FSX ONTAP:

Consulte la "Guía del usuario de FSX para ONTAP – ONTAP" Para obtener más información sobre la creación de relaciones de SnapMirror con FSX.

Registre las interfaces lógicas de interconexión de clústeres de origen y destino

Para el sistema ONTAP de origen que reside en las instalaciones, puede recuperar la información de LIF entre clústeres desde System Manager o desde la CLI.

1. En ONTAP System Manager, desplácese a la página Network Overview y recupere las direcciones IP de Type: Interclúster configurado para comunicarse con el VPC donde se instaló FSX.



2. Para recuperar las direcciones IP de interconexión de clústeres para FSX, inicie sesión en la CLI y ejecute el siguiente comando:

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

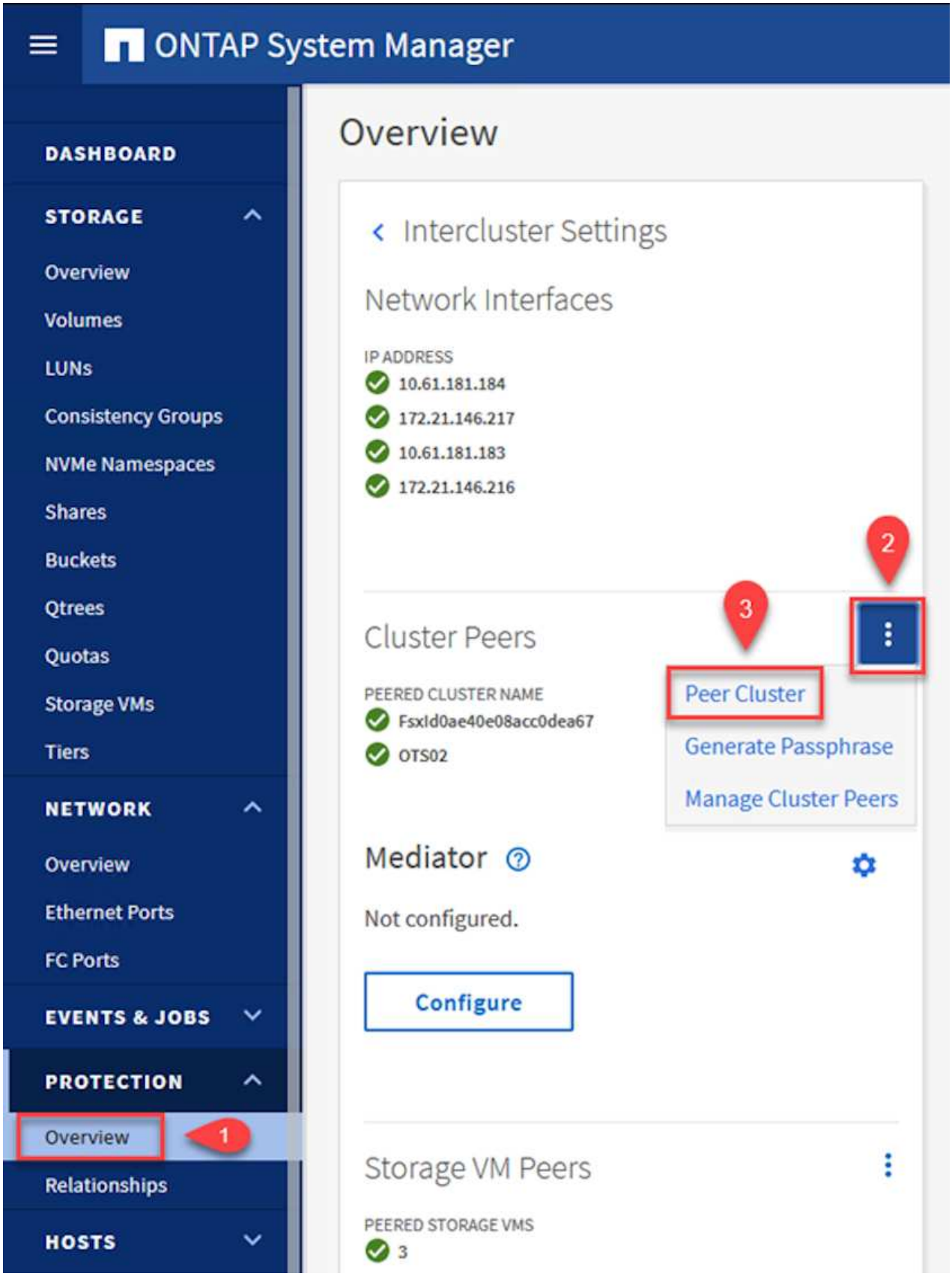
Establecer una relación entre clústeres y FSX y ONTAP

Para establecer una relación entre iguales de clústeres entre clústeres ONTAP, se debe confirmar una clave de acceso única introducida en el clúster de ONTAP de inicio en el otro clúster de paridad.

1. Configure peering en el clúster FSX de destino mediante el `cluster peer create` comando. Cuando se le solicite, introduzca una clave de acceso única que se usará más adelante en el clúster de origen para finalizar el proceso de creación.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. En el clúster de origen, puede establecer la relación de paridad de clústeres mediante ONTAP System Manager o CLI. En ONTAP System Manager, desplácese hasta Protection > Overview y seleccione Peer Cluster.

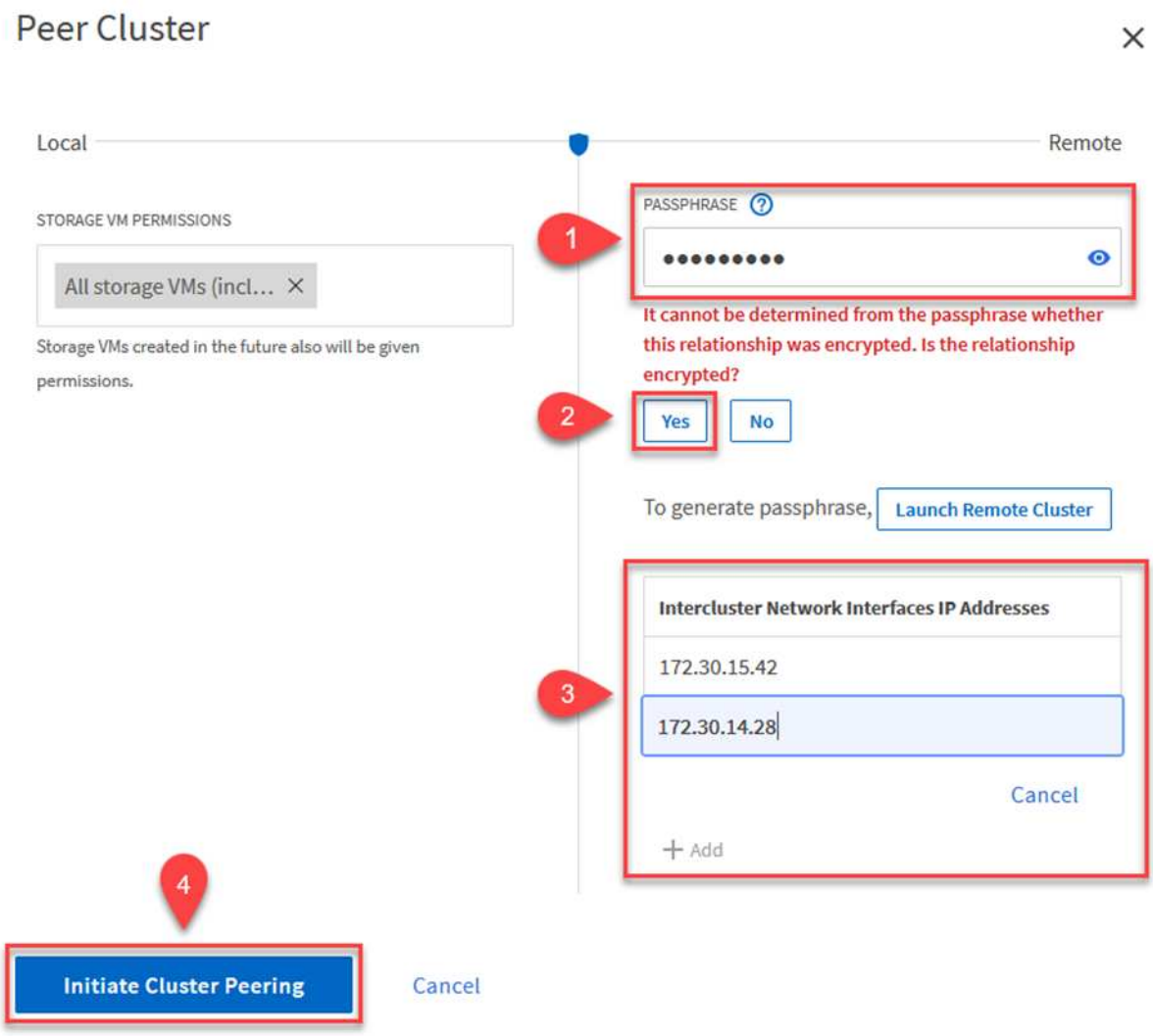


3. En el cuadro de diálogo Peer Cluster, rellene la información que corresponda:
   a. Introduzca la clave de acceso que se utilizó para establecer la relación de clúster entre iguales en el clúster FSX de destino.

b. Seleccione `Yes` para establecer una relación cifrada.

c. Introduzca las direcciones IP de la LIF entre clústeres del clúster FSX de destino.

d. Haga clic en Iniciar Cluster peering para finalizar el proceso.



4. Compruebe el estado de la relación de paridad del clúster desde el clúster FSX con el siguiente comando:

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

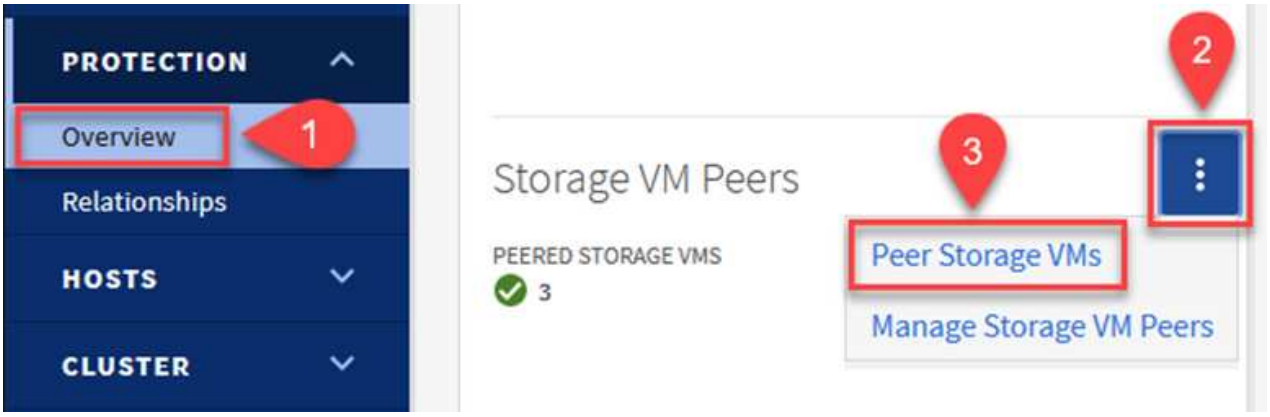
Establecer la relación de paridad de SVM

El siguiente paso consiste en configurar una relación de SVM entre las máquinas virtuales de almacenamiento de destino y origen que contengan los volúmenes que se incluirán en las relaciones de SnapMirror.

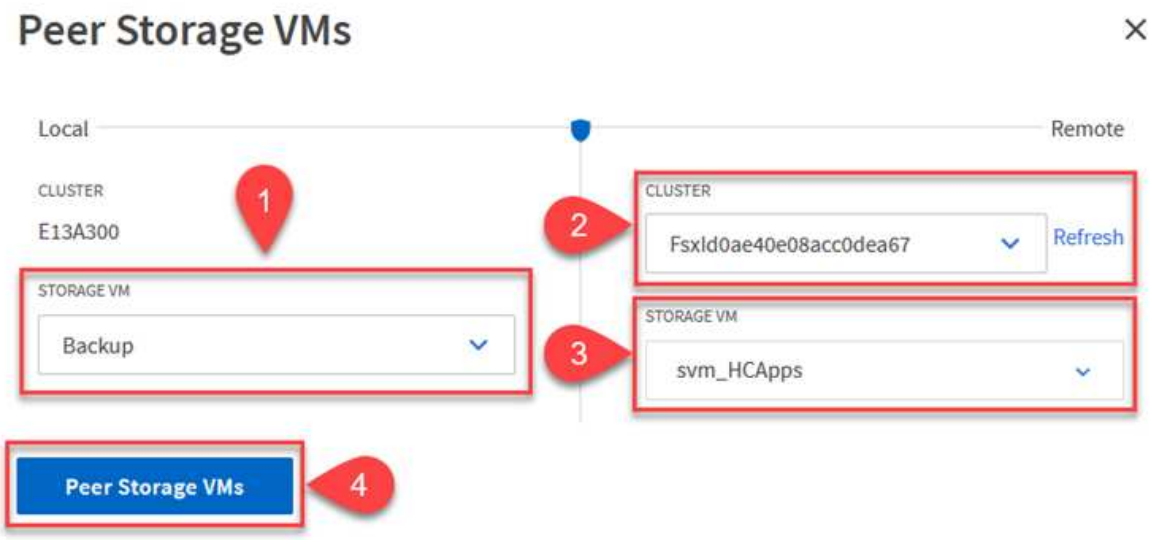
1. En el clúster FSX de origen, use el siguiente comando de la CLI para crear la relación entre iguales de SVM:

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. En el clúster de ONTAP de origen, acepte la relación de paridad con ONTAP System Manager o CLI.
3. En ONTAP System Manager, vaya a Protection > Overview y seleccione Peer Storage VMs, en Storage VM peers.



4. En el cuadro de diálogo de la VM de almacenamiento del mismo nivel, rellene los campos necesarios:
   - La máquina virtual de almacenamiento de origen
   - El clúster de destino
   - La máquina virtual de almacenamiento de destino



5. Haga clic en Peer Storage VMs para completar el proceso de paridad de SVM.

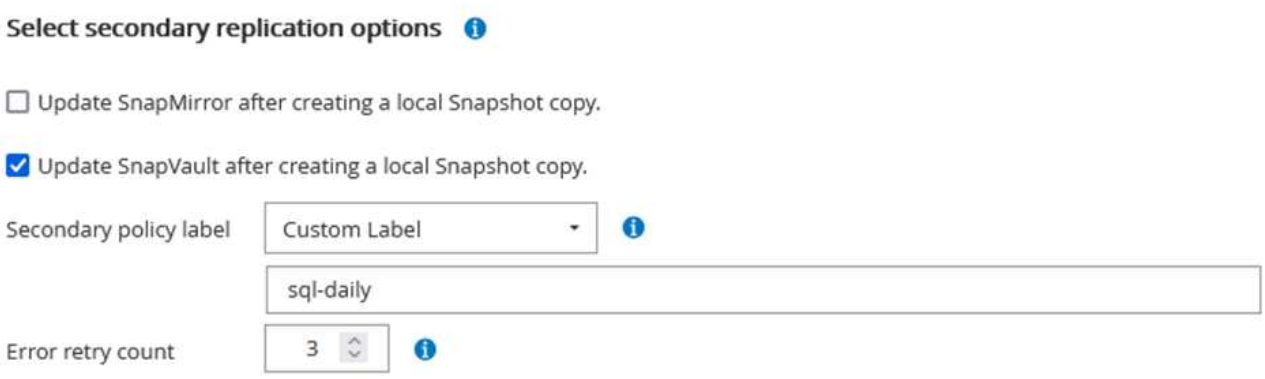
Crear una política de retención de snapshots

SnapCenter gestiona los programas de retención para los backups que existen como copias Snapshot en el sistema de almacenamiento principal. Esto se establece al crear una política en SnapCenter. SnapCenter no gestiona las políticas de retención para backups que se conservan en sistemas de almacenamiento secundario. Estas políticas se gestionan por separado mediante una política de SnapMirror creada en el clúster FSX secundario y asociada con los volúmenes de destino que se encuentran en una relación de SnapMirror con el volumen de origen.

Al crear una política de SnapCenter, tiene la opción de especificar una etiqueta de política secundaria que se añada a la etiqueta de SnapMirror de cada snapshot generada al realizar un backup de SnapCenter.

> En el almacenamiento secundario, estas etiquetas se adaptan a las reglas de normativas asociadas con el volumen de destino con el fin de aplicar la retención de copias Snapshot.

El siguiente ejemplo muestra una etiqueta de SnapMirror presente en todas las copias de Snapshot generadas como parte de una política utilizada para los backups diarios de nuestros volúmenes de registros y base de datos de SQL Server.



Para obtener más información sobre la creación de políticas de SnapCenter para una base de datos de SQL Server, consulte "Documentación de SnapCenter".

Primero debe crear una política de SnapMirror con reglas que exijan el número de copias de snapshot que se retendrán.

1. Cree la política SnapMirror en el clúster FSX.

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. Añada reglas a la política con etiquetas de SnapMirror que coincidan con las etiquetas de política secundaria especificadas en las políticas de SnapCenter.

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

El siguiente script ofrece un ejemplo de una regla que se puede agregar a una directiva:

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

Crear reglas adicionales para cada etiqueta de SnapMirror y el número de copias de Snapshot que se retendrán (período de retención).

Crear volúmenes de destino

Para crear un volumen de destino en FSX que será el destinatario de copias Snapshot de nuestros volúmenes de origen, ejecute el siguiente comando en FSX ONTAP:

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

Crear las relaciones de SnapMirror entre los volúmenes de origen y de destino

Para crear una relación de SnapMirror entre un volumen de origen y de destino, ejecute el siguiente comando en la ONTAP de FSX:

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

Inicializar las relaciones de SnapMirror

Inicialice la relación de SnapMirror. Este proceso inicia una snapshot nueva generada del volumen de origen y la copia al volumen de destino.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Implemente y configure servidores de Windows SnapCenter localmente.

Ponga en marcha Windows SnapCenter Server en las instalaciones

Esta solución utiliza SnapCenter de NetApp para realizar backups coherentes con las aplicaciones de bases de datos de SQL Server y Oracle. Junto con Veeam Backup & Replication para realizar backups de VMDK de máquinas virtuales, esto ofrece una completa solución de recuperación ante desastres para centros de datos en las instalaciones y basados en cloud.

El software SnapCenter está disponible en el sitio de soporte de NetApp y se puede instalar en sistemas Microsoft Windows que residan en un dominio o un grupo de trabajo. Encontrará una guía de planificación detallada e instrucciones de instalación en la "Centro de documentación de NetApp".

El software SnapCenter puede obtenerse en "este enlace".

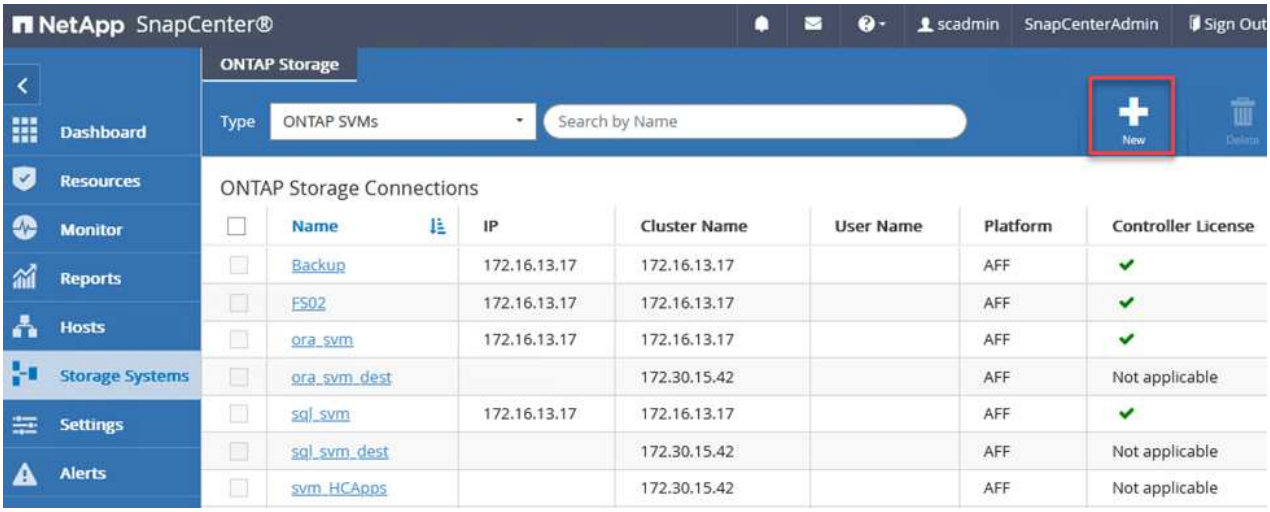
Una vez instalado, puede acceder a la consola SnapCenter desde un explorador Web utilizando *https://Virtual_Cluster_IP_or_FQDN:8146*.

Después de iniciar sesión en la consola, debe configurar SnapCenter para las bases de datos de SQL Server y Oracle.

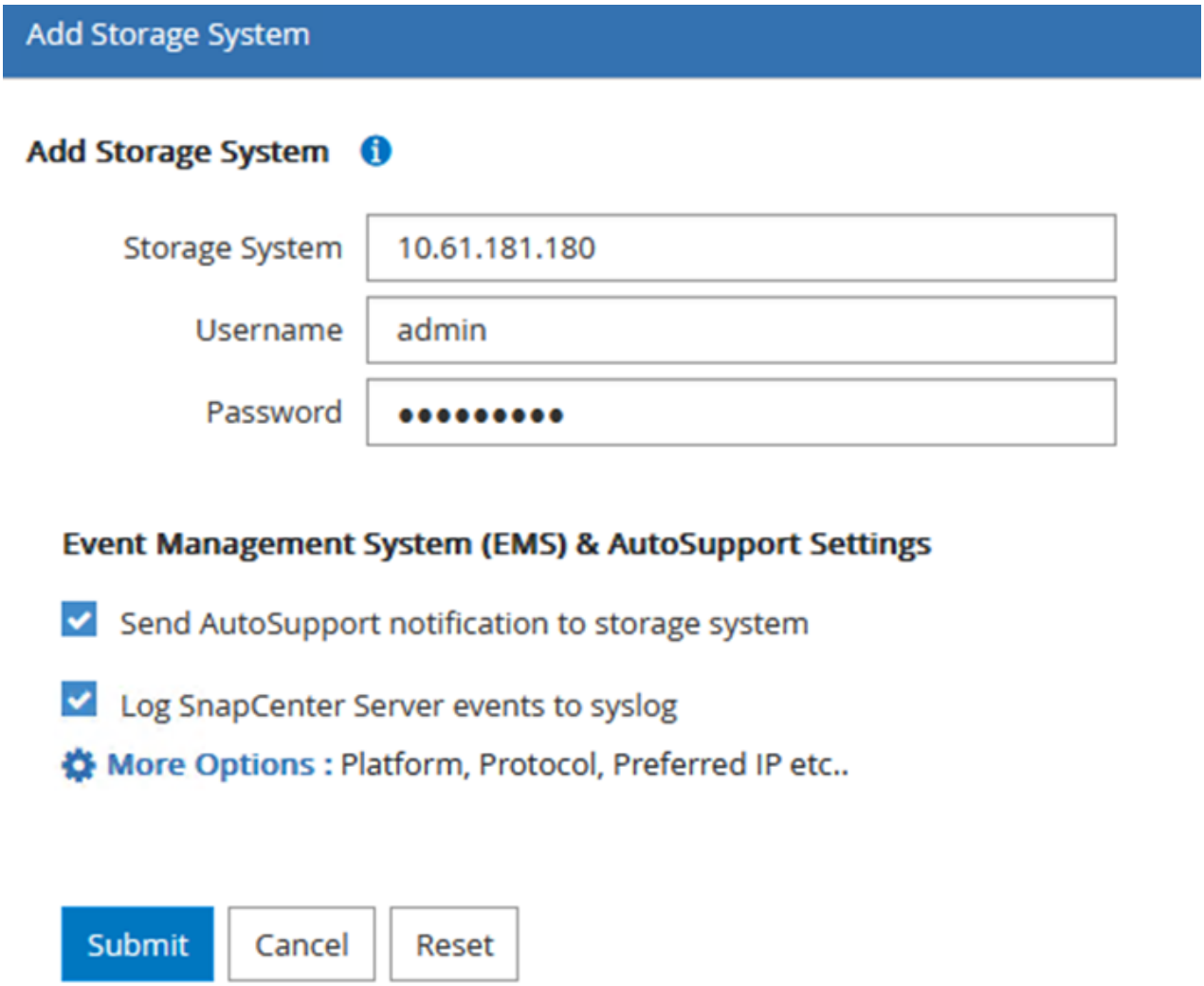
Añada controladoras de almacenamiento a SnapCenter

Para añadir controladoras de almacenamiento a SnapCenter, complete los siguientes pasos:

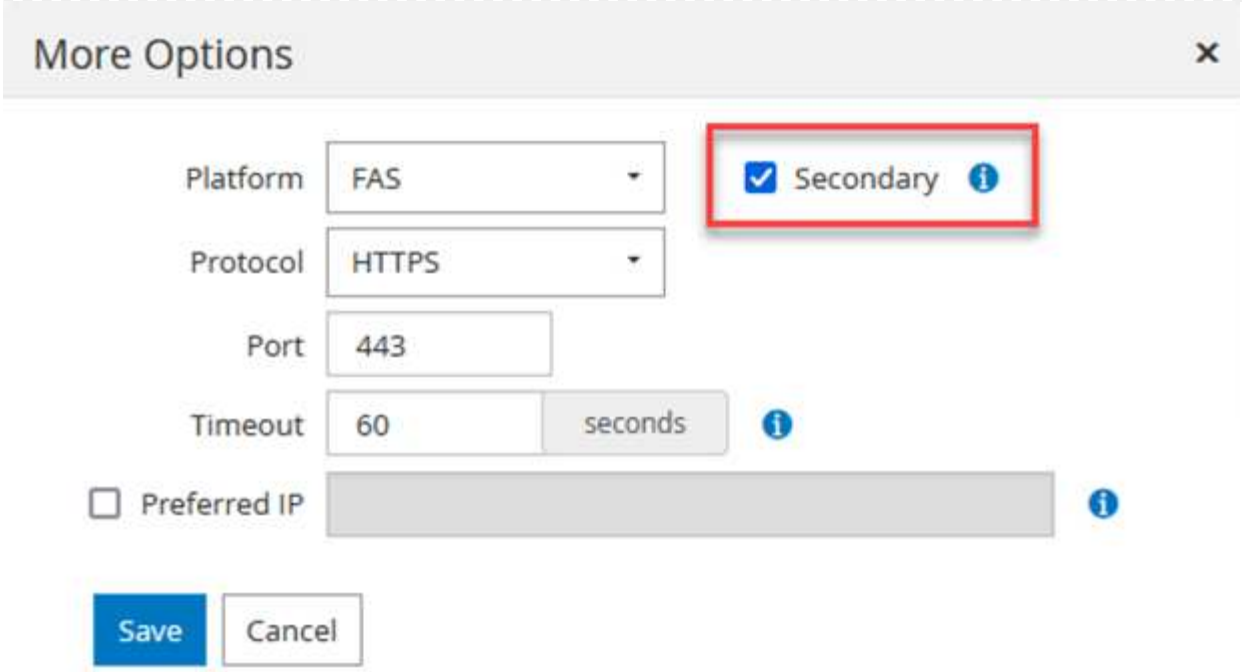
1. En el menú de la izquierda, seleccione Storage Systems y haga clic en New para comenzar el proceso de adición de controladoras de almacenamiento a SnapCenter.



2. En el cuadro de diálogo Add Storage System, añada la dirección IP de gestión para el clúster de ONTAP en las instalaciones locales, y el nombre de usuario y la contraseña. A continuación, haga clic en Submit para iniciar la detección del sistema de almacenamiento.



3. Repita este proceso para agregar el sistema FSX ONTAP a SnapCenter. En este caso, seleccione más opciones en la parte inferior de la ventana Add Storage System y haga clic en la casilla de comprobación for Secondary para designar el sistema FSX como sistema de almacenamiento secundario actualizado con copias SnapMirror o nuestras copias Snapshot de backup principales.

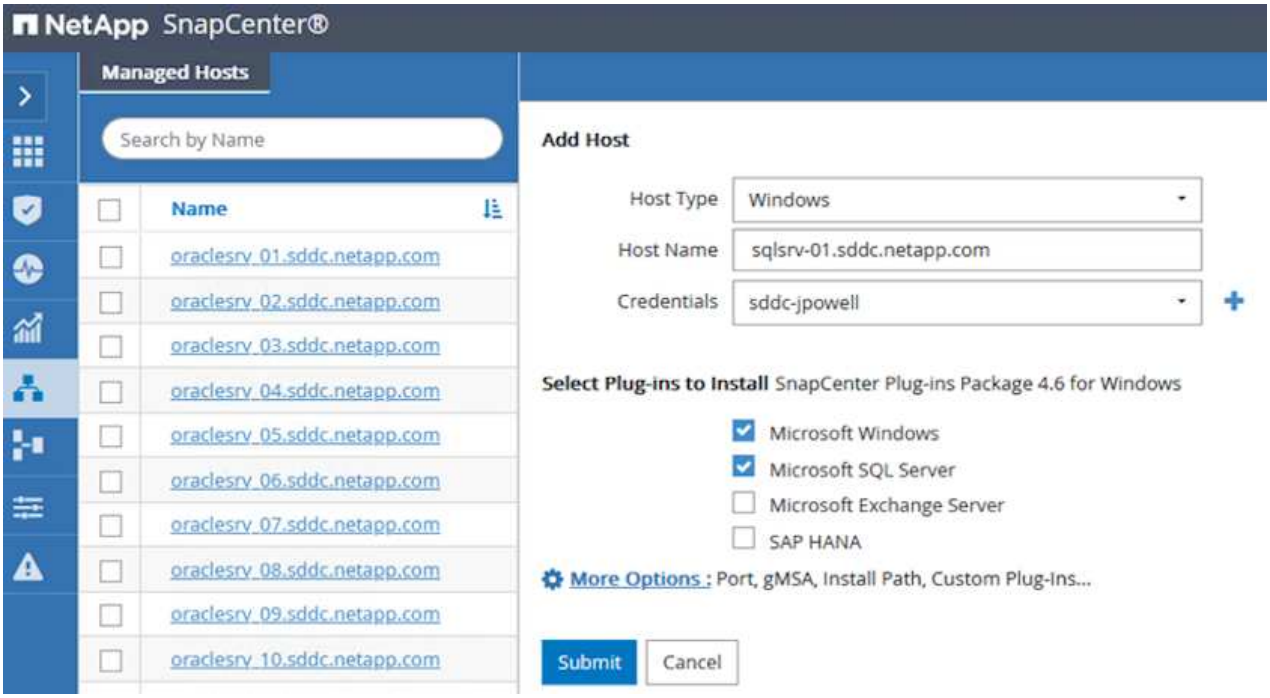


Para obtener más información relacionada con la adición de sistemas de almacenamiento a SnapCenter, consulte la documentación en "este enlace".

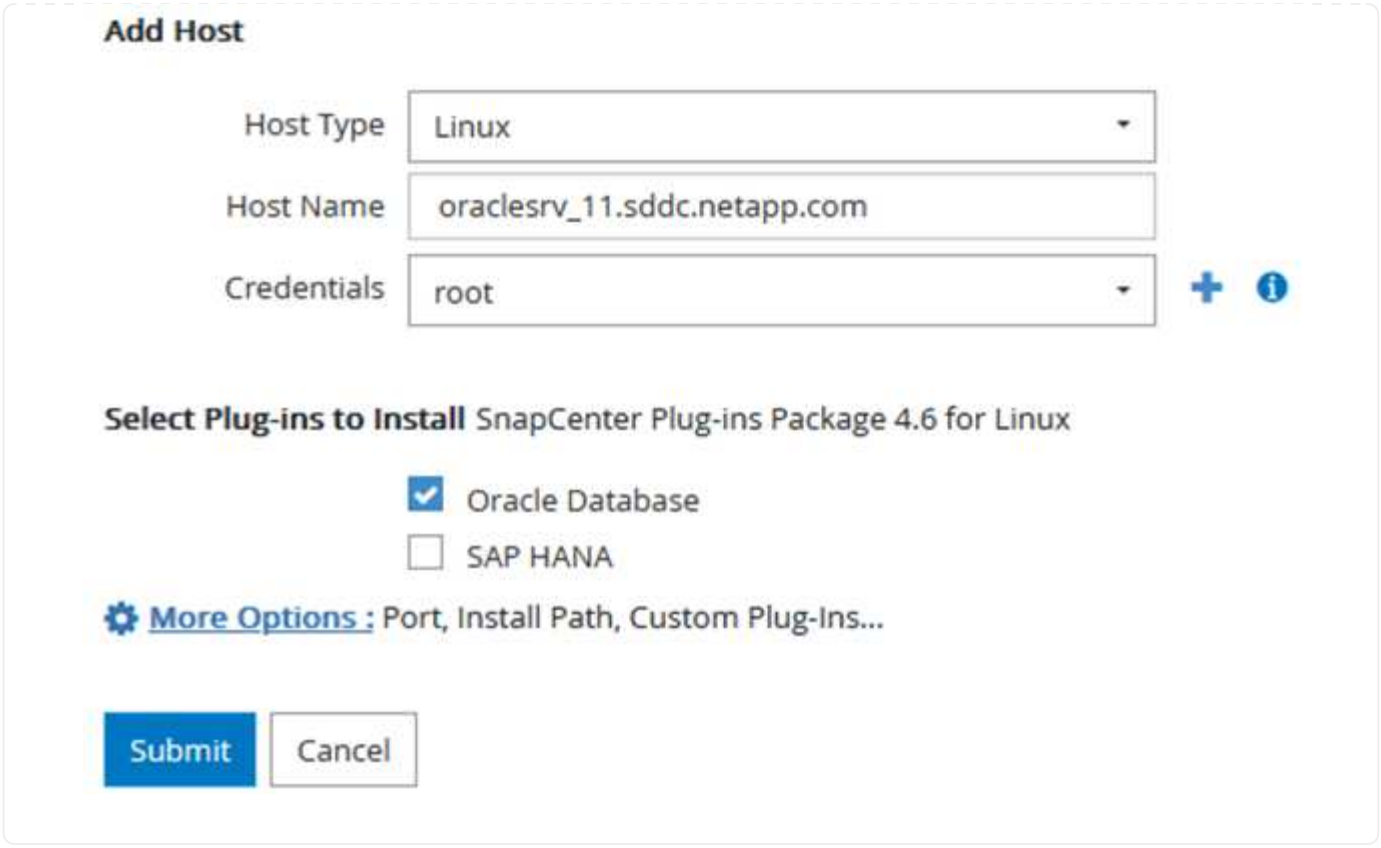
Añada hosts a SnapCenter

El siguiente paso es agregar servidores de aplicaciones host a SnapCenter. El proceso es similar tanto para SQL Server como para Oracle.

1. En el menú de la izquierda, seleccione hosts y haga clic en Añadir para comenzar el proceso de añadir controladoras de almacenamiento a SnapCenter.
2. En la ventana Add hosts, añada el tipo de host, el nombre de host y las credenciales del sistema host. Seleccione el tipo de plugin. Para SQL Server, seleccione el plugin para Microsoft Windows y Microsoft SQL Server.



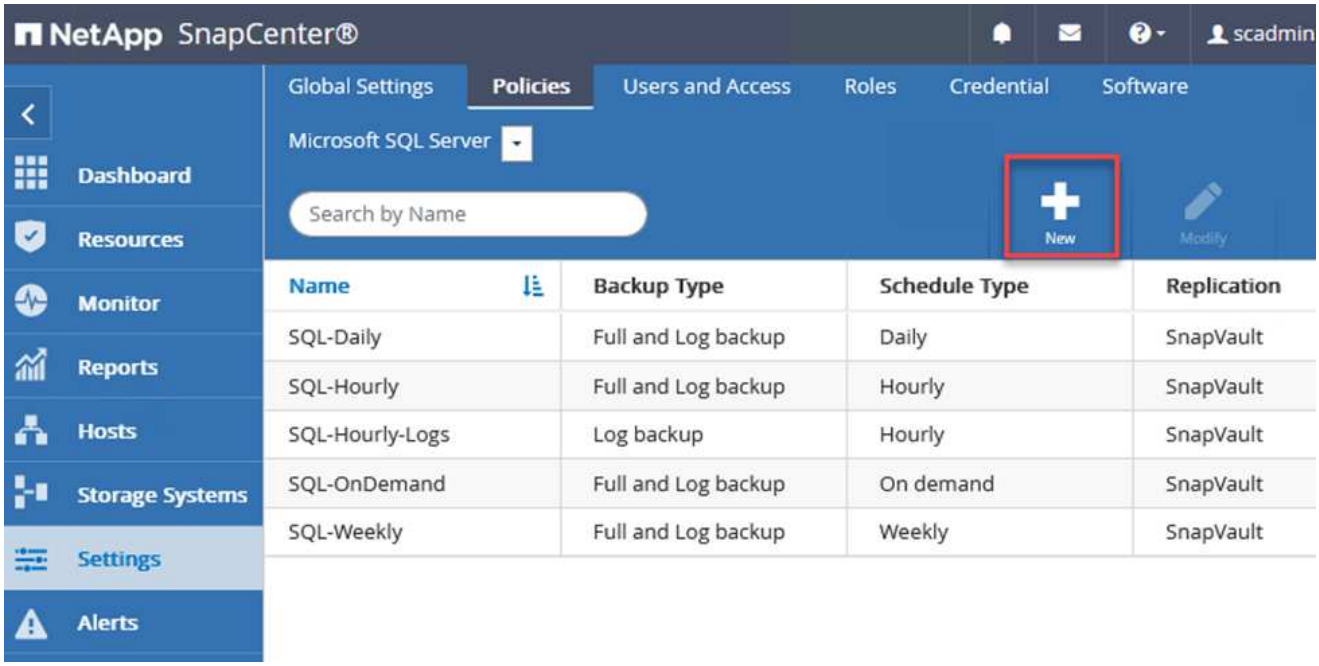
3. Para Oracle, rellene los campos obligatorios en el cuadro de diálogo Add Host y seleccione la casilla de comprobación del plugin de base de datos de Oracle. A continuación, haga clic en Enviar para iniciar el proceso de detección y añadir el host a SnapCenter.


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

Crear políticas de SnapCenter

Las políticas establecen las reglas específicas que se deben seguir para una tarea de backup. Incluyen, entre otros, la programación de backup, el tipo de replicación y cómo SnapCenter realiza el backup y los truncamiento de transacciones.

Puede acceder a las políticas en la sección Configuración del cliente web de SnapCenter.



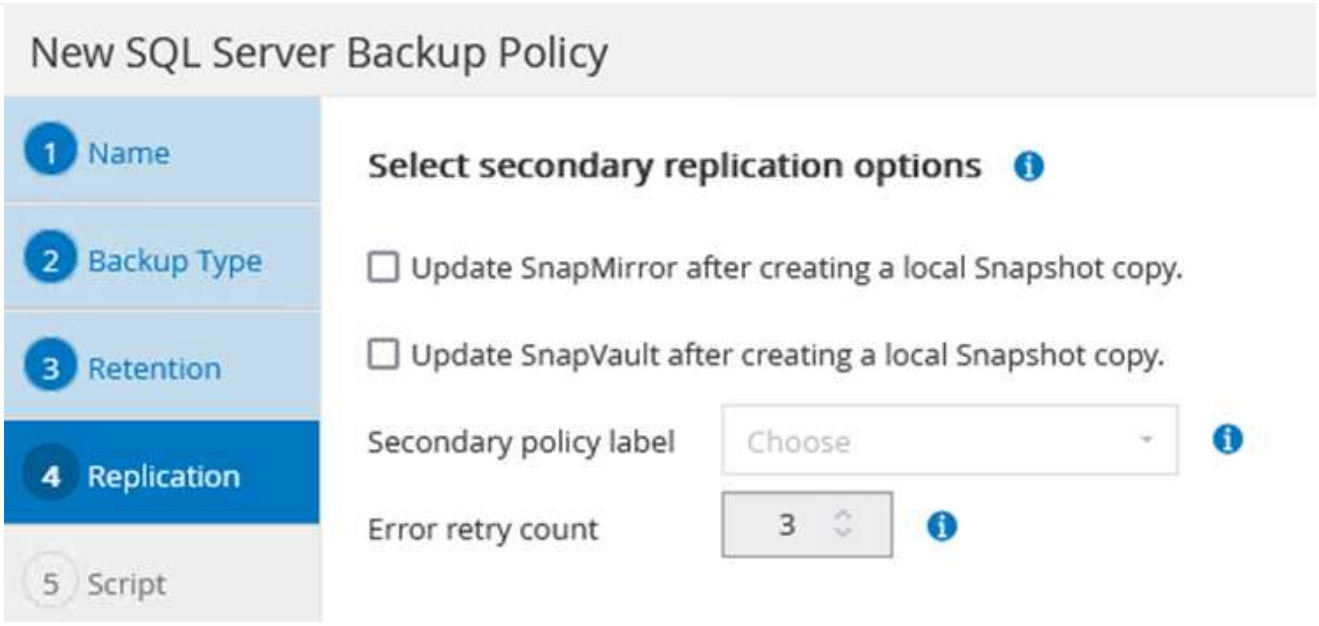
Para obtener información completa sobre la creación de políticas para backups de SQL Server, consulte "Documentación de SnapCenter".

Para obtener toda la información sobre la creación de políticas para backups de Oracle, consulte "Documentación de SnapCenter".

Notas:

- A medida que avanza por el asistente de creación de políticas, tenga una nota especial de la sección Replication. En esta sección, usted establece los tipos de copias secundarias de SnapMirror que desea realizar durante el proceso de backup.
- La configuración "Actualizar SnapMirror después de crear una copia Snapshot local" hace referencia a la actualización de una relación de SnapMirror cuando esa relación existe entre dos máquinas virtuales de almacenamiento que residen en el mismo clúster.
- La opción “Actualizar SnapVault después de crear una copia snapshot local” se utiliza para actualizar una relación de SnapMirror que existe entre dos clústeres independientes y entre un sistema ONTAP local y Cloud Volumes ONTAP o FSxN.

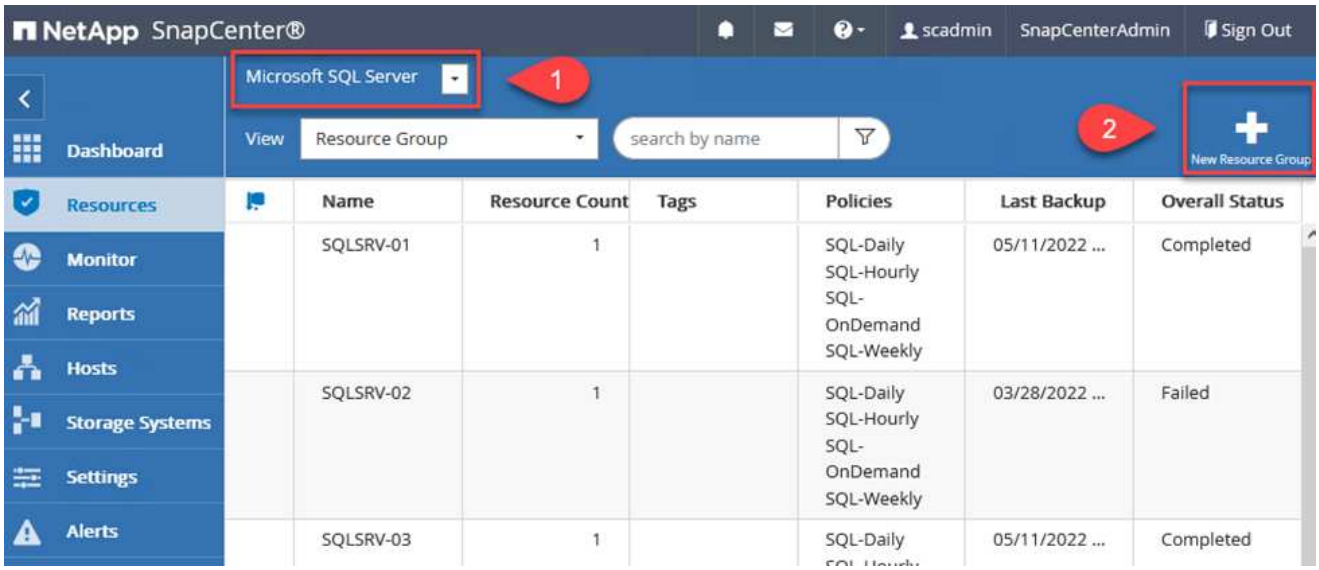
En la siguiente imagen, se muestran las opciones anteriores y su aspecto en el asistente de política de backup.



Crear grupos de recursos de SnapCenter

Los grupos de recursos permiten seleccionar los recursos de la base de datos que desea incluir en los backups y las políticas aplicadas a esos recursos.

1. Vaya a la sección Recursos del menú de la izquierda.
2. En la parte superior de la ventana, seleccione el tipo de recurso con el que trabajar (en este caso Microsoft SQL Server) y, a continuación, haga clic en Nuevo grupo de recursos.



La documentación de SnapCenter recoge detalles paso a paso para crear grupos de recursos para bases de datos de SQL Server y Oracle.

Para realizar backups de recursos de SQL, siga "este enlace".

Para realizar backups de recursos de Oracle, siga "este enlace".

Ponga en marcha y configure Veeam Backup Server

La solución utiliza el software Veeam Backup & Replication para realizar backups de nuestros equipos virtuales de aplicaciones y archivar una copia de los backups en un bloque de Amazon S3 mediante un repositorio de backup de escalado horizontal (SOBR) de Veeam. Veeam se pone en marcha en servidores Windows como parte de esta solución. Para obtener directrices específicas sobre la puesta en marcha de Veeam, consulte "Documentación técnica del centro de ayuda de Veeam".

Configurar el repositorio de backup de escalado horizontal de Veeam

Después de implementar y obtener licencias del software, puede crear un repositorio de backup de escalado horizontal (SOBR) como almacenamiento de destino para tareas de backup. También debería incluir un bloque de S3 como backup de datos de máquinas virtuales fuera de sus instalaciones para la recuperación ante desastres.

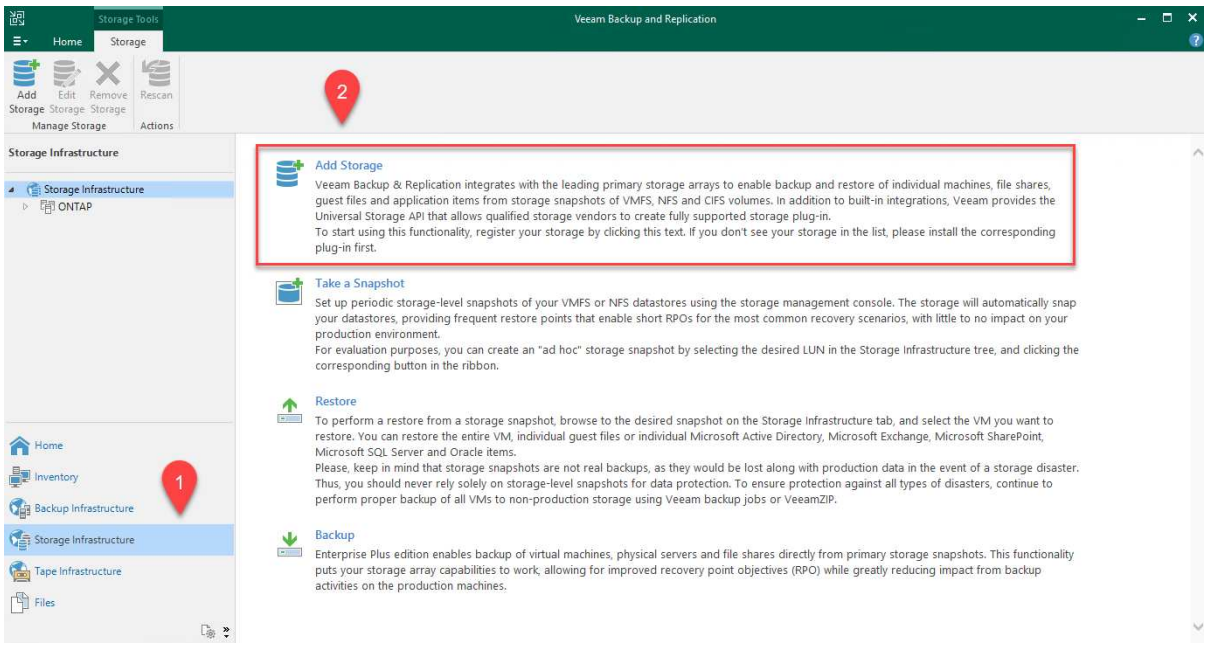
Consulte los siguientes requisitos previos antes de comenzar.

1. Cree un recurso compartido de archivos SMB en su sistema ONTAP local como almacenamiento objetivo para backups.
2. Cree un bloque de Amazon S3 para incluirlo en el SBR. Este es un repositorio para los backups fuera de las instalaciones.

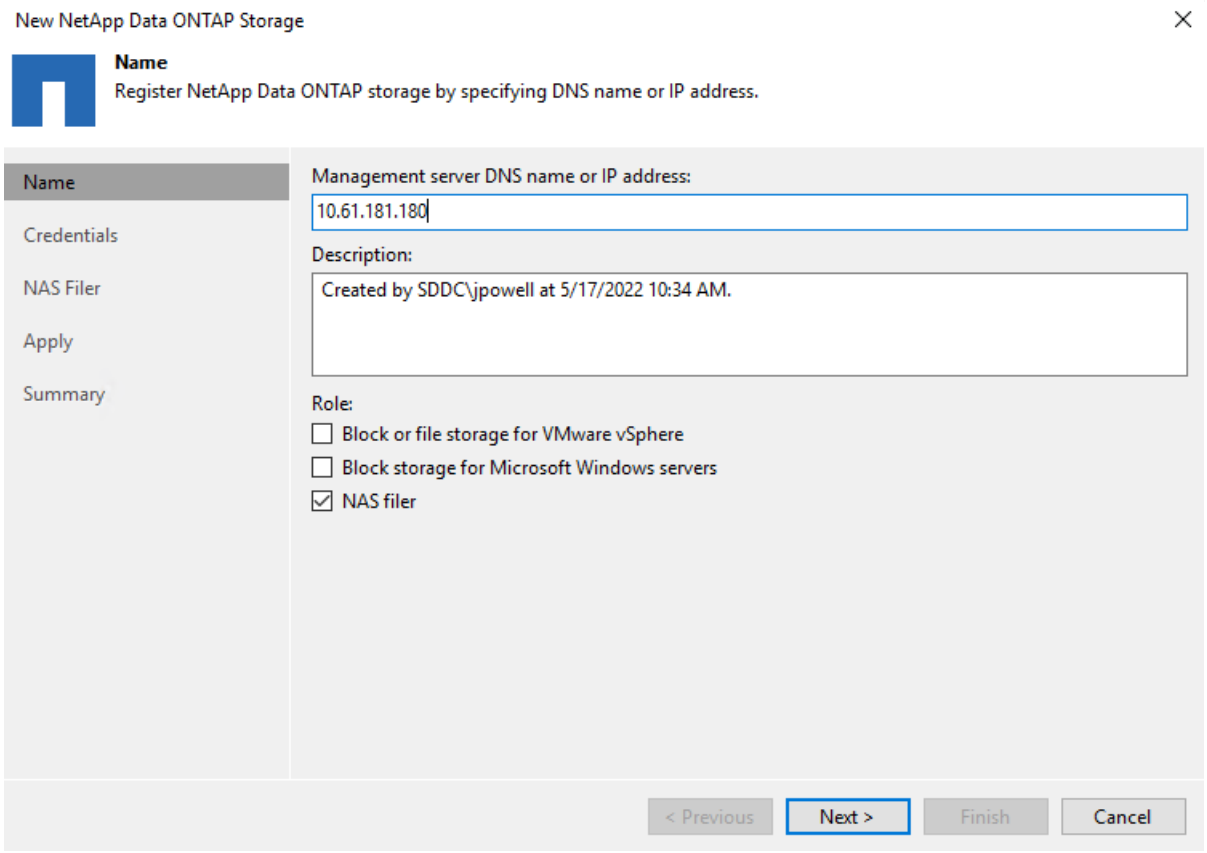
Añada el almacenamiento de ONTAP a Veeam

En primer lugar, añada el clúster de almacenamiento de ONTAP y el sistema de archivos SMB/NFS asociado como infraestructura de almacenamiento en Veeam.

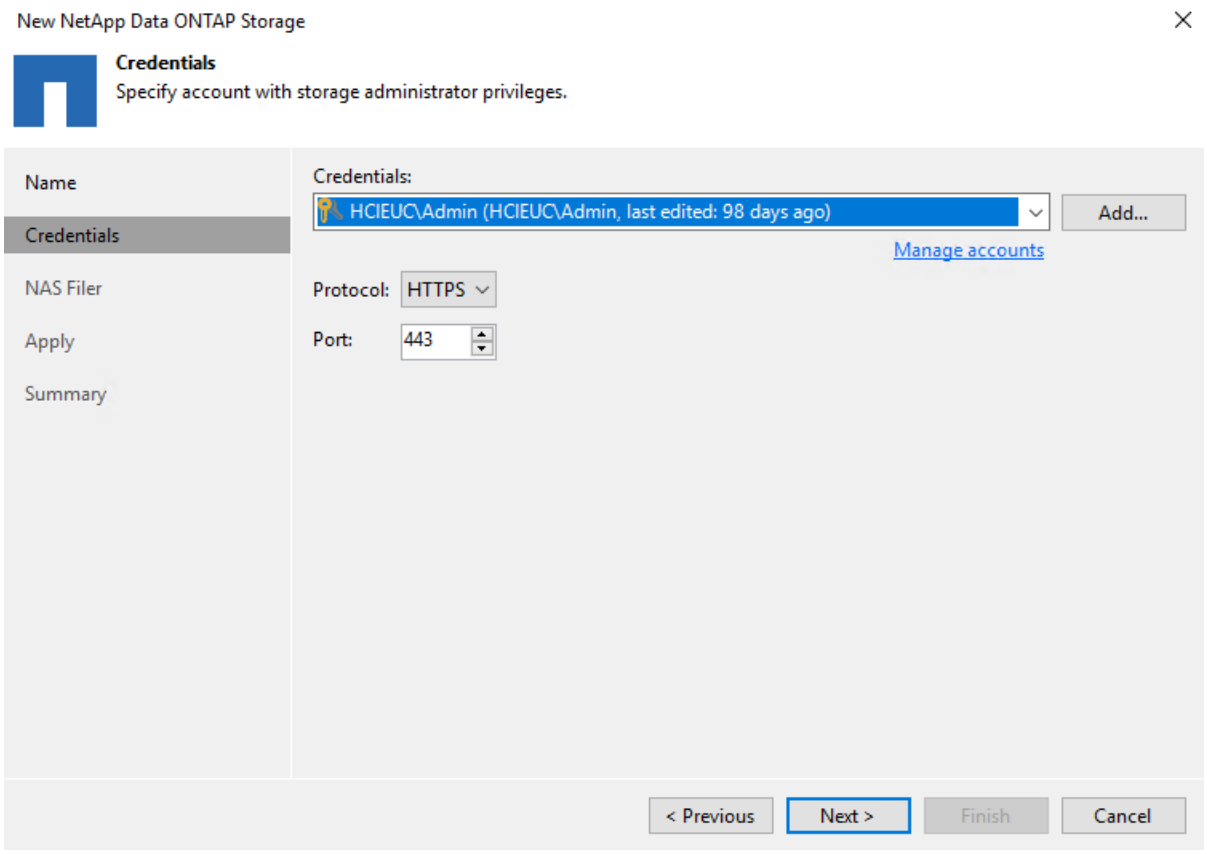
1. Abra la consola de Veeam e inicie sesión. Vaya a Storage Infrastructure y seleccione Add Storage.



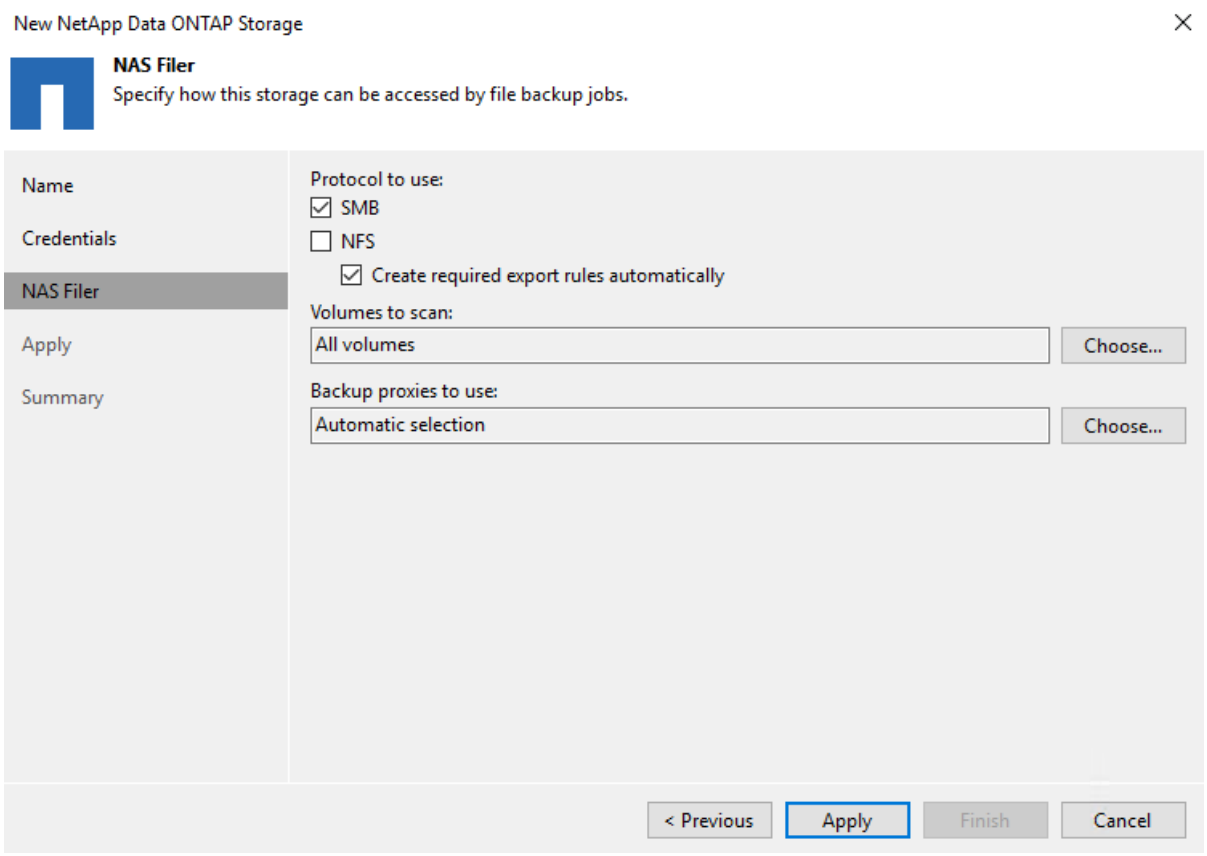
2. En el asistente Add Storage, seleccione NetApp como proveedor de almacenamiento y, a continuación, seleccione Data ONTAP.
3. Introduzca la dirección IP de administración y active la casilla de verificación servidor dedicado a almacenamiento NAS. Haga clic en Siguiente.



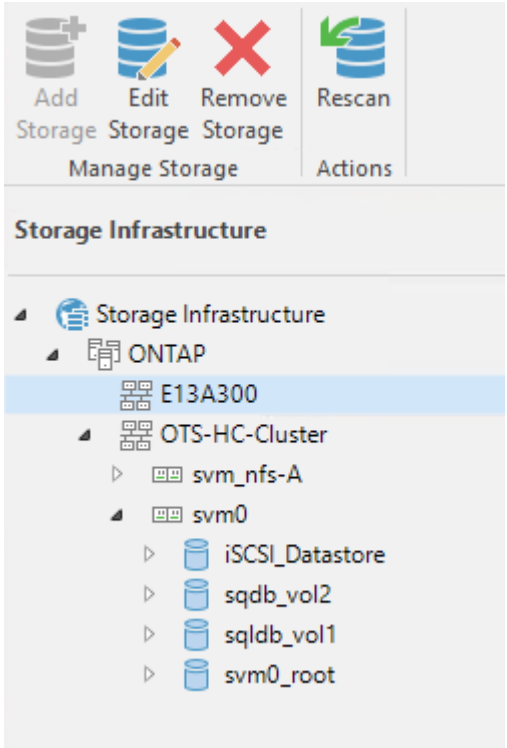
4. Añada sus credenciales para acceder al clúster de ONTAP.



5. En la página NAS Filer, elija los protocolos que desea analizar y seleccione Next.

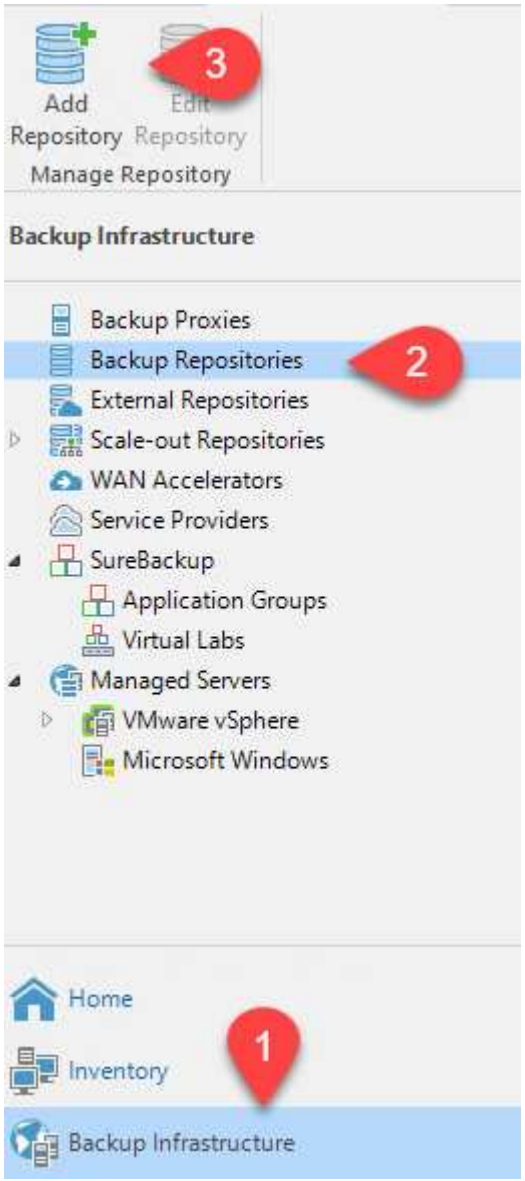


6. Complete las páginas Apply y Summary del asistente y haga clic en Finish para iniciar el proceso de detección de almacenamiento. Una vez finalizada la exploración, se añade el clúster ONTAP junto con los servidores dedicados a almacenamiento NAS como recursos disponibles.

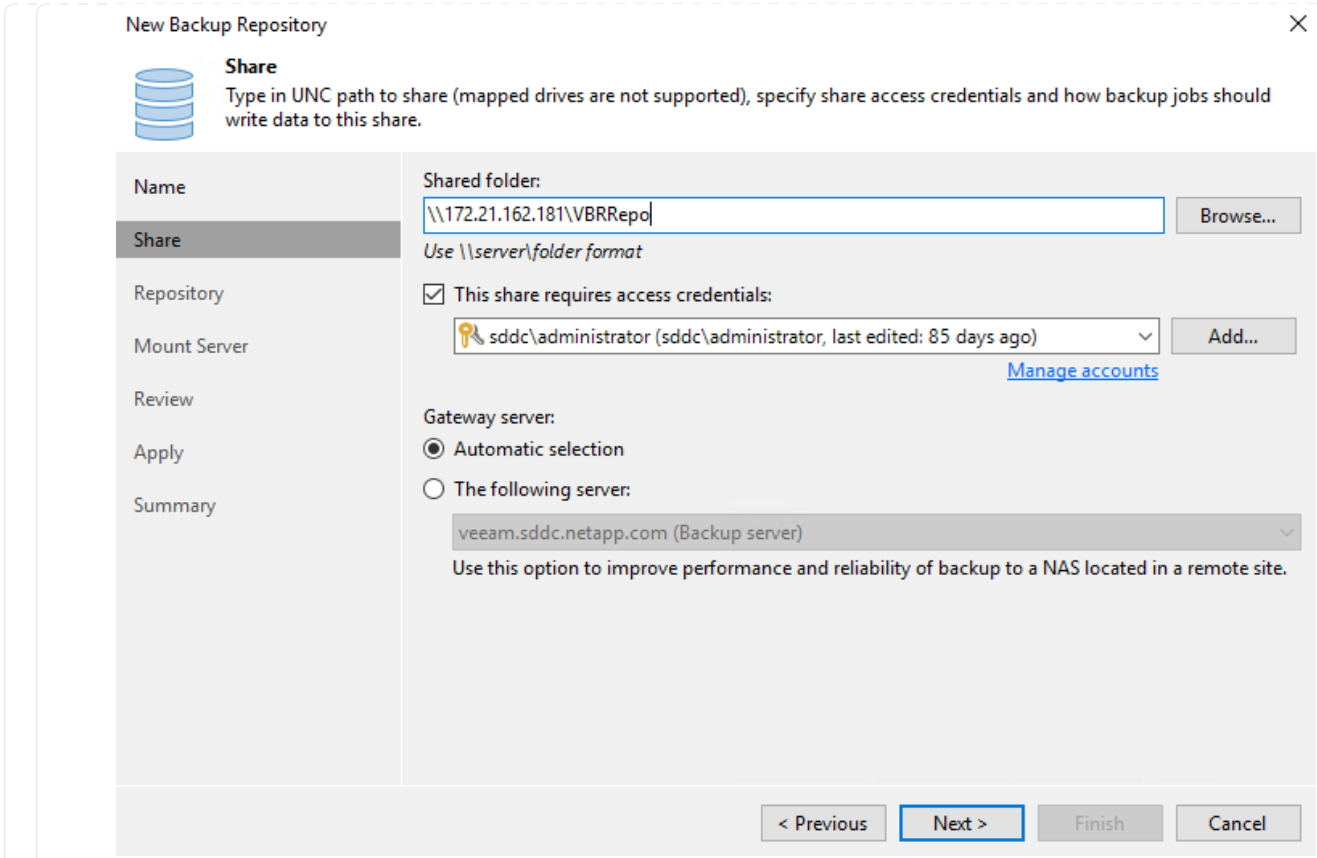


7. Cree un repositorio de backup con los recursos compartidos NAS recién detectados. En Infraestructura de copia de seguridad, seleccione repositorios de copia de seguridad y haga clic

en el elemento de menú Agregar repositorio.



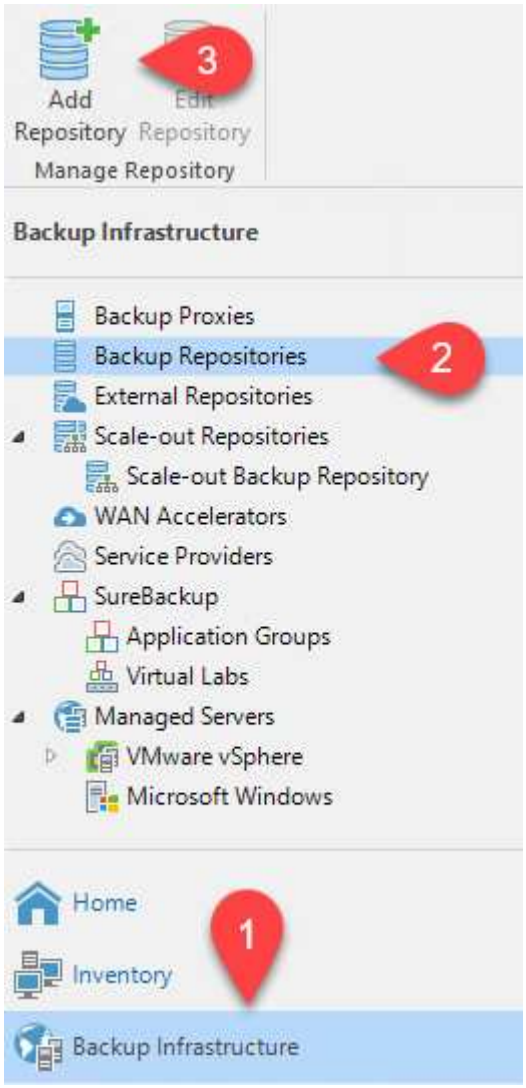
8. Siga todos los pasos del Asistente para crear un repositorio de copia de seguridad nuevo para crear el repositorio. Para obtener información detallada sobre la creación de repositorios de Veeam Backup, consulte "Documentación de Veeam".


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

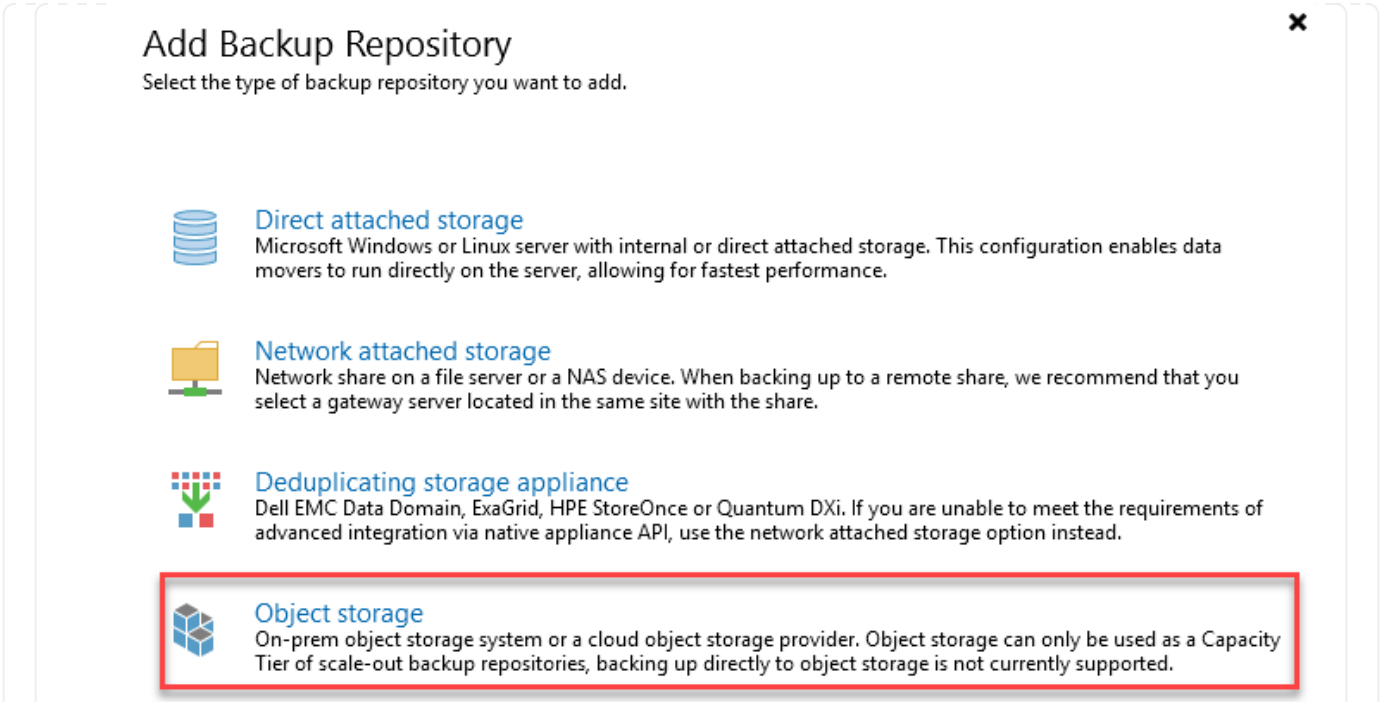
Añada el bloque de Amazon S3 como repositorio de backup

El paso siguiente es añadir el almacenamiento Amazon S3 como repositorio de backup.

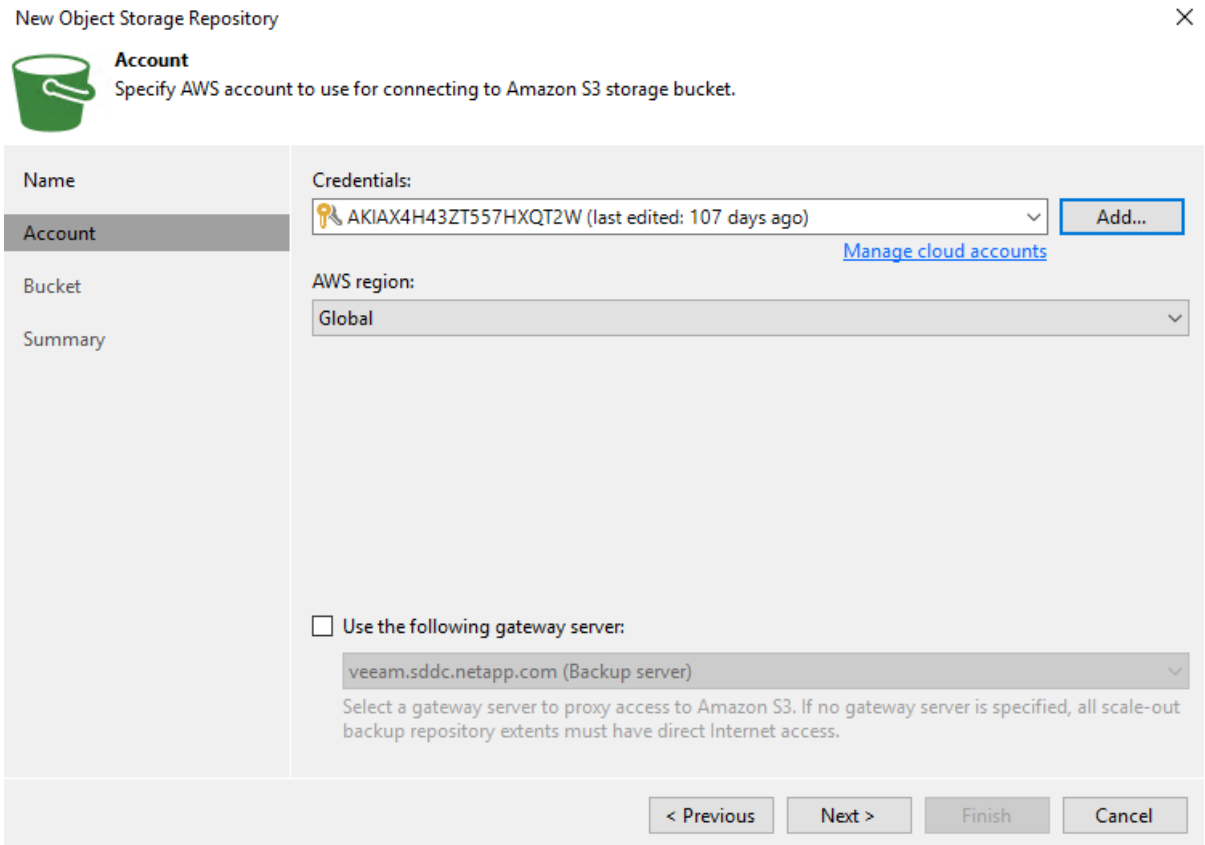
1. Vaya a Backup Infrastructure > repositorios de backup. Haga clic en Add Repository.



2. En el asistente Add Backup Repository, seleccione Object Storage y, a continuación, Amazon S3. Esto inicia el asistente Nuevo repositorio de almacenamiento de objetos.



3. Proporcione un nombre para el repositorio de almacenamiento de objetos y haga clic en Next.
4. En la siguiente sección, introduzca sus credenciales. Necesita una clave de acceso de AWS y una clave secreta.

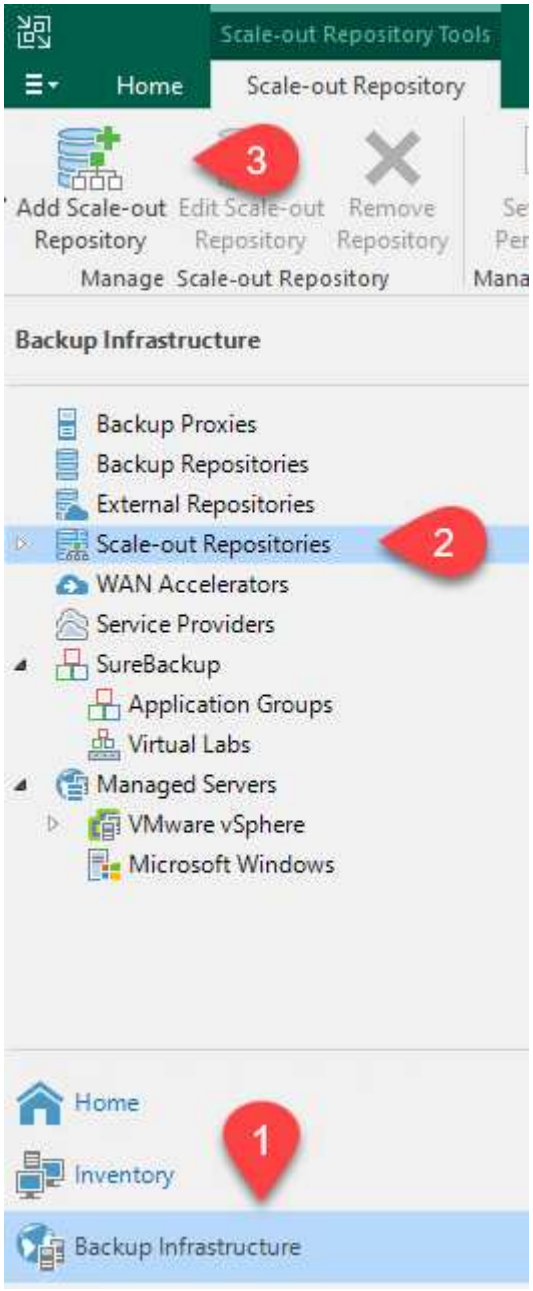


5. Una vez que se haya cargado la configuración de Amazon, seleccione su centro de datos, bloque y carpeta y haga clic en Apply. Por último, haga clic en Finalizar para cerrar el asistente.

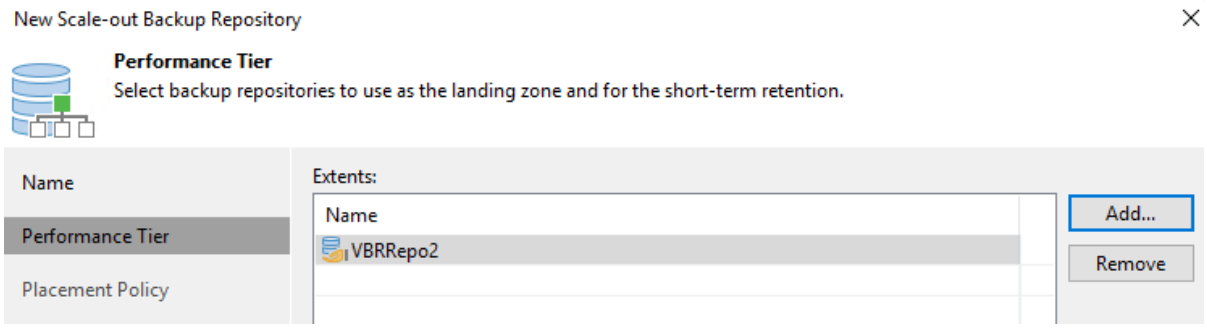
Cree un repositorio de backup de escalado horizontal

Ahora que hemos añadido nuestros repositorios de almacenamiento a Veeam, podemos crear el SOBR para organizar automáticamente en niveles las copias de backup en nuestro almacenamiento de objetos Amazon S3 externo para la recuperación ante desastres.

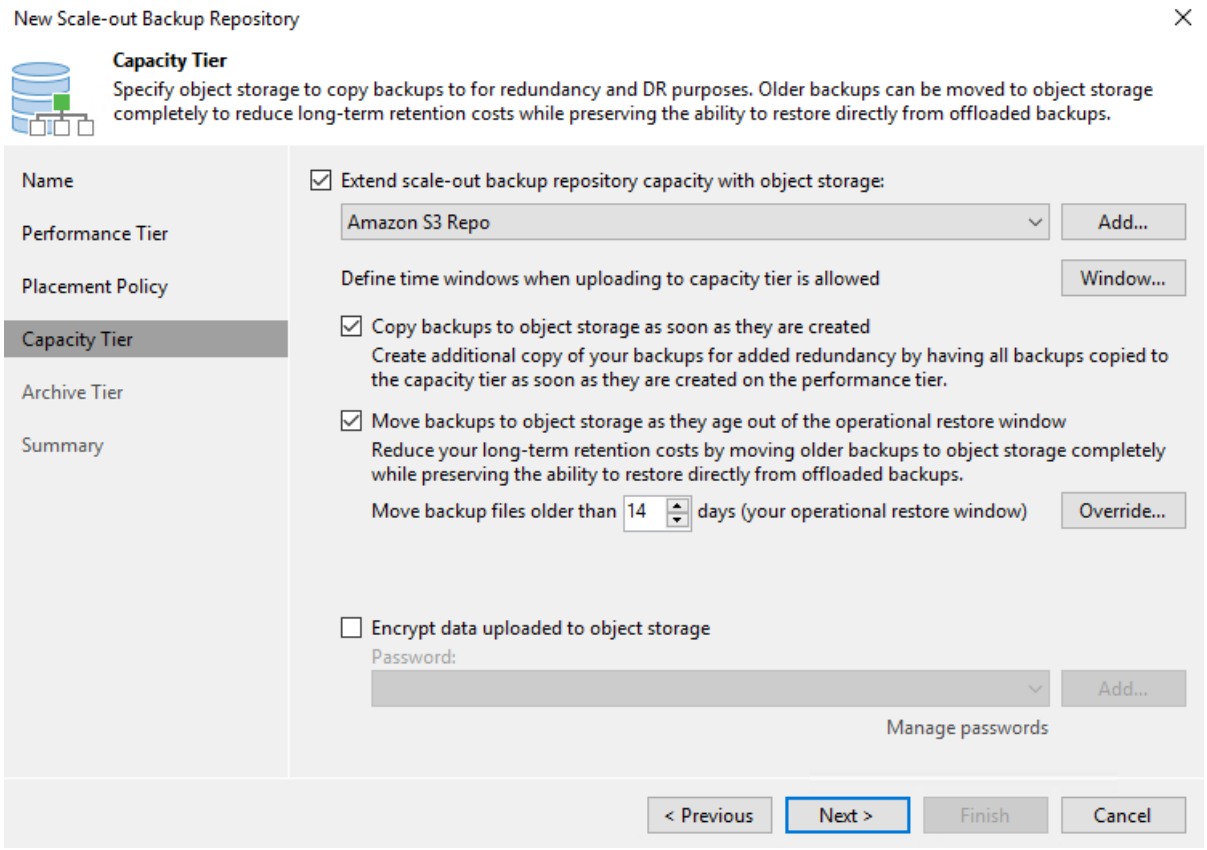
1. En Backup Infrastructure, seleccione repositorios de escalado horizontal y, a continuación, haga clic en el elemento de menú Add Scale-Out Repository.



2. En el nuevo repositorio de copia de seguridad de escalado horizontal, proporcione un nombre para SOBR y haga clic en Siguiente.
3. Para el nivel de rendimiento, elija el repositorio de backup que contiene el recurso compartido de SMB que reside en el clúster de ONTAP local.



4. Para la Política de colocación, elija la ubicación de los datos o el rendimiento en función de sus requisitos. Seleccione Siguiente.
5. Para el nivel de capacidad, hemos ampliado el SOBR con el almacenamiento de objetos Amazon S3. Para la recuperación ante desastres, seleccione Copy backups to Object Storage tan pronto como se creen para garantizar una entrega puntual de nuestros backups secundarios.



6. Por último, seleccione aplicar y Finalizar para finalizar la creación del SORR.

Crear las tareas del repositorio de backup de escalado horizontal

El paso final para configurar Veeam es crear tareas de backup utilizando el SOBR recién creado como destino del backup. La creación de empleos de respaldo es una parte normal del repertorio de cualquier administrador de almacenamiento y no cubrimos los pasos detallados aquí. Si desea obtener más información acerca de la creación de trabajos de backup en Veeam, consulte "Documentación técnica del centro de ayuda de Veeam".

Configuración y herramientas de backup y recuperación de BlueXP

Para llevar a cabo una conmutación al nodo de respaldo de los equipos virtuales de aplicación y los volúmenes de base de datos en los servicios de VMware Cloud Volume que se ejecutan en AWS, debe instalar y configurar una instancia en ejecución tanto de SnapCenter Server como de Veeam Backup and Replication Server. Una vez finalizada la conmutación al respaldo, también debe configurar estas herramientas para reanudar las operaciones de backup normales hasta que se haya planificado y ejecutado una conmutación tras recuperación al centro de datos en las instalaciones.

Implemente un servidor SnapCenter secundario de Windows

El servidor SnapCenter se pone en marcha en VMware Cloud SDDC o se instala en una instancia EC2 que reside en un VPC con conectividad de red al entorno cloud de VMware.

El software SnapCenter está disponible en el sitio de soporte de NetApp y se puede instalar en sistemas Microsoft Windows que residan en un dominio o un grupo de trabajo. Encontrará una guía de planificación detallada e instrucciones de instalación en la "Centro de documentación de NetApp".

Puede encontrar el software de SnapCenter en "este enlace".

Configurar servidor SnapCenter secundario de Windows

Para realizar una restauración de datos de aplicación reflejados en FSX ONTAP, primero debe realizar una restauración completa de la base de datos de SnapCenter local. Una vez completado este proceso, se restablece la comunicación con los equipos virtuales y los backups de aplicaciones pueden reanudarse usando FSX ONTAP como almacenamiento principal.

Para ello, debe completar los siguientes elementos en el servidor SnapCenter:

1. Configure el nombre del equipo para que sea idéntico al servidor SnapCenter local original.
2. Configure las redes para comunicarse con VMware Cloud y la instancia de FSX ONTAP.
3. Complete el procedimiento para restaurar la base de datos de SnapCenter.
4. Confirmar que SnapCenter se encuentra en el modo de recuperación ante desastres para garantizar que FSX es ahora el almacenamiento principal de los backups.
5. Confirmar que se restablece la comunicación con las máquinas virtuales restauradas.

Para obtener más información sobre cómo completar estos pasos, consulte la sección "Proceso de restauración de bases de datos de SnapCenter".

Ponga en marcha el servidor de replicación de & de Veeam secundario

Puede instalar el servidor de Veeam Backup & Replication en un servidor de Windows en el cloud de VMware en AWS o en una instancia de EC2. Para obtener instrucciones detalladas sobre la implementación, consulte "Documentación técnica del centro de ayuda de Veeam".

Configurar el servidor de replicación secundario de Veeam Backup &

Para realizar una restauración de máquinas virtuales cuyo backup se ha realizado en el almacenamiento de Amazon S3, debe instalar Veeam Server en un servidor Windows y configurarlo para comunicarse con VMware Cloud, FSX ONTAP y el bloque de S3 que contiene el repositorio de backup original. También debe tener un nuevo repositorio de backup configurado en FSX ONTAP para realizar nuevos backups de las máquinas virtuales después de restaurarlas.

Para realizar este proceso, deben completarse los siguientes elementos:

1. Configurar las redes para que se comuniquen con VMware Cloud, FSX ONTAP y el bloque de S3 que contiene el repositorio de backup original.
2. Configure un recurso compartido de SMB en FSX ONTAP y así sea un nuevo repositorio de backup.
3. Monte el bloque original de S3 que se utilizó como parte del repositorio de backup de escalado horizontal en las instalaciones.
4. Después de restaurar la máquina virtual, establezca nuevas tareas de backup para proteger las máquinas virtuales de SQL y Oracle.

Si desea obtener más información sobre la restauración de máquinas virtuales mediante Veeam, consulte la sección "Restaure equipos virtuales de aplicación con Veeam Full Restore".

Backup de la base de datos de SnapCenter para recuperación ante desastres

SnapCenter permite realizar las tareas de backup y recuperación de sus datos de configuración y base de datos MySQL subyacentes con el fin de recuperar el servidor SnapCenter en caso de desastre. Para nuestra solución, recuperamos la base de datos y la configuración de SnapCenter en una instancia de EC2 de AWS que reside en nuestro VPC. Para obtener más información sobre este paso, consulte "este enlace".

Requisitos previos de backup de SnapCenter

Se requieren los siguientes requisitos previos para el backup de SnapCenter:

- Se creó un volumen y un recurso compartido de SMB en el sistema ONTAP en las instalaciones para localizar los archivos de configuración y base de datos con backup.
- Una relación de SnapMirror entre el sistema ONTAP en las instalaciones y FSX o CVO en la cuenta de AWS. Esta relación se utiliza para transportar la snapshot que contiene la base de datos y los archivos de configuración de SnapCenter con backup.
- Windows Server instalado en la cuenta del cloud, ya sea en una instancia de EC2 o en una máquina virtual del centro de datos definido por software de VMware Cloud.
- SnapCenter instalado en la instancia o máquina virtual de EC2 de Windows en VMware Cloud.

Resumen del proceso de backup y restauración de SnapCenter

- Cree un volumen en el sistema ONTAP local para alojar la base de datos de copia de seguridad y los archivos de configuración.
- Configuración de una relación de SnapMirror entre on-premises y FSX/CVO.
- Monte el recurso compartido de SMB.
- Recupere el token de autorización de Swagger para realizar tareas de API.
- Inicie el proceso de restauración de la base de datos.
- Utilice la utilidad xcopy para copiar el directorio local de la base de datos y el archivo de configuración en el recurso compartido SMB.
- En FSX, cree un clon del volumen ONTAP (copiado mediante SnapMirror desde las instalaciones).
- Monte el recurso compartido de SMB de FSX a EC2/VMware Cloud.
- Copie el directorio de restauración del recurso compartido SMB en un directorio local.
- Ejecute el proceso de restauración de SQL Server desde Swagger.

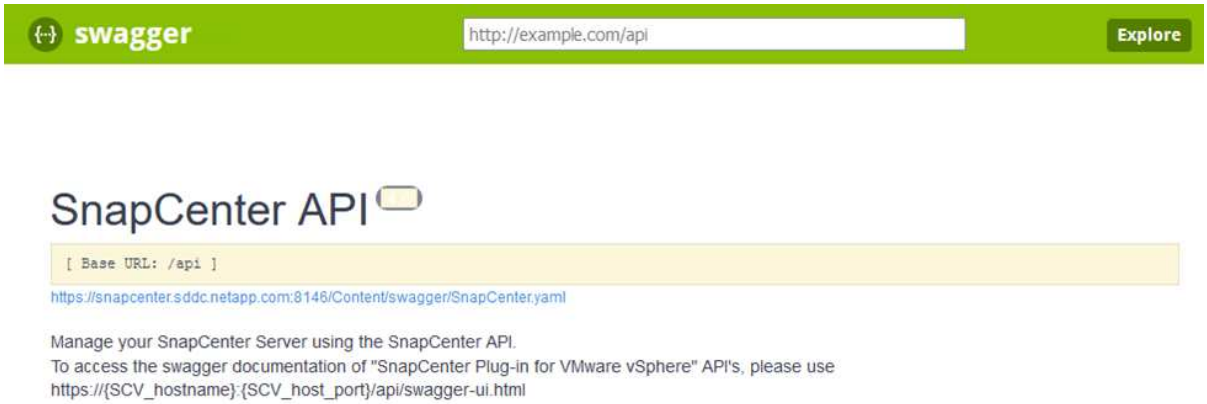
Realice un backup de la base de datos de SnapCenter y la configuración

SnapCenter proporciona una interfaz de cliente web para ejecutar comandos de la API DE REST. Para obtener información sobre cómo acceder a las API DE REST a través de Swagger, consulte la documentación de SnapCenter en "este enlace".

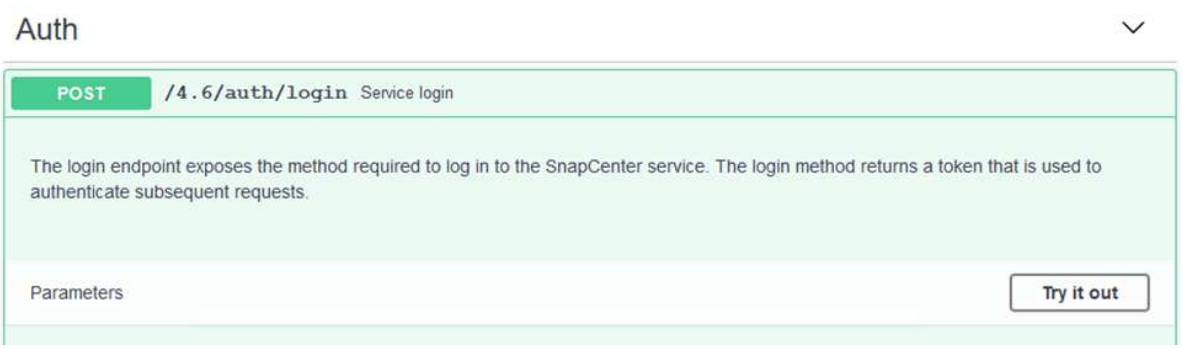
Inicie sesión en Swagger y obtenga el token de autorización

Después de navegar por la página de Swagger, debe recuperar un token de autorización para iniciar el proceso de restauración de base de datos.

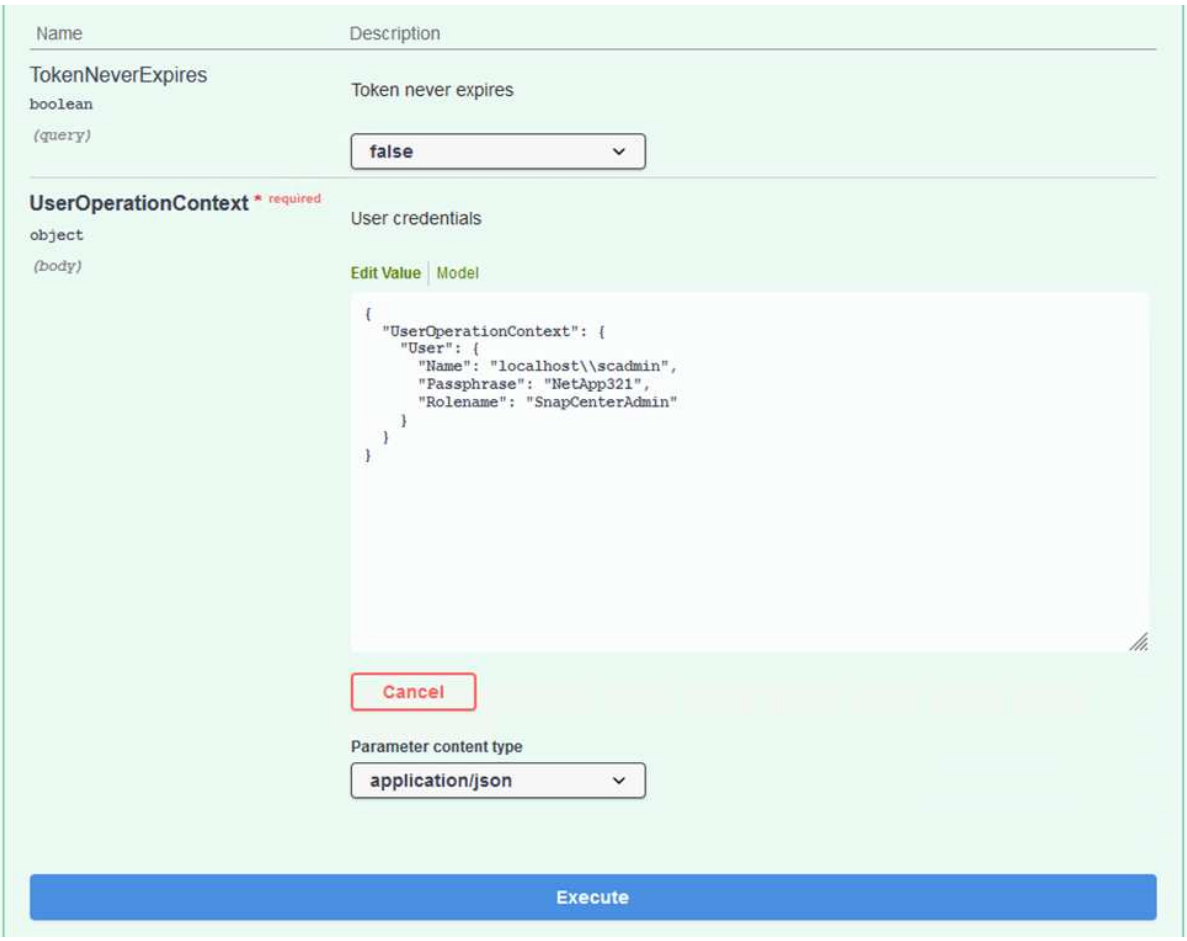
1. Acceda a la página web de API de SnapCenter Swagger en *https://<SnapCenter Server IP>:8146/swagger/*.



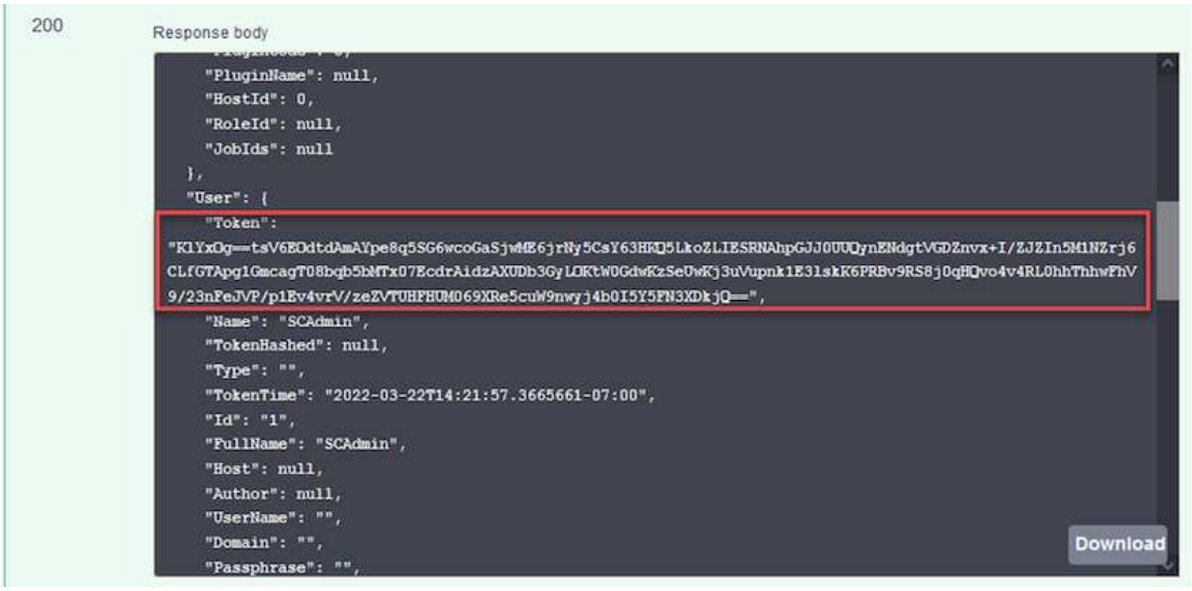
2. Expanda la sección Auth y haga clic en Inténtelo.



3. En el área UserOperationContext, rellene las credenciales y la función de SnapCenter y haga clic en Ejecutar.



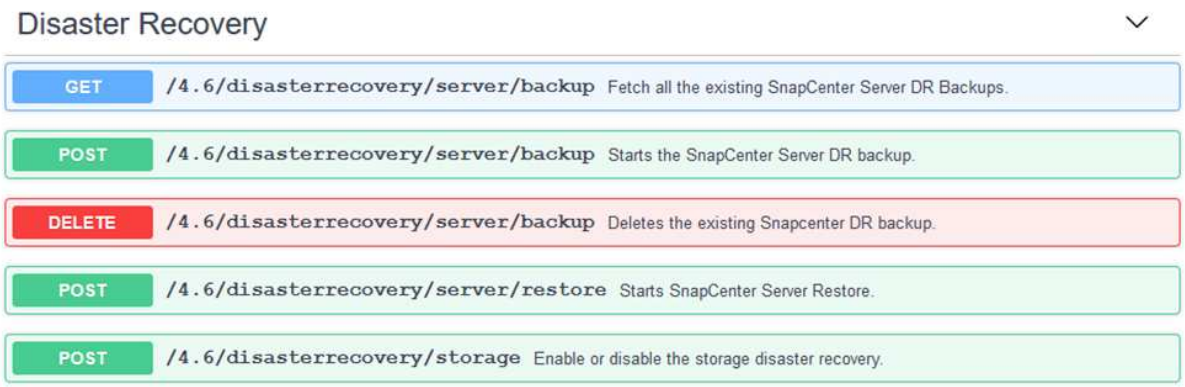
4. En el cuerpo de respuesta que aparece a continuación, puede ver el token. Copie el texto del token para la autenticación al ejecutar el proceso de backup.



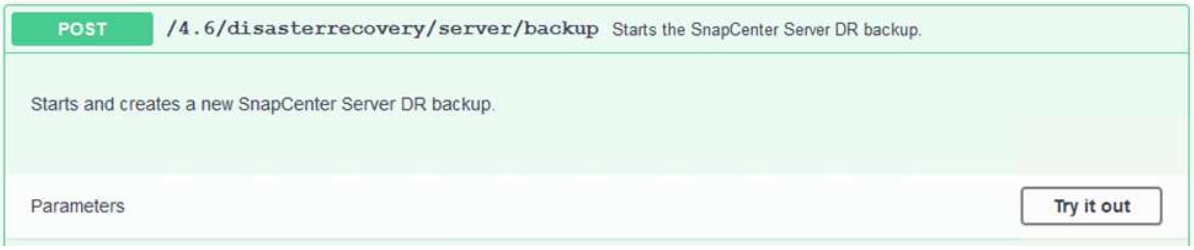
Realizar un backup de base de datos de SnapCenter

A continuación, vaya al área de recuperación ante desastres de la página Swagger para iniciar el proceso de backup de SnapCenter.

1. Expanda el área de recuperación ante desastres haciendo clic en ella.

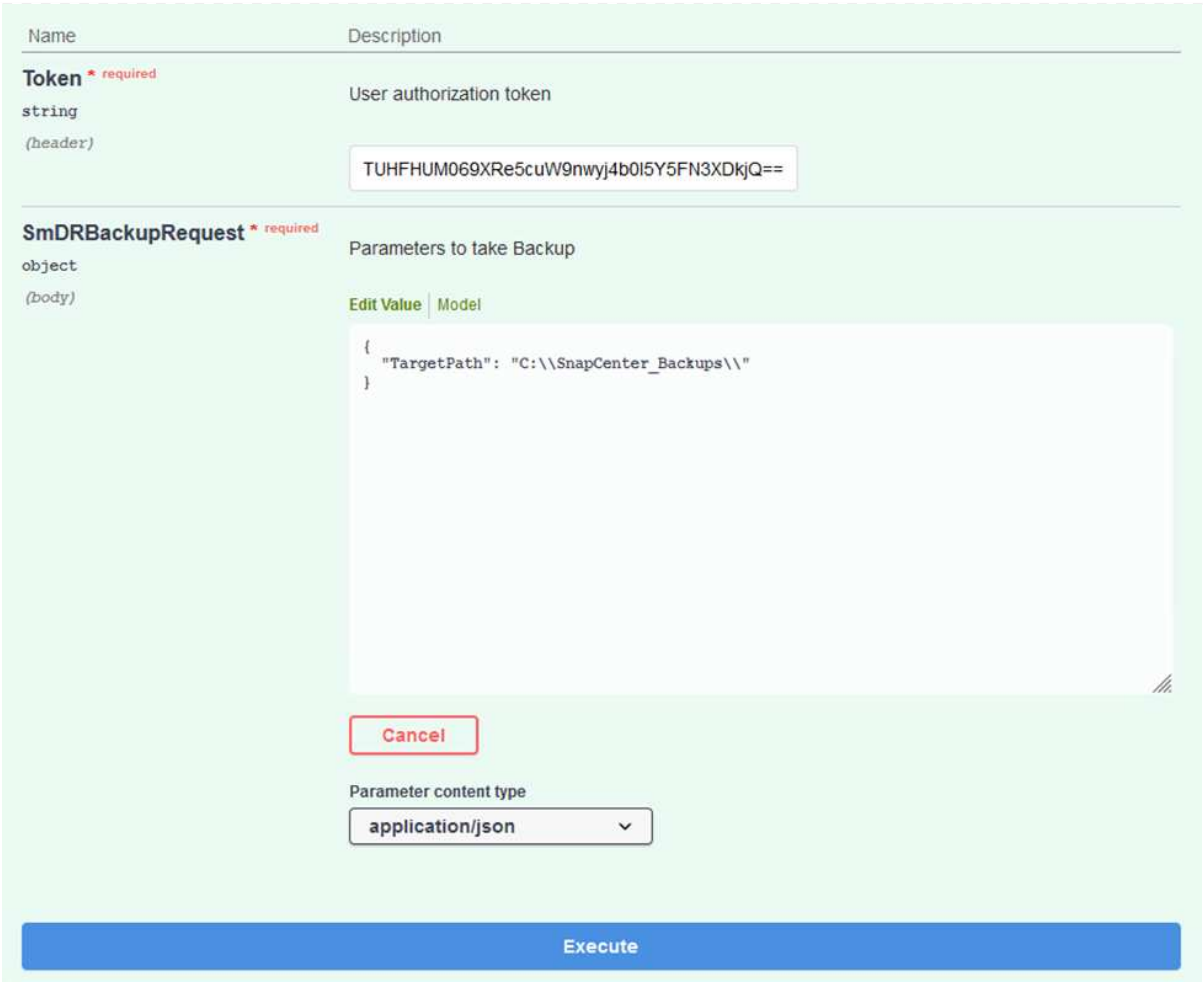


2. Expanda el `/4.6/disasterrecovery/server/backup` Y haga clic en probar.



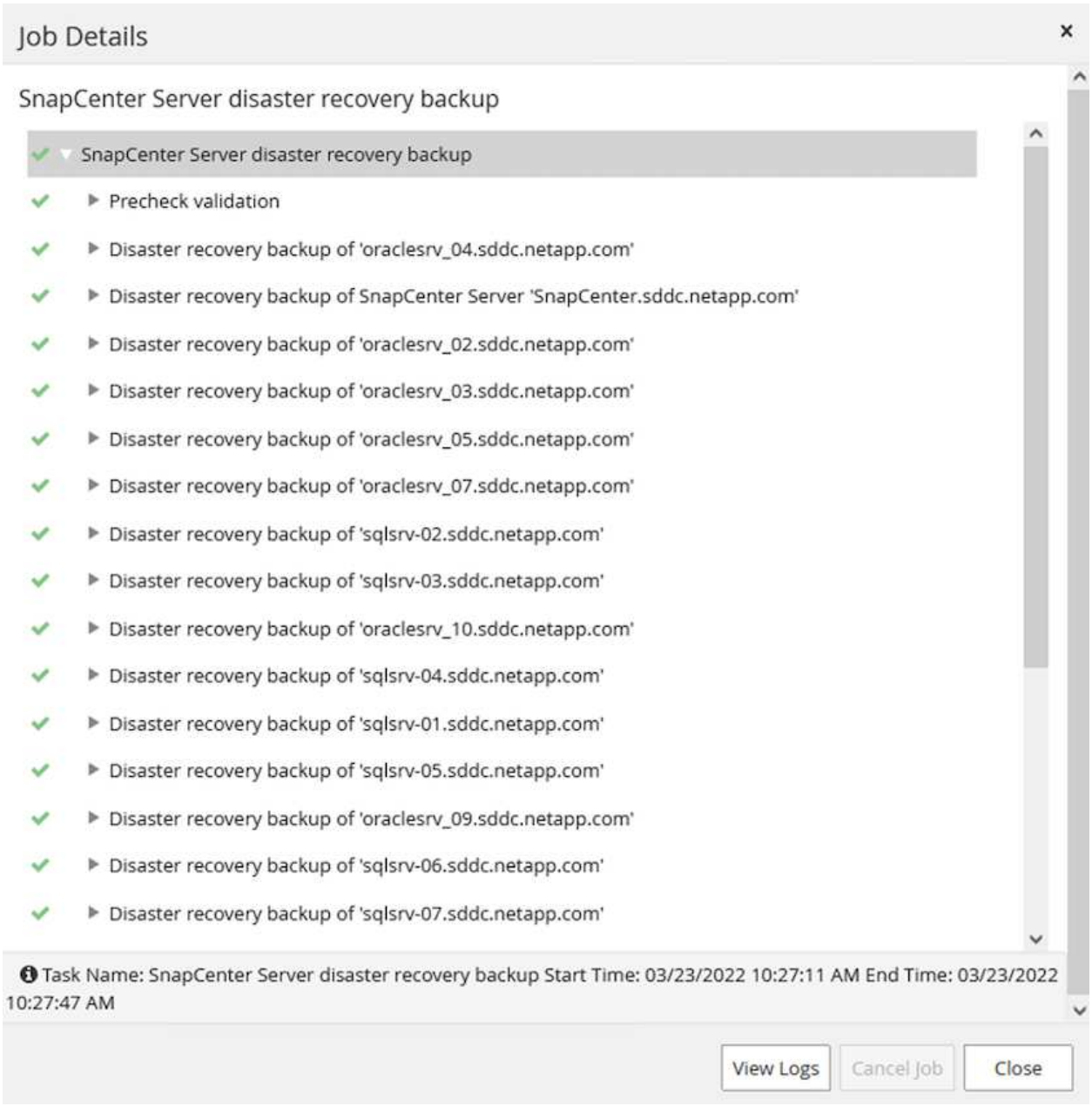
3. En la sección SmDRBackupRequest, añada la ruta de acceso correcta al destino local y seleccione Execute para iniciar el backup de la base de datos y la configuración de SnapCenter.

> El proceso de backup no permite realizar el backup directamente en un recurso compartido de archivos NFS o CIFS.


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

Supervise el trabajo de backup desde SnapCenter

Inicie sesión en SnapCenter para revisar los archivos de registro al iniciar el proceso de restauración de la base de datos. En la sección Supervisión, puede ver los detalles del backup de recuperación ante desastres del servidor SnapCenter.



Utilice la utilidad XCOPY para copiar el archivo de copia de seguridad de la base de datos en el recurso compartido SMB

A continuación, debe mover el backup de la unidad local del servidor SnapCenter al recurso compartido CIFS que se utiliza para copiar los datos en la ubicación secundaria ubicada en la instancia de FSX en AWS. Utilice xcopy con opciones específicas que conserven los permisos de los archivos.

Abra un símbolo del sistema como Administrador. Desde el símbolo del sistema, introduzca los siguientes comandos:

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X
/E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O
/X /E /H /K
```

Conmutación al respaldo

Desastre ocurre en el sitio principal

Para un desastre que se produzca en el centro de datos principal en las instalaciones, nuestro escenario incluye la conmutación al respaldo en un sitio secundario que reside en la infraestructura de Amazon Web Services mediante VMware Cloud en AWS. Asumimos que ya no se puede acceder a las máquinas virtuales y al clúster ONTAP que ofrecemos en las instalaciones. Además, ya no se puede acceder a las máquinas virtuales SnapCenter y Veeam y deben reconstruirse en nuestro sitio secundario.

En esta sección se aborda la conmutación por error de nuestra infraestructura al cloud y se tratan los siguientes temas:

- Restauración de la base de datos de SnapCenter. Una vez establecido un nuevo servidor SnapCenter, restaure los archivos de configuración y de base de datos de MySQL y coloque la base de datos en modo de recuperación ante desastres para permitir que el almacenamiento FSX secundario se convierta en el dispositivo de almacenamiento primario.
- Restaure los equipos virtuales de aplicaciones mediante Veeam Backup & Replication. Conecte el almacenamiento S3 que contiene los backups de la máquina virtual, importe los backups y restáutelos en VMware Cloud en AWS.
- Restaure los datos de aplicaciones de SQL Server mediante SnapCenter.
- Restaure los datos de la aplicación Oracle mediante SnapCenter.

Proceso de restauración de bases de datos de SnapCenter

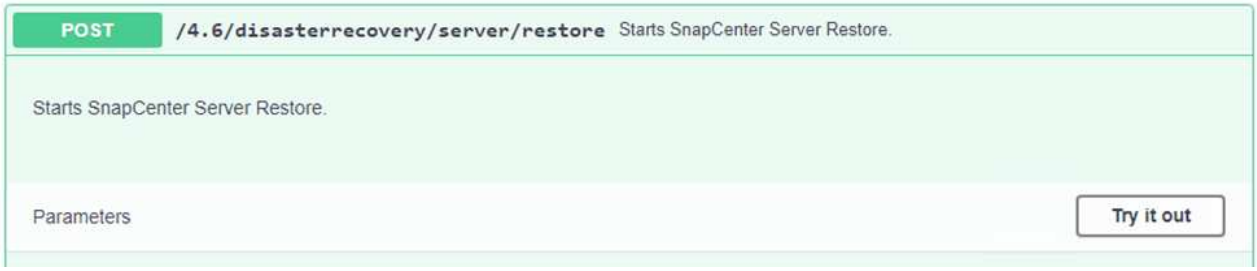
SnapCenter admite escenarios de recuperación ante desastres, ya que permite el backup y la restauración de sus archivos de configuración y base de datos de MySQL. Esto permite a un administrador mantener backups periódicos de la base de datos de SnapCenter en el centro de datos local y restaurar posteriormente esa base de datos a una base de datos de SnapCenter secundaria.

Para acceder a los archivos de copia de seguridad de SnapCenter en el servidor SnapCenter remoto, siga estos pasos:

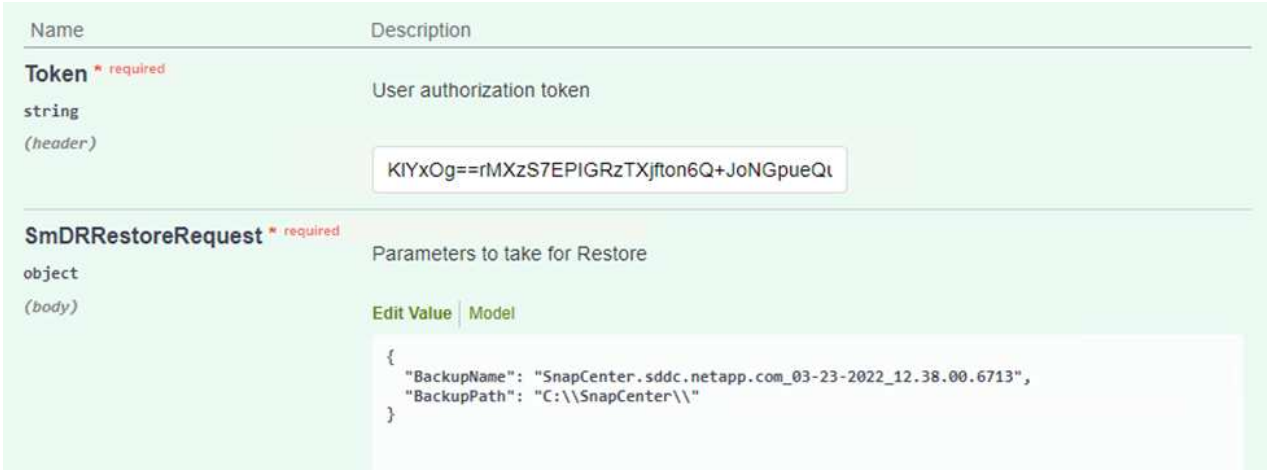
1. Rompa la relación de SnapMirror del clúster FSX y haga que el volumen sea de lectura/escritura.
2. Cree un servidor CIFS (si es necesario) y cree un recurso compartido CIFS que señale la ruta de unión del volumen clonado.
3. Utilice xcopy para copiar los archivos de copia de seguridad en un directorio local del sistema SnapCenter secundario.
4. Instale SnapCenter v4.6.
5. Asegúrese de que el servidor SnapCenter tiene el mismo FQDN que el servidor original. Esto es necesario para que la restauración de la base de datos se realice correctamente.

Para iniciar el proceso de restauración, lleve a cabo los siguientes pasos:

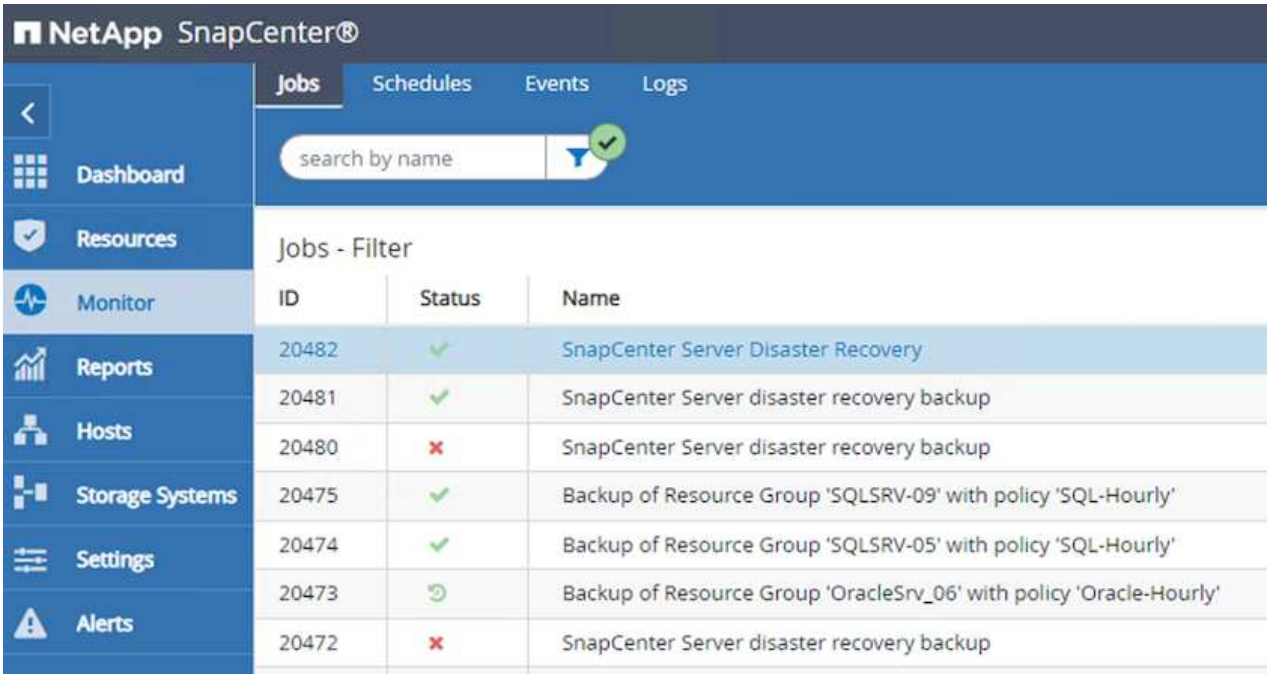
1. Acceda a la página web de API de Swagger para el servidor SnapCenter secundario y siga las instrucciones anteriores para obtener un token de autorización.
2. Desplácese hasta la sección Disaster Recovery de la página Swagger, seleccione `/4.6/disasterrecovery/server/restore`Y haga clic en probar.

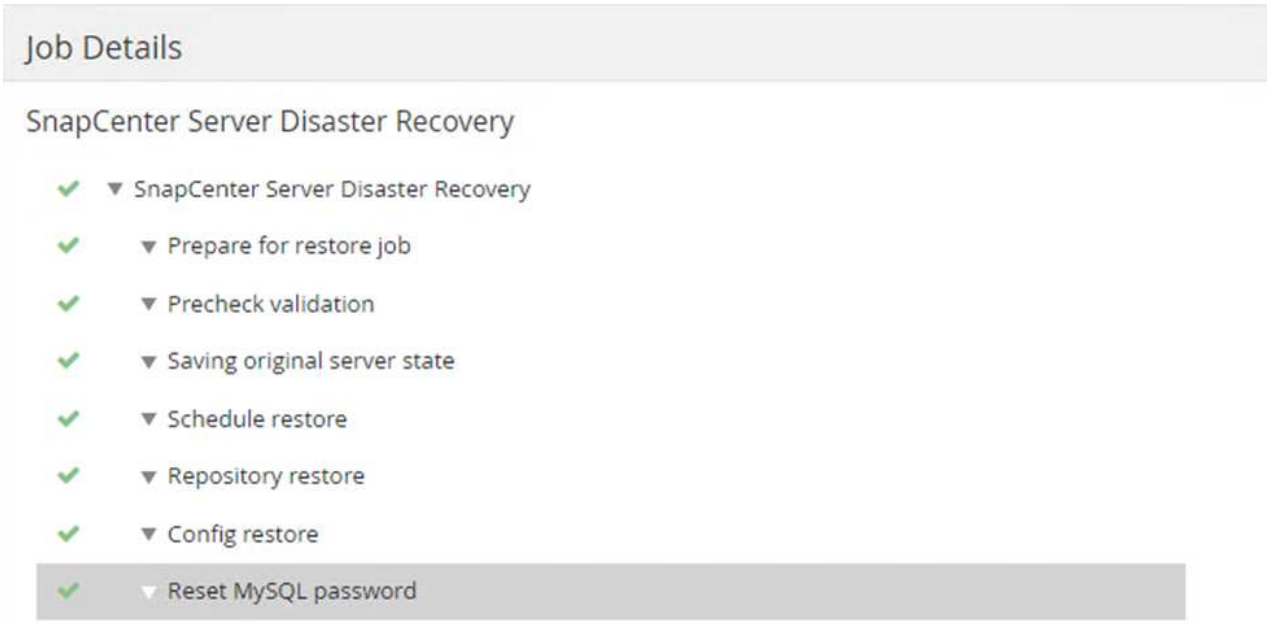


3. Pegue el token de autorización y, en la sección SmDRResterRequest, pegue el nombre del backup y el directorio local del servidor SnapCenter secundario.



4. Seleccione el botón Ejecutar para iniciar el proceso de restauración.
5. En SnapCenter, desplácese hasta la sección Supervisión para ver el progreso del trabajo de restauración.





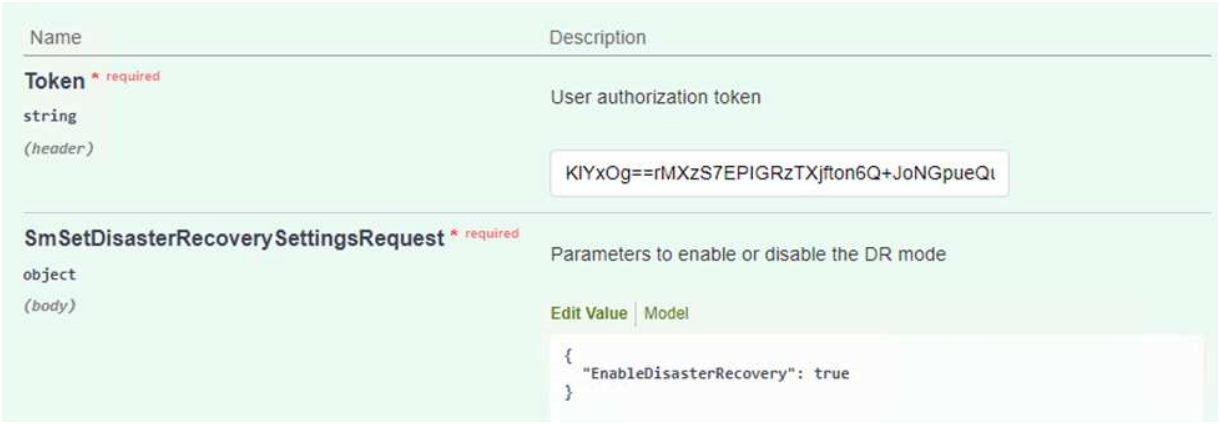
6. Para habilitar las restauraciones de SQL Server a partir de almacenamiento secundario, es necesario cambiar la base de datos de SnapCenter al modo de recuperación ante desastres. Esto se realiza como una operación independiente y se inicia en la página web de la API de Swagger.

   a. Desplácese hasta la sección Disaster Recovery y haga clic en `/4.6/disasterrecovery/storage`.

   b. Pegar en el token de autorización de usuario.

   c. En la sección SmSetDisasterRecoverySettingsRequest, cambie `EnableDisasterRecover` para `true`.

d. Haga clic en Execute para habilitar el modo de recuperación ante desastres para SQL Server.



Consulte los comentarios sobre procedimientos adicionales.

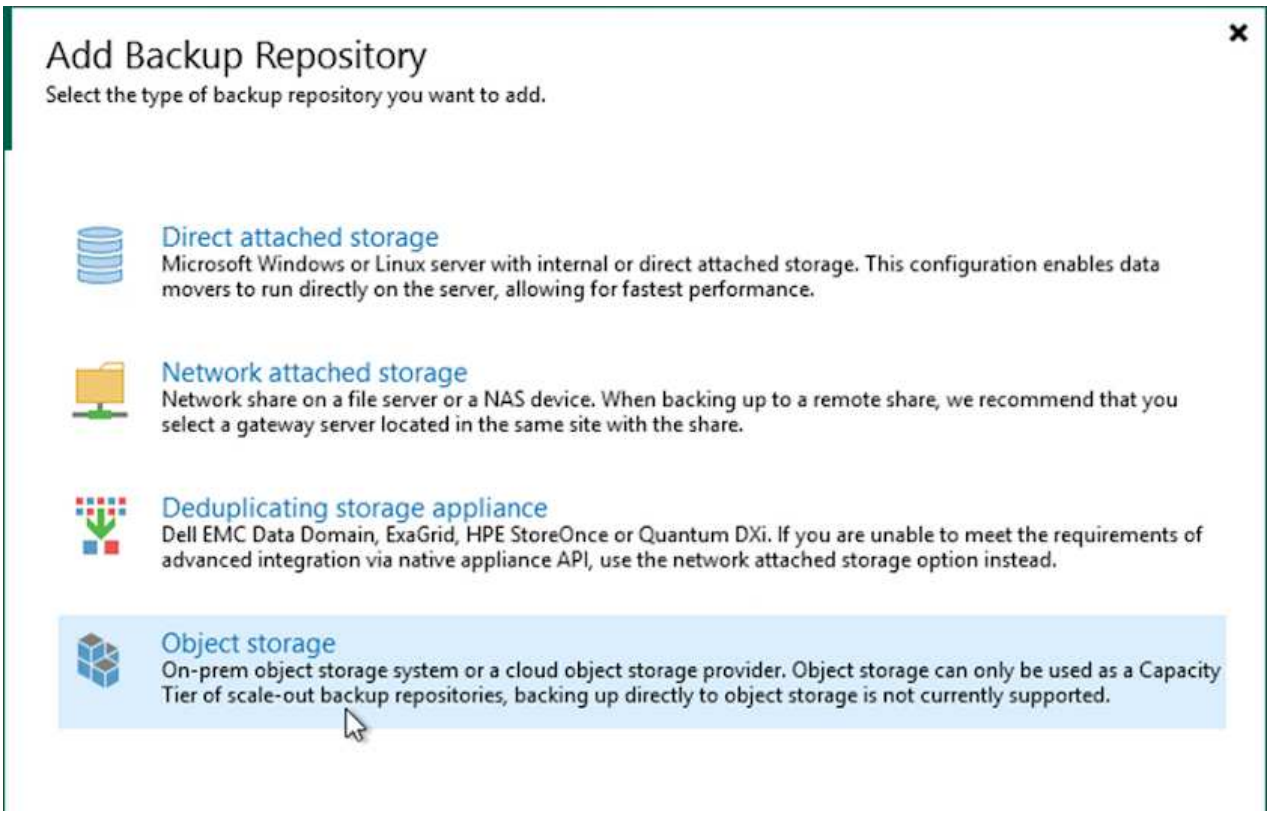
Restaure equipos virtuales de aplicación con la restauración completa de Veeam

Cree un repositorio de backup e importe los backups desde S3

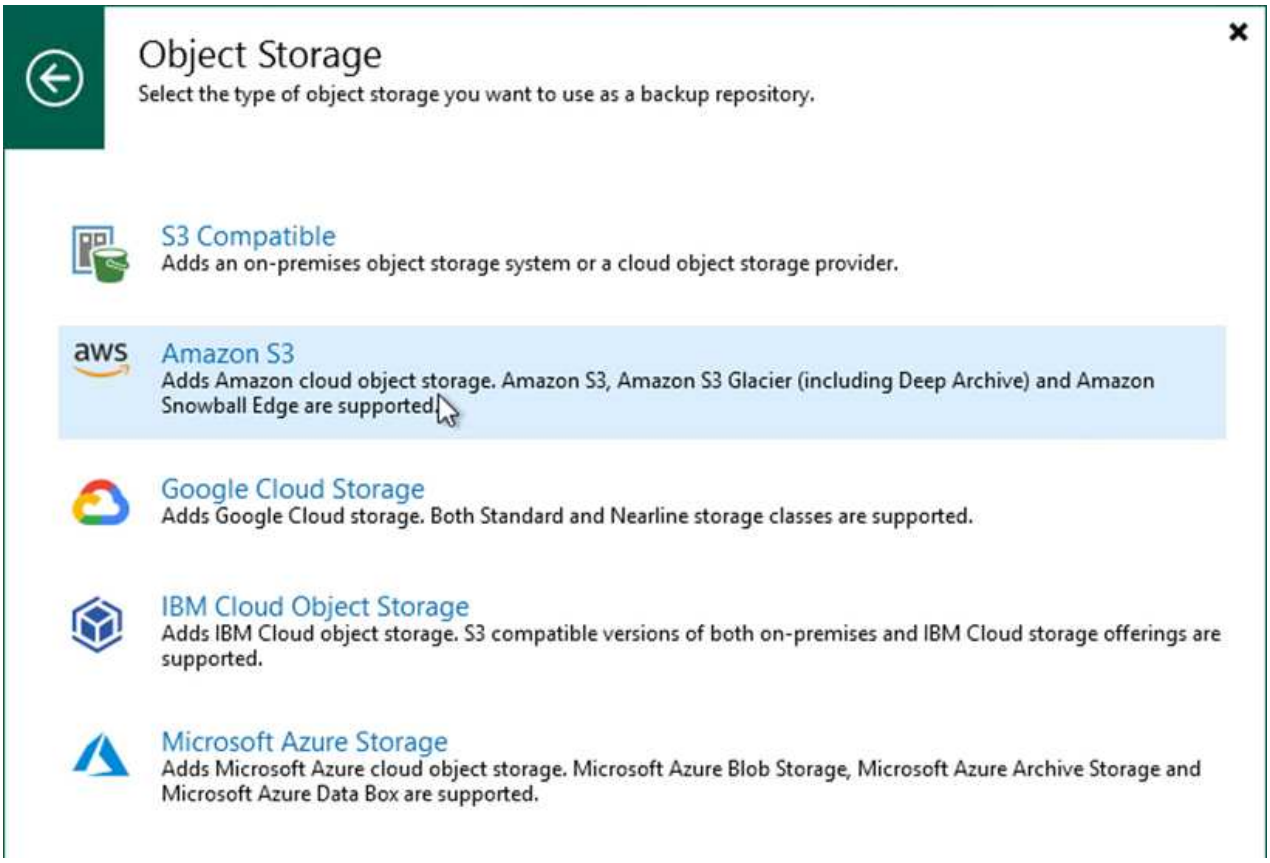
Desde el servidor de Veeam secundario, importe los backups desde el almacenamiento S3 y restaure las máquinas virtuales de SQL Server y Oracle al clúster de VMware Cloud.

Para importar los backups del objeto S3 que formaba parte del repositorio de backup de escalado horizontal en las instalaciones, complete los siguientes pasos:

1. Vaya a repositorios de copia de seguridad y haga clic en Añadir repositorio en el menú superior para abrir el asistente Añadir repositorio de copia de seguridad. En la primera página del asistente, seleccione Object Storage como el tipo de repositorio de backup.

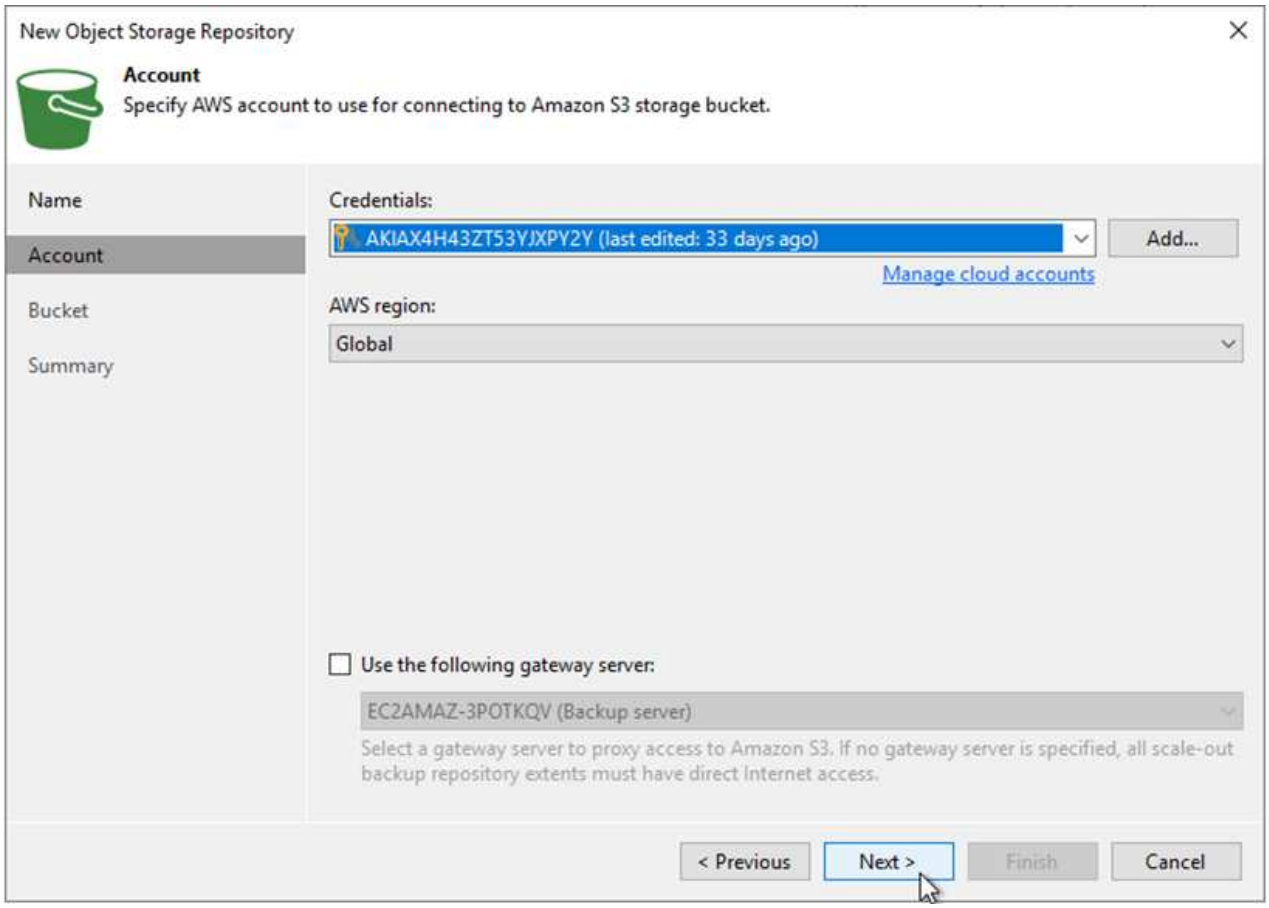


2. Seleccione Amazon S3 como tipo de almacenamiento de objetos.

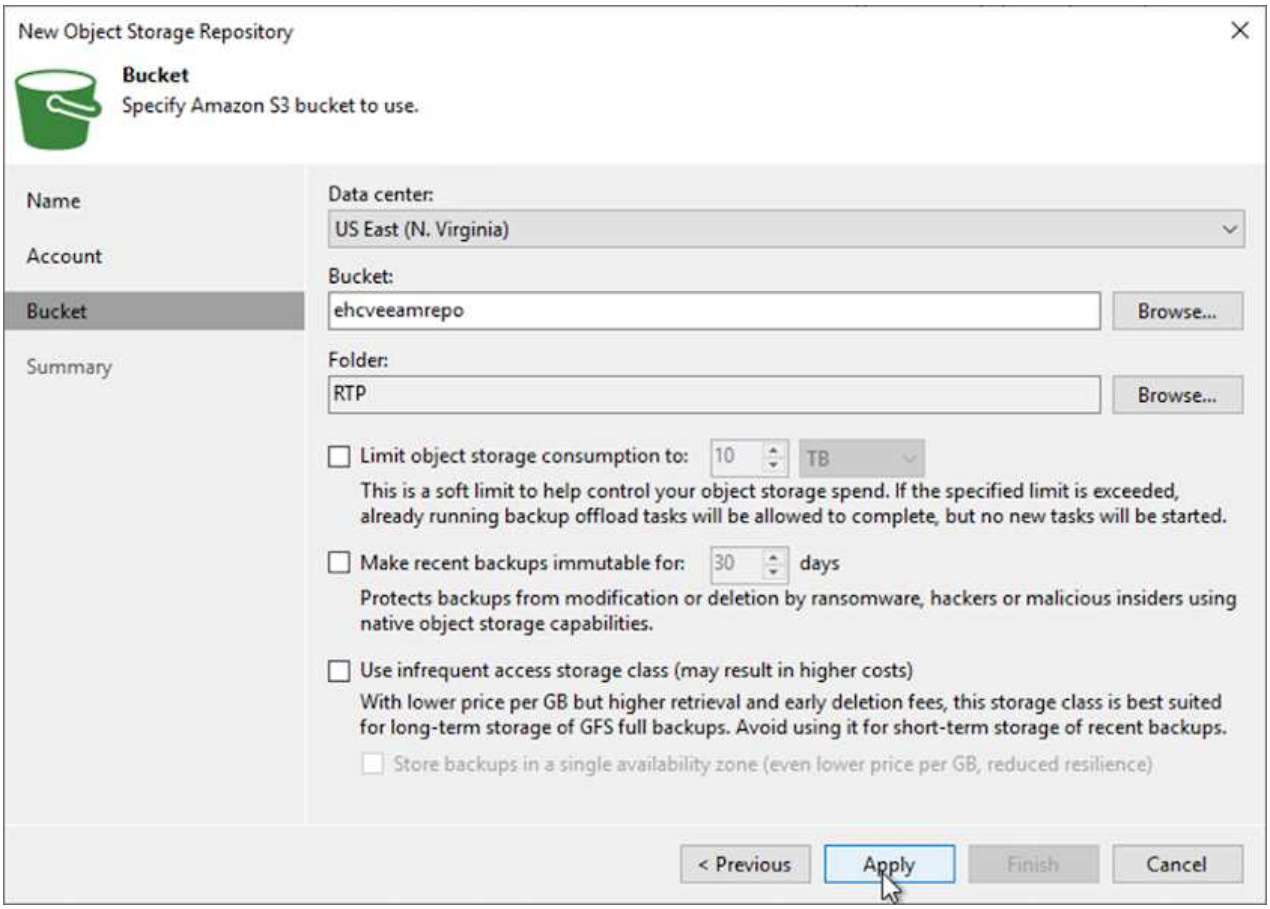


3. En la lista de Amazon Cloud Storage Services, seleccione Amazon S3.

4. Seleccione las credenciales introducidas previamente en la lista desplegable o añada una nueva credencial para acceder al recurso de almacenamiento en cloud. Haga clic en Siguiente para continuar.



5. En la página Bucket, introduzca el centro de datos, el bloque, la carpeta y las opciones que desee. Haga clic en Apply.

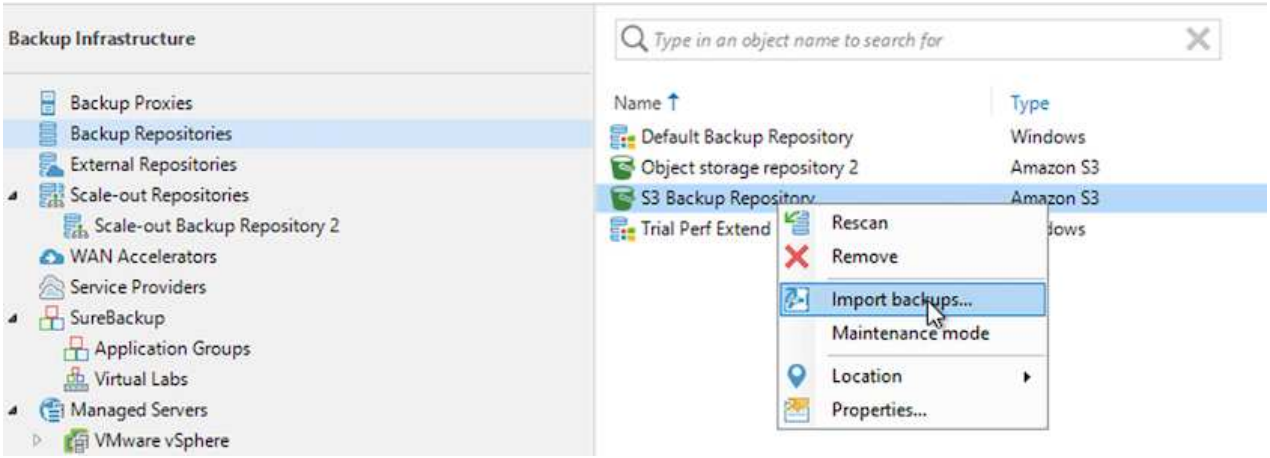


6. Finalmente, seleccione Finalizar para completar el proceso y agregar el repositorio.

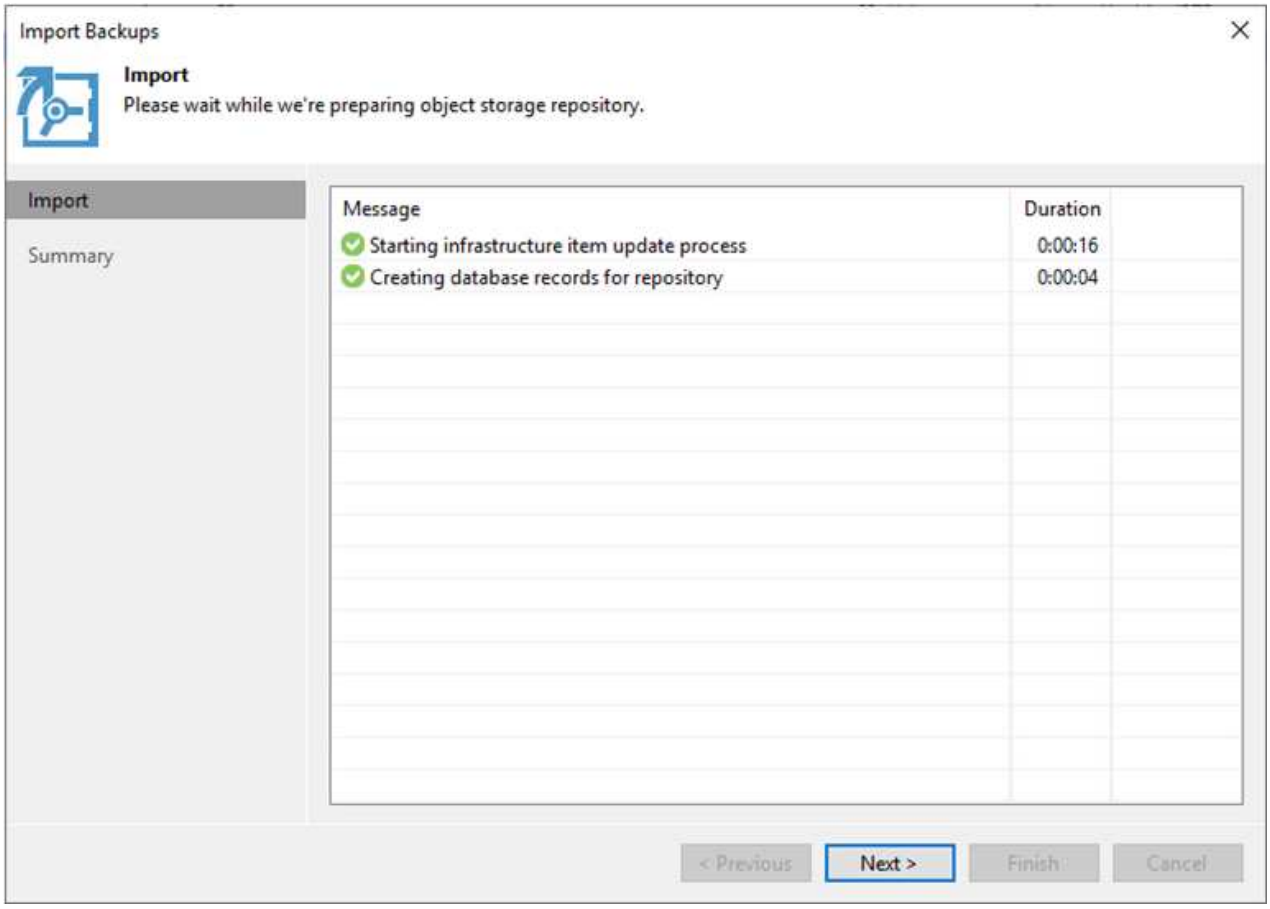
Importe los backups desde el almacenamiento de objetos S3

Para importar los backups desde el repositorio de S3 que se agregó en la sección anterior, complete los siguientes pasos.

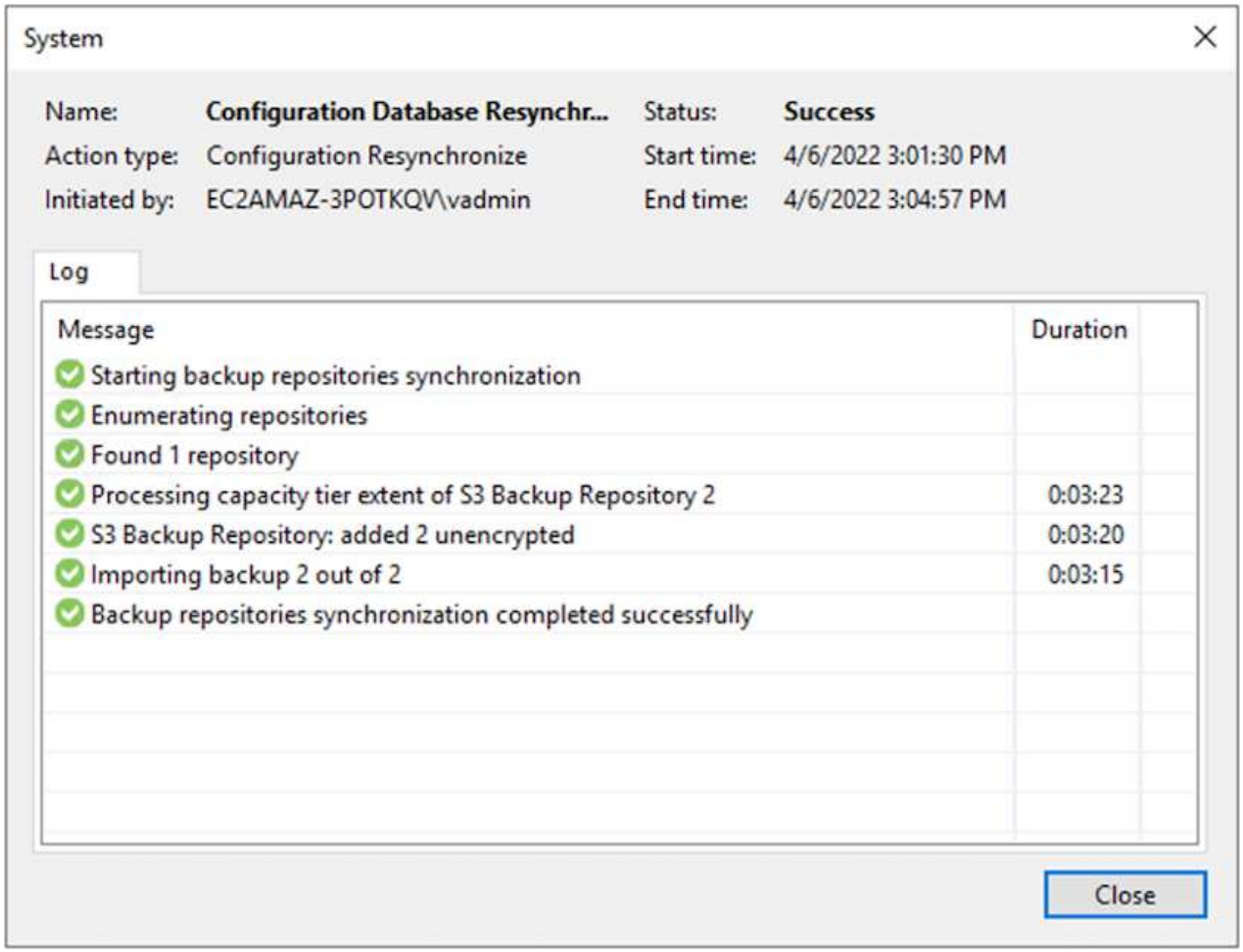
1. En el repositorio de backup de S3, seleccione Import backups para abrir el asistente Import backups.



2. Una vez creados los registros de la base de datos para la importación, seleccione Siguiente y, a continuación, Finalizar en la pantalla de resumen para iniciar el proceso de importación.



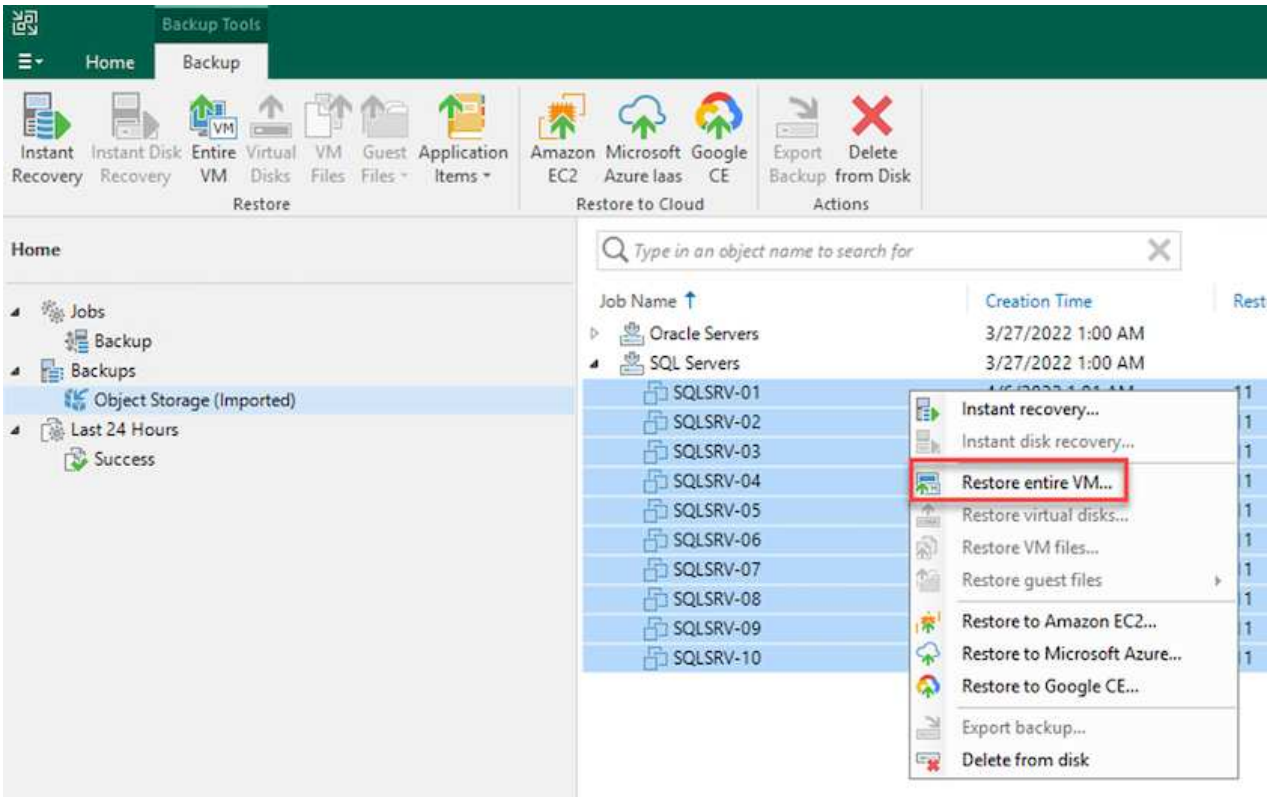
3. Una vez finalizada la importación, puede restaurar máquinas virtuales en el clúster de cloud de VMware.


System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

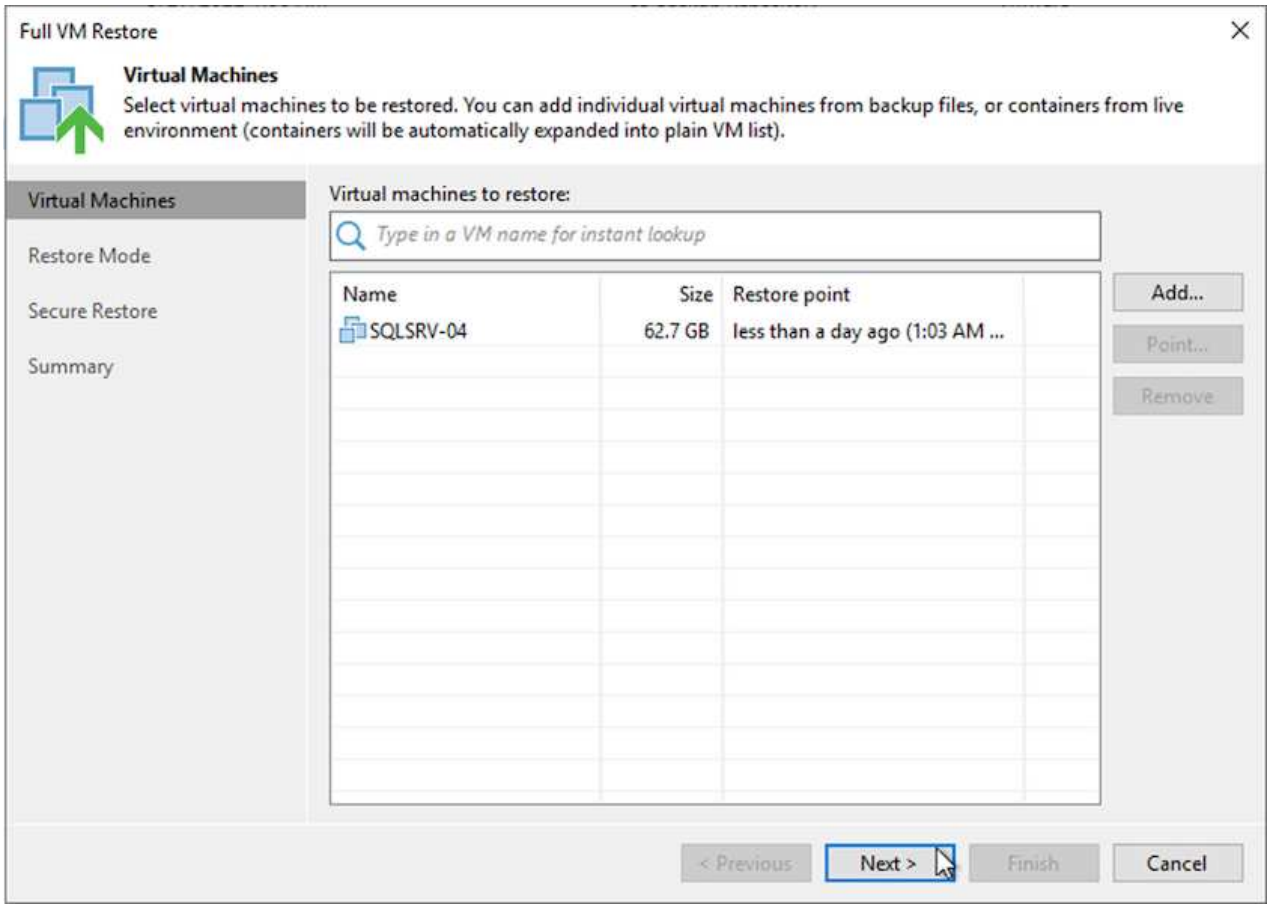
Restaure equipos virtuales de aplicación con la funcionalidad de restauración completa de Veeam en VMware Cloud

Para restaurar las máquinas virtuales de SQL y Oracle en VMware Cloud en el dominio/clúster de carga de trabajo de AWS, realice los siguientes pasos.

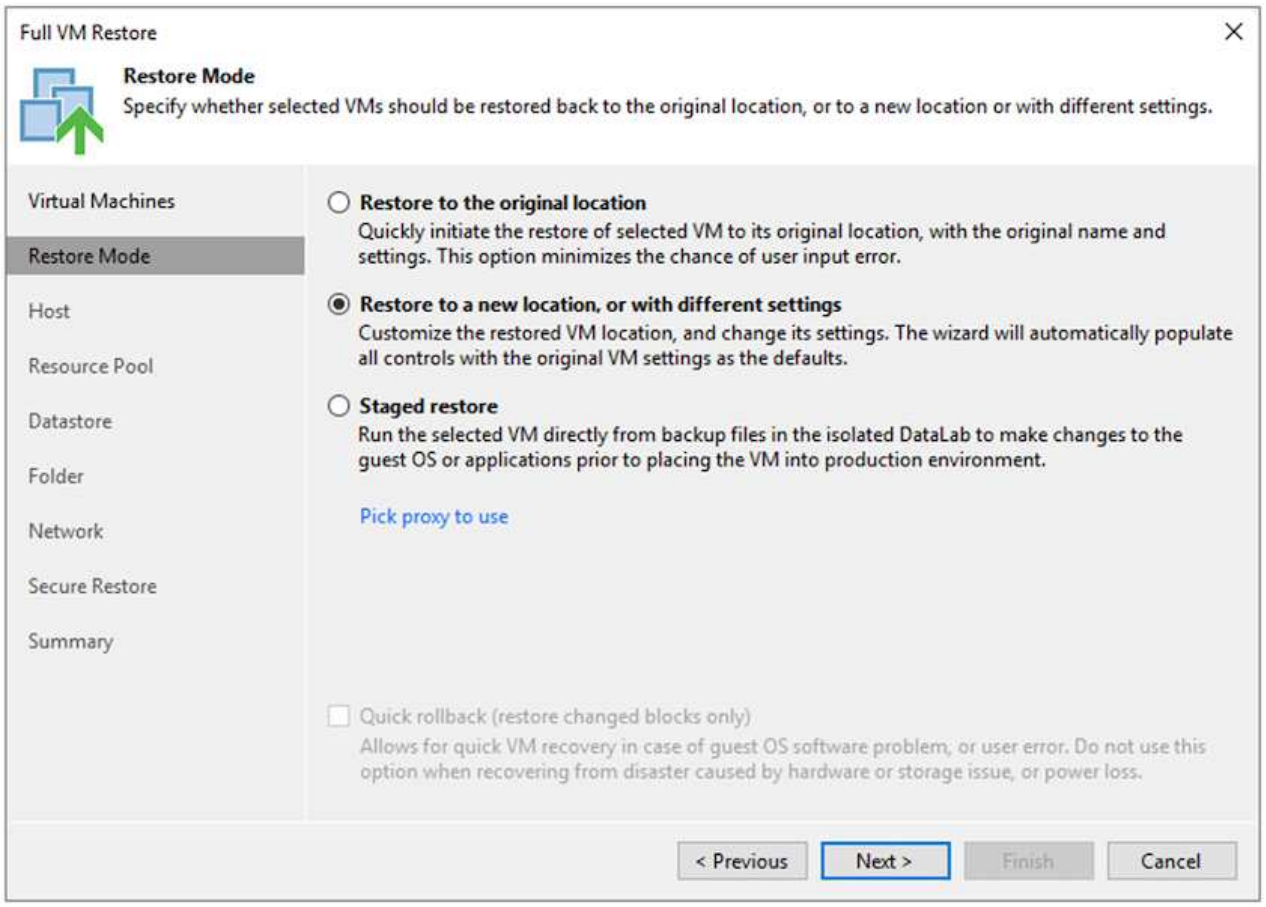
1. En la página Veeam Home, seleccione el almacenamiento de objetos que contiene los backups importados, seleccione las máquinas virtuales que desea restaurar y, a continuación, haga clic con el botón derecho en Restore entire VM.



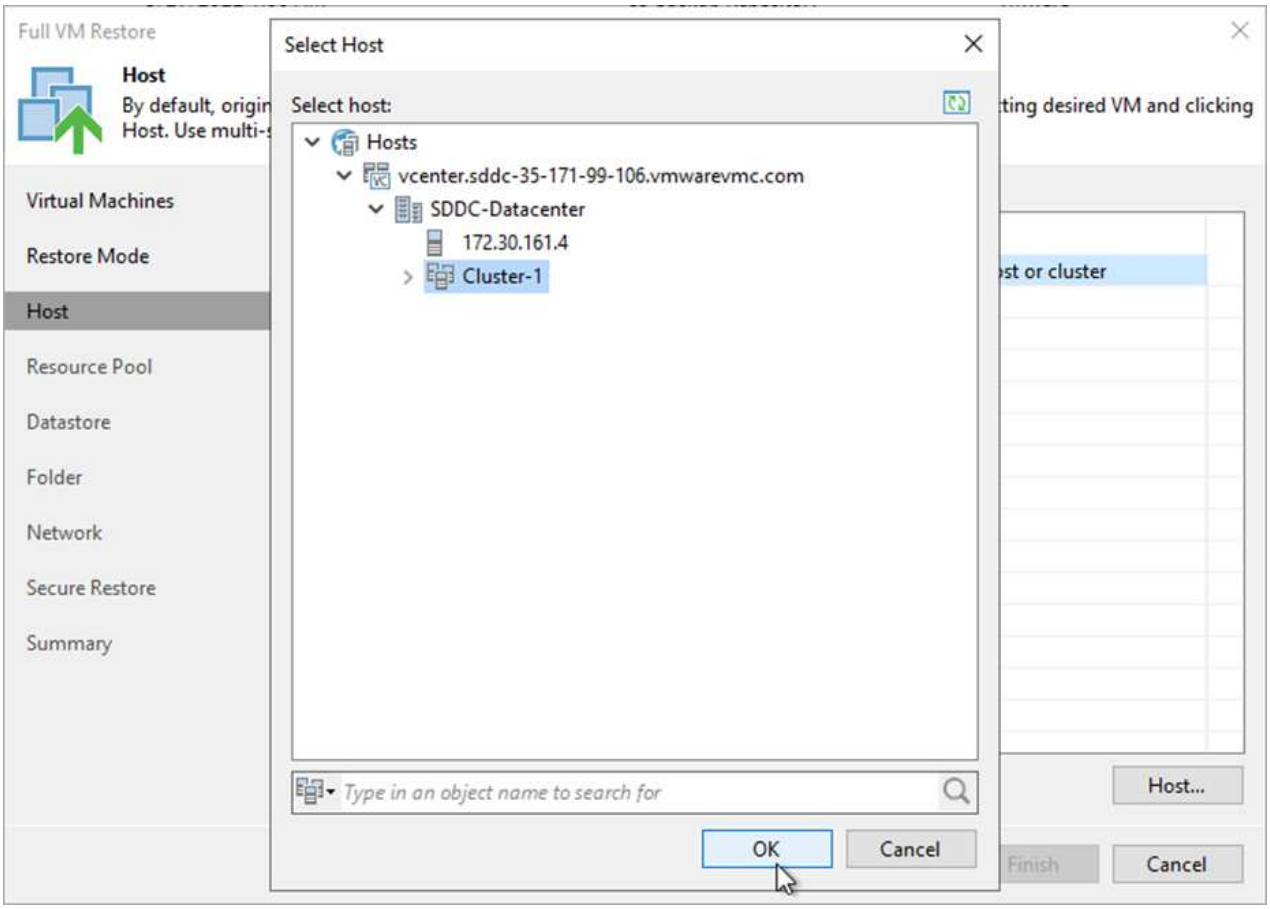
2. En la primera página del asistente Full VM Restore, modifique las máquinas virtuales para realizar el backup si lo desea y seleccione Next.



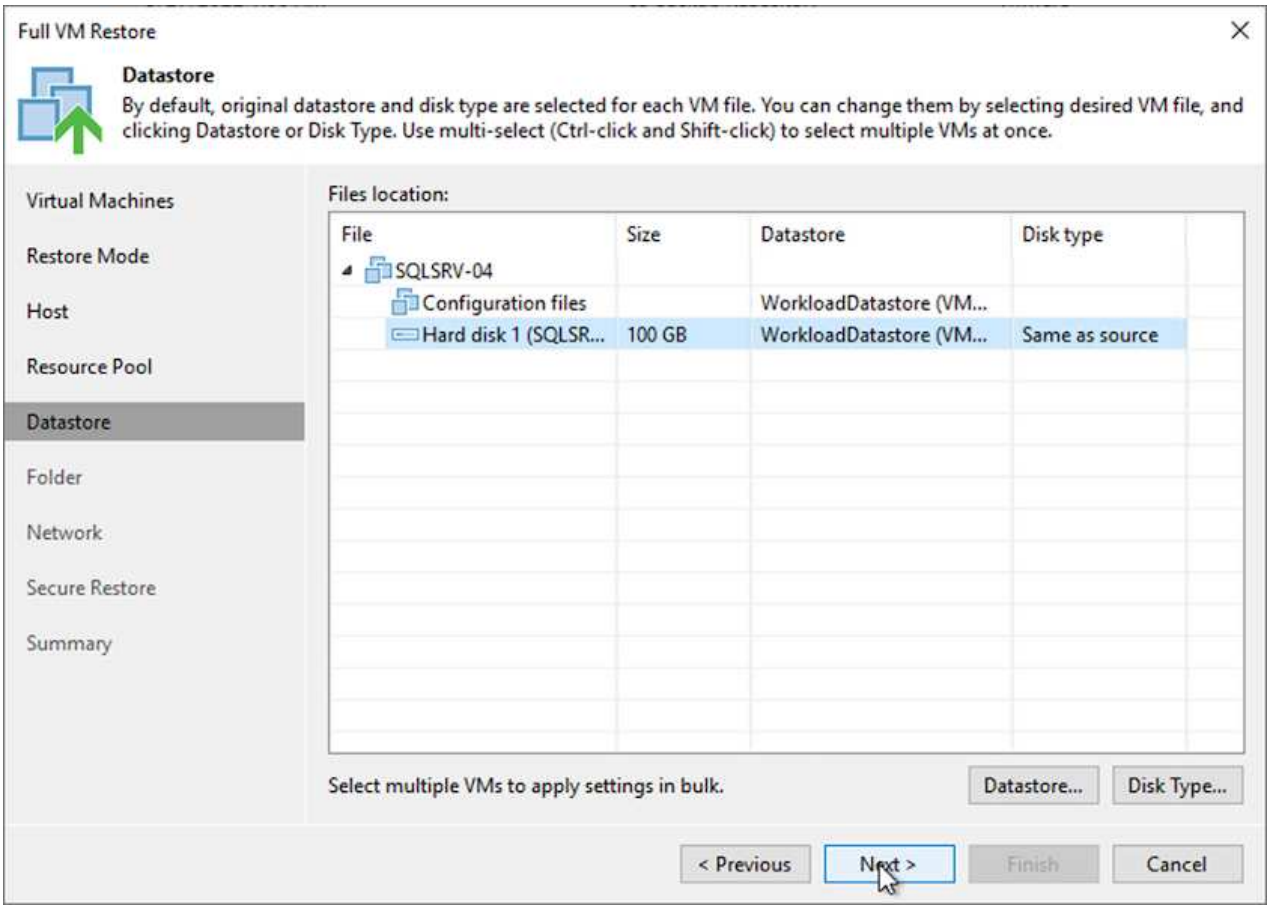
3. En la página Restore Mode, seleccione Restore to a New Location o with Disfruta de una configuración diferente.



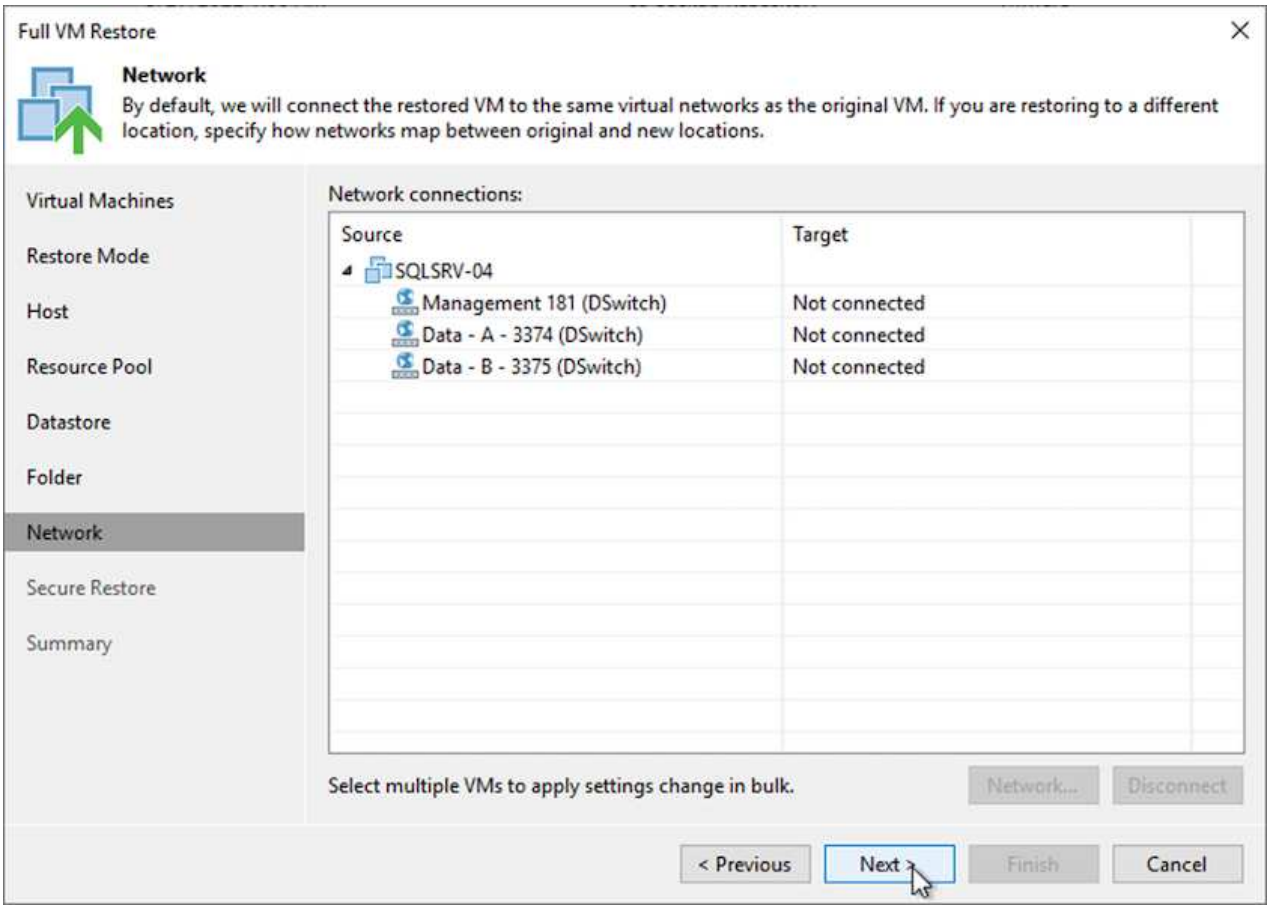
4. En la página host, seleccione el host o el clúster de destino ESXi al que desea restaurar la máquina virtual.

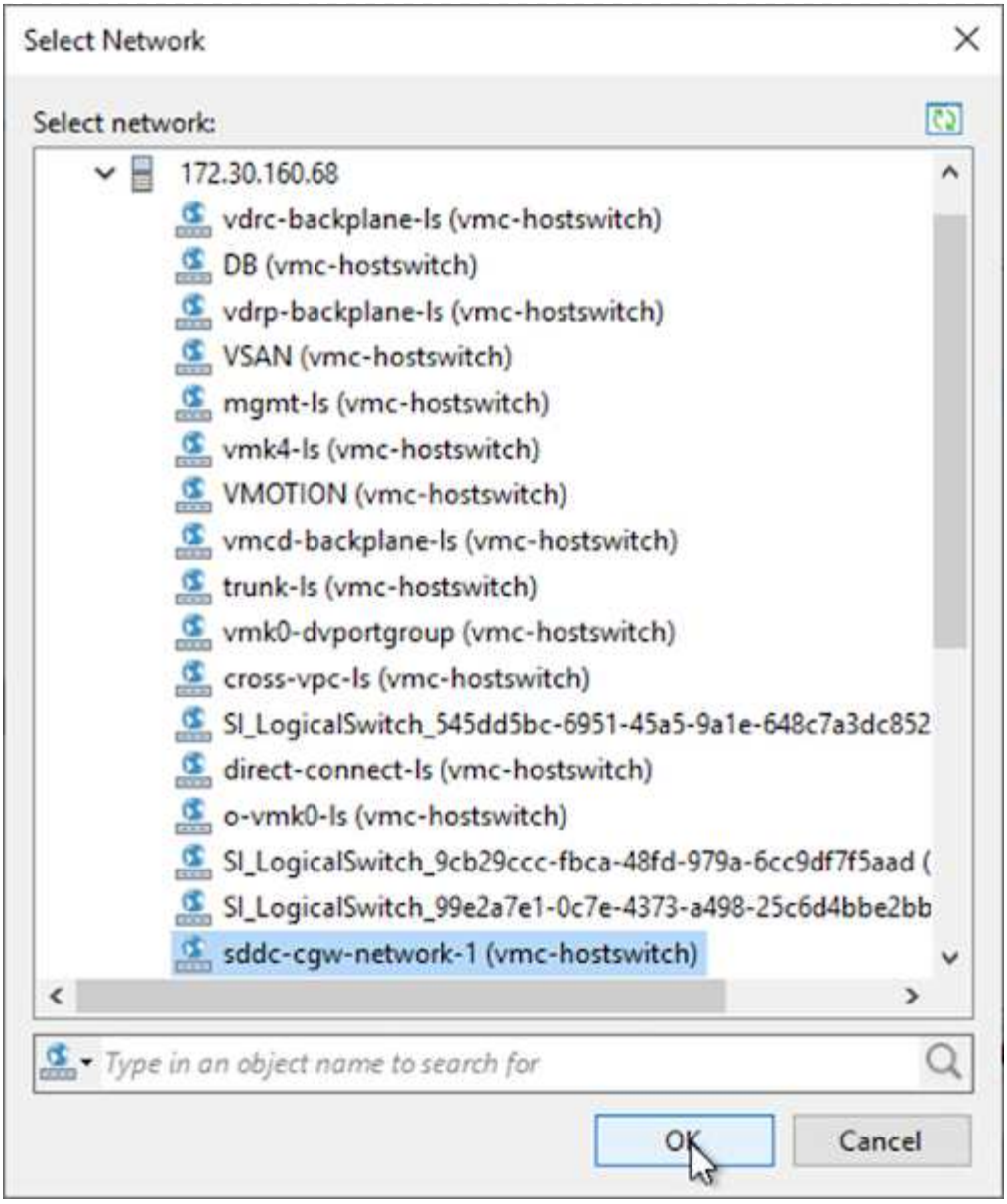


5. En la página datastores, seleccione la ubicación del almacén de datos de destino para los archivos de configuración y el disco duro.



6. En la página Network, asigne las redes originales en el equipo virtual a las redes en la nueva ubicación de destino.


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. Seleccione si desea analizar el malware en el equipo virtual restaurado, revise la página de resumen y haga clic en Finish para iniciar la restauración.

Restauración de datos de aplicaciones de SQL Server

El siguiente proceso proporciona instrucciones sobre cómo recuperar un servidor SQL Server en VMware Cloud Services en AWS en caso de un desastre que haga que el sitio local deje de funcionar.

Se asume que los siguientes requisitos previos están completos para continuar con los pasos de recuperación:

1. La máquina virtual de Windows Server se ha restaurado en el cloud SDDC de VMware mediante Veeam Full Restore.
2. Se ha establecido un servidor SnapCenter secundario y se ha completado la restauración y configuración de bases de datos SnapCenter siguiendo los pasos descritos en la sección "Resumen del proceso de backup y restauración de SnapCenter."

VM: Configuración posterior a la restauración para máquina virtual de SQL Server

Una vez finalizada la restauración de la máquina virtual, debe configurar la red y otros elementos durante la preparación para volver a detectar la máquina virtual host en SnapCenter.

1. Asigne nuevas direcciones IP para Management e iSCSI o NFS.
2. Una el host al dominio de Windows.
3. Añada los nombres de host a DNS o al archivo hosts del servidor SnapCenter.

Si el plugin de SnapCenter se implementó mediante credenciales de dominio diferentes al dominio actual, es necesario cambiar la cuenta de inicio de sesión del plugin para el servicio de Windows en la máquina virtual de SQL Server. Después de cambiar la cuenta de inicio de sesión, reinicie los servicios de SnapCenter SMCore, del plugin para Windows y del plugin para SQL Server.

Para volver a detectar automáticamente las máquinas virtuales restauradas en SnapCenter, el FQDN debe ser idéntico a la máquina virtual que se añadió originalmente a SnapCenter en las instalaciones.

Configurar almacenamiento FSX para la restauración de SQL Server

Para realizar el proceso de restauración de recuperación ante desastres de una máquina virtual de SQL Server, debe interrumpir la relación de SnapMirror existente del clúster FSX y otorgar acceso al volumen. Para ello, lleve a cabo los siguientes pasos.

1. Para romper la relación de SnapMirror existente de la base de datos de SQL Server y los volúmenes de registro, ejecute el siguiente comando desde la CLI de FSX:

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. Conceda acceso a la LUN mediante la creación de un grupo de iniciadores que contenga el IQN de iSCSI de la máquina virtual de SQL Server Windows:

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

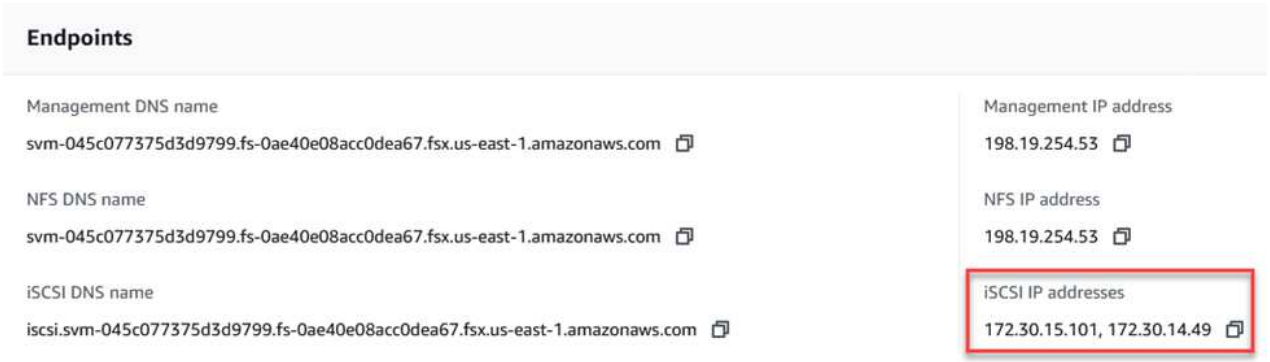
3. Finalmente, asigne las LUN al iGroup que acaba de crear:

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

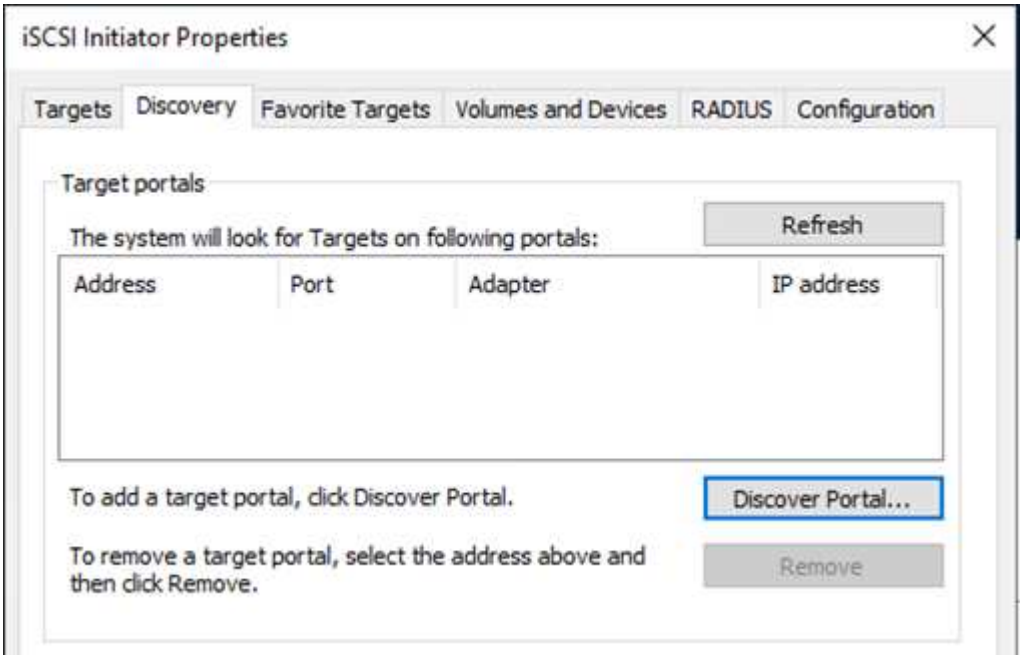
4. Para encontrar el nombre de ruta, ejecute el `lun show` comando.

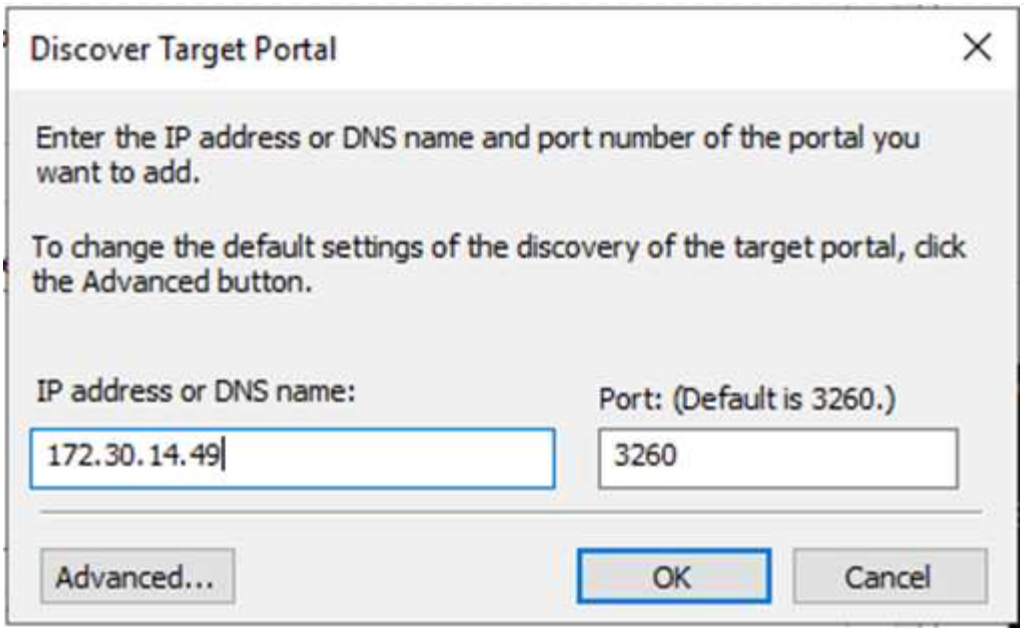
Configure la máquina virtual de Windows para acceder a iSCSI y detectar los sistemas de archivos

1. Desde la máquina virtual de SQL Server, configure el adaptador de red iSCSI para que se comunique en el grupo de puertos de VMware que se ha establecido con conectividad a las interfaces de destino iSCSI de la instancia de FSX.
2. Abra la utilidad iSCSI Initiator Properties y borre la configuración de conectividad antigua de las fichas Discovery, Favorite Targets y Targets.
3. Busque las direcciones IP para acceder a la interfaz lógica iSCSI en la instancia/clúster de FSX. Encontrará información en la consola de AWS en Amazon FSX > ONTAP > Storage Virtual Machines.

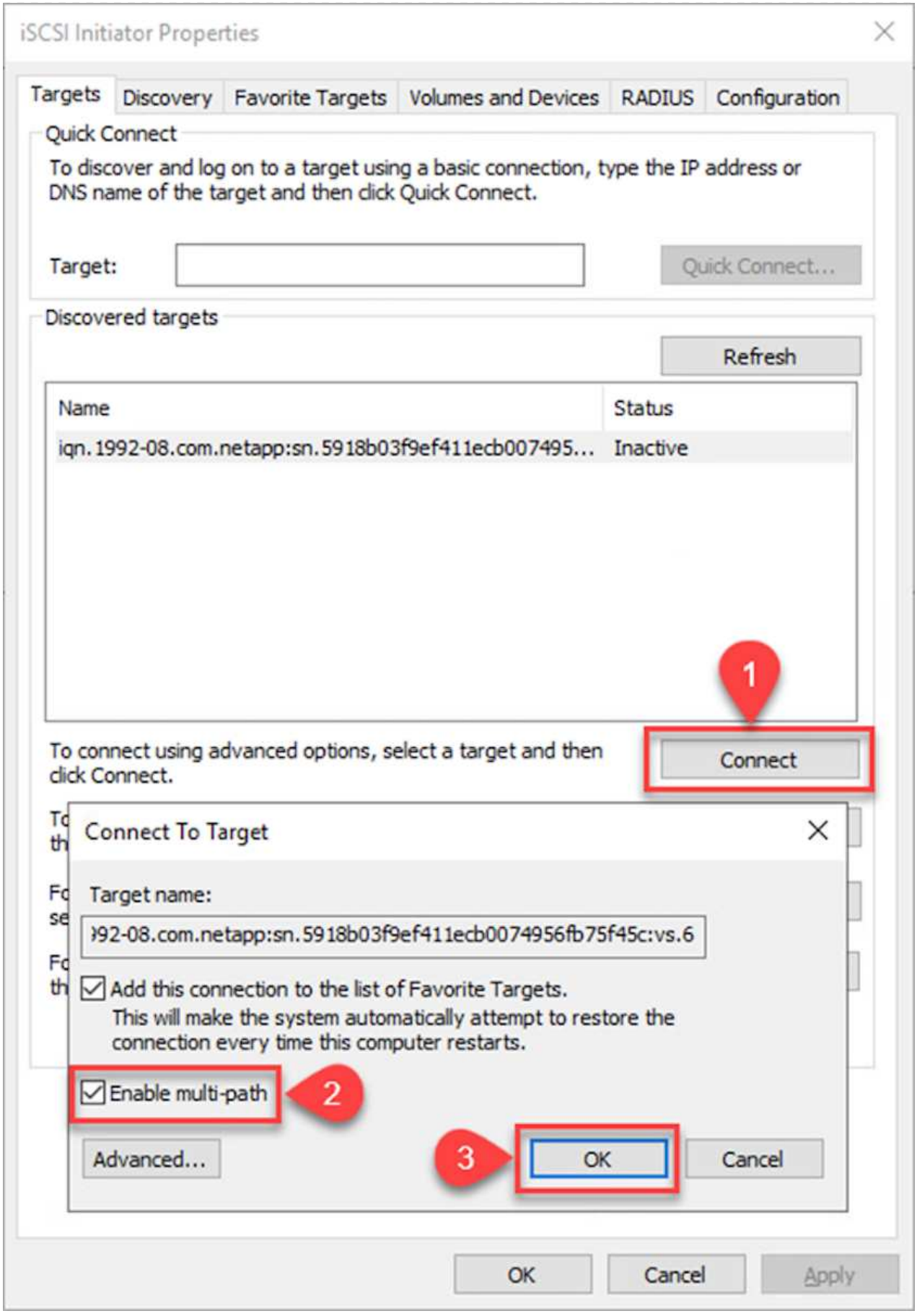


4. En la pestaña Discovery, haga clic en Discover Portal e introduzca las direcciones IP para los destinos iSCSI de FSX.

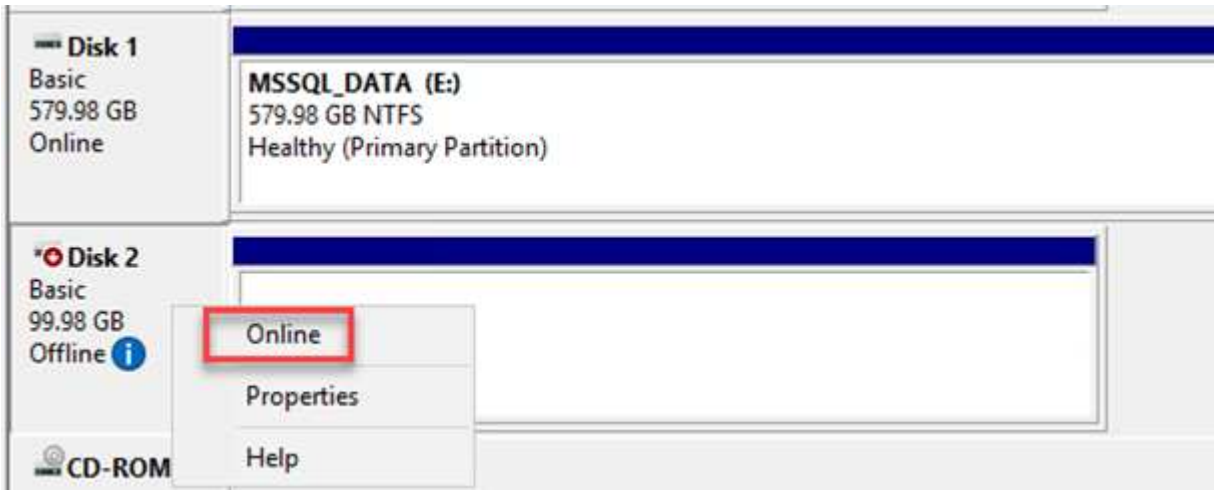




5. En la ficha destino, haga clic en conectar, seleccione Activar Multi-Path si es apropiado para su configuración y, a continuación, haga clic en Aceptar para conectarse al destino.

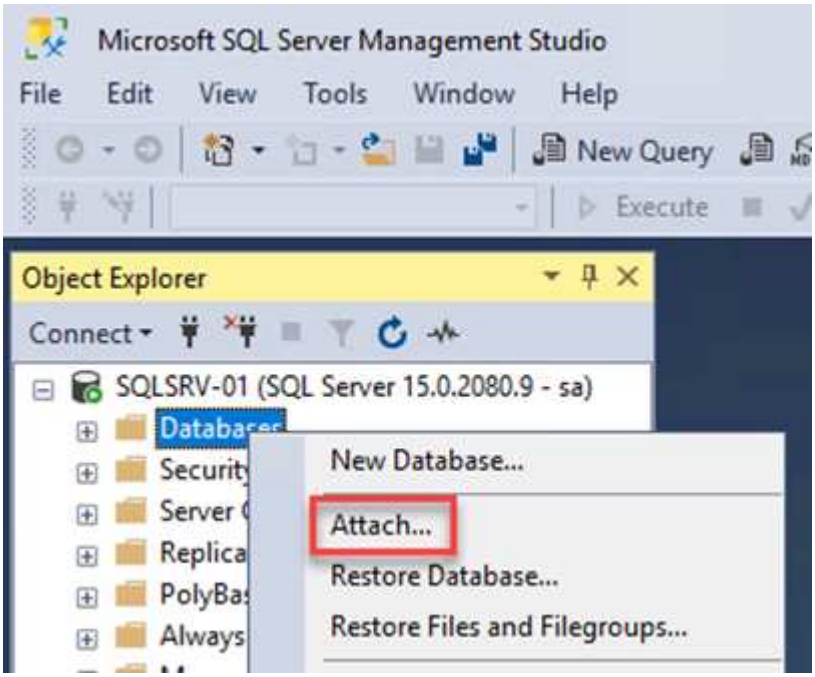

iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.
Target:
Quick Connect...
Discovered targets
Refresh
Name
Status
iqn.1992-08.com.netapp:sn.5918b03f9ef411ecb007495...
Inactive
1
To connect using advanced options, select a target and then click Connect.
Connect
Connect To Target
Target name:
)92-08.com.netapp:sn.5918b03f9ef411ecb0074956fb75f45c:vs.6
Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.
Enable multi-path
2
Advanced...
3
OK
Cancel
OK
Cancel
Apply

6. Abra la utilidad Administración de equipos y ponga los discos en línea. Compruebe que conservan las mismas letras de unidad que tenían anteriormente.

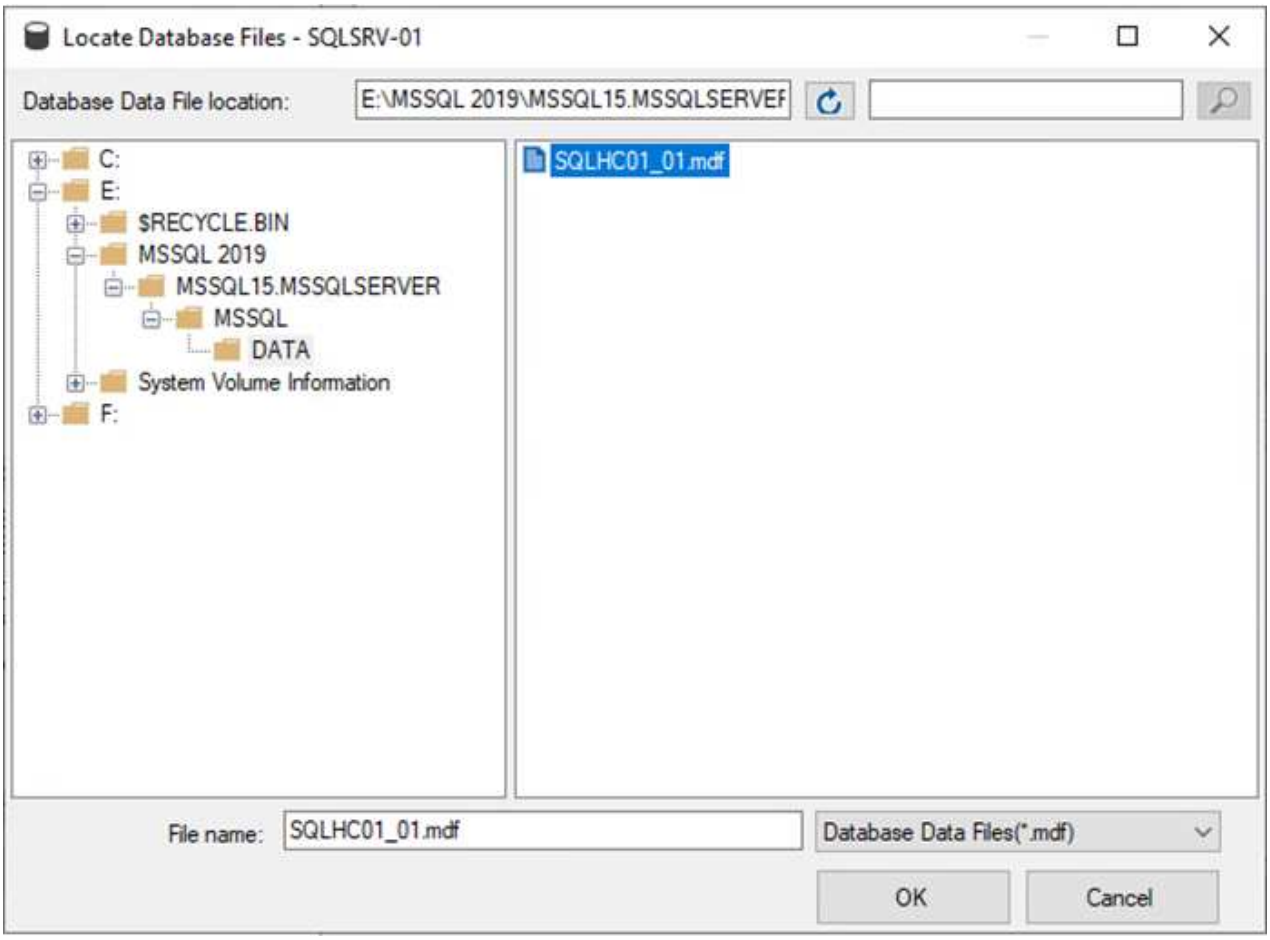


Conecte las bases de datos de SQL Server

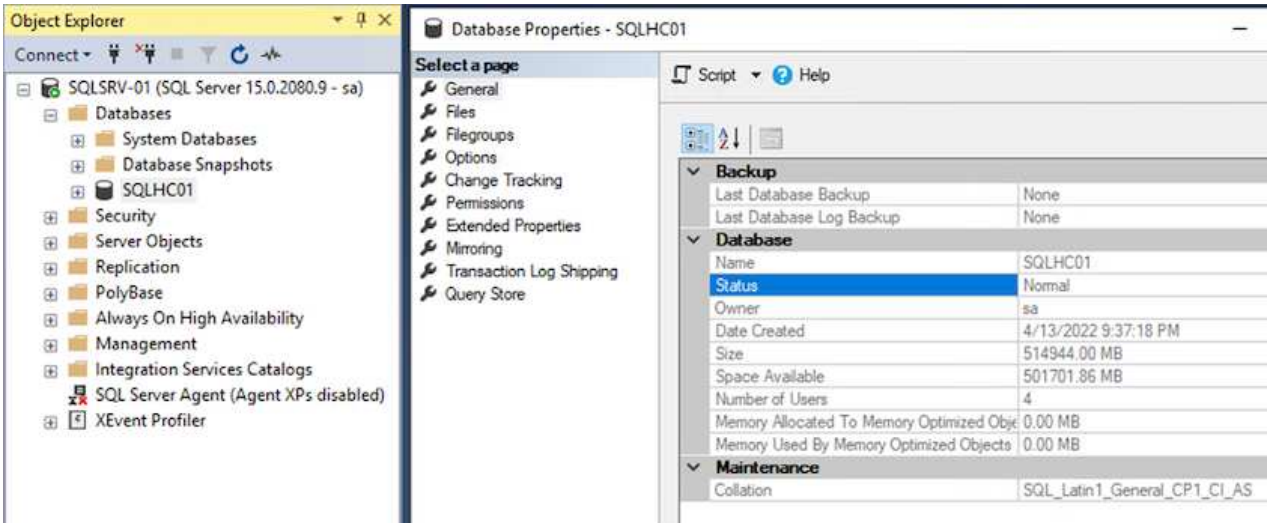
1. En la máquina virtual de SQL Server, abra Microsoft SQL Server Management Studio y seleccione Attach para iniciar el proceso de conexión a la base de datos.



2. Haga clic en Agregar y desplácese a la carpeta que contiene el archivo de base de datos principal de SQL Server, selecciónelo y haga clic en Aceptar.



3. Si los registros de transacciones se encuentran en una unidad independiente, elija la carpeta que contiene el registro de transacciones.
4. Cuando haya terminado, haga clic en Aceptar para adjuntar la base de datos.

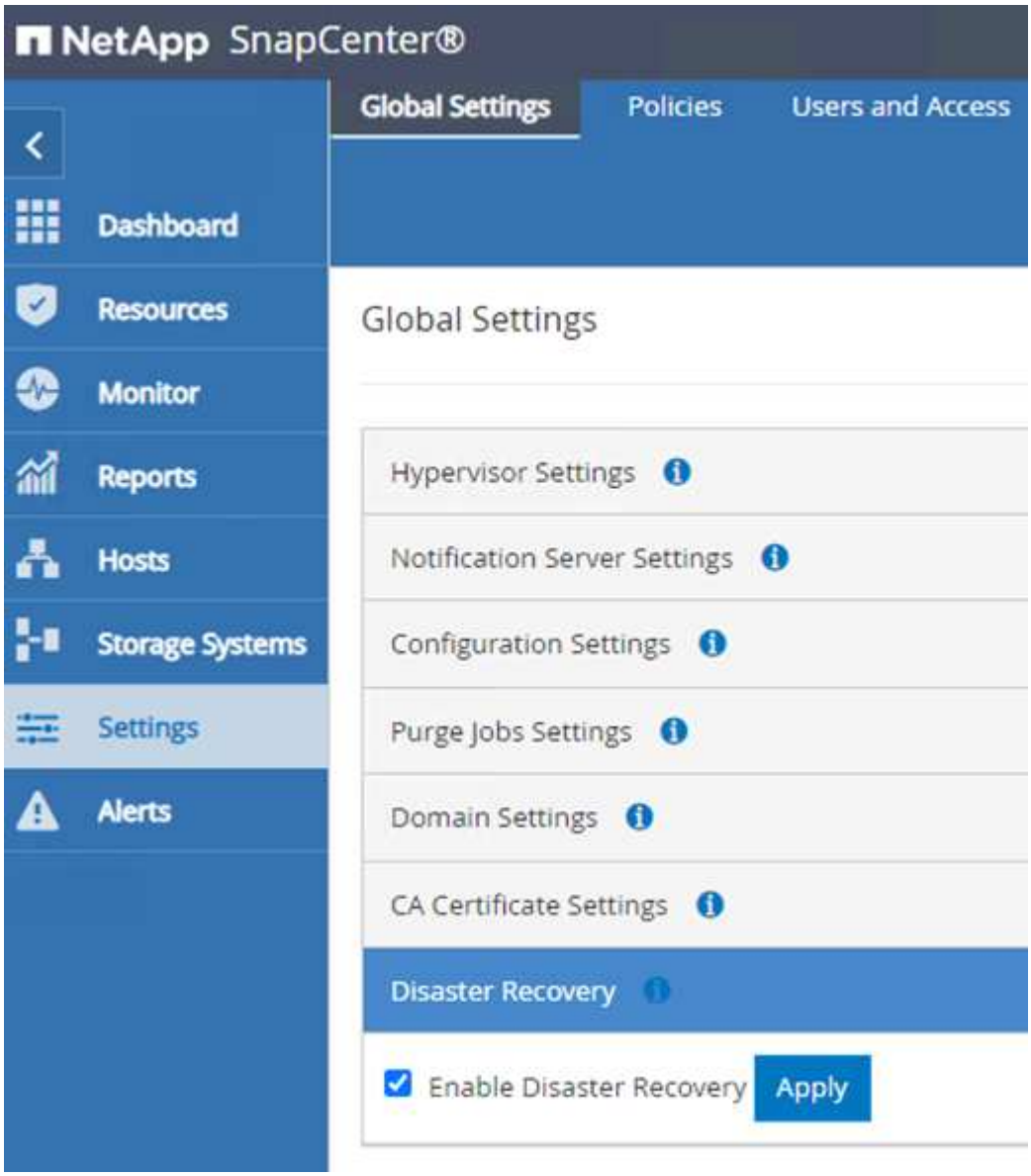


Confirme la comunicación de SnapCenter con el plugin de SQL Server

Cuando la base de datos SnapCenter se restaura a su estado anterior, se vuelven a detectar automáticamente los hosts de SQL Server. Para que esto funcione correctamente, tenga en cuenta los siguientes requisitos previos:

- SnapCenter debe ponerse en modo de recuperación ante desastres. Esto se puede realizar a través de la API de Swagger o con la configuración global en recuperación ante desastres.
- El FQDN de SQL Server debe ser idéntico a la instancia que se ejecutaba en el centro de datos local.
- Debe romperse la relación de SnapMirror original.
- Las LUN que contienen la base de datos deben montarse en la instancia de SQL Server y la base de datos adjunta.

Para confirmar que SnapCenter está en modo de recuperación ante desastres, vaya a Configuración desde el cliente web SnapCenter. Vaya a la ficha Configuración global y, a continuación, haga clic en recuperación ante desastres. Asegúrese de que la casilla Habilitar recuperación ante desastres esté habilitada.



Restaure los datos de la aplicación Oracle

El siguiente proceso proporciona instrucciones sobre cómo recuperar los datos de aplicaciones de Oracle en VMware Cloud Services en AWS en caso de un desastre que haga que el sitio local deje de funcionar.

Complete los siguientes requisitos previos para continuar con los pasos de recuperación:

1. La máquina virtual del servidor Oracle Linux se ha restaurado en el VMware Cloud SDDC con Veeam Full Restore.
2. Se ha establecido un servidor SnapCenter secundario y se han restaurado los archivos de base de datos y configuración de SnapCenter siguiendo los pasos descritos en esta sección "Resumen del proceso de backup y restauración de SnapCenter."

Configurar FSX para la restauración de Oracle – rompa la relación de SnapMirror

Para que los servidores Oracle puedan acceder a los volúmenes de almacenamiento secundario alojados en la instancia de FSxN, primero debe romper la relación de SnapMirror existente.

1. Después de iniciar sesión en la CLI de FSX, ejecute el siguiente comando para ver los volúmenes filtrados por el nombre correcto.

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

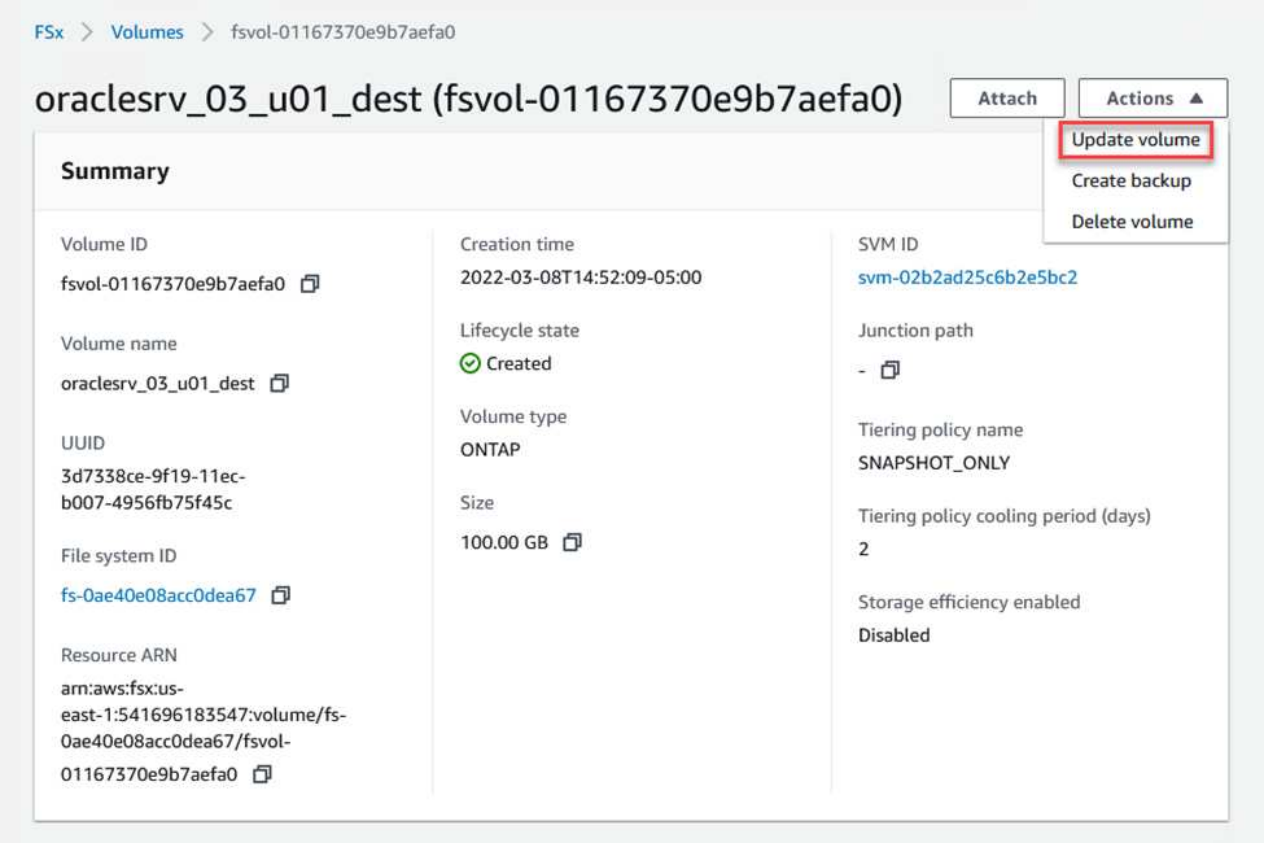
2. Ejecute el siguiente comando para interrumpir las relaciones de SnapMirror existentes.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

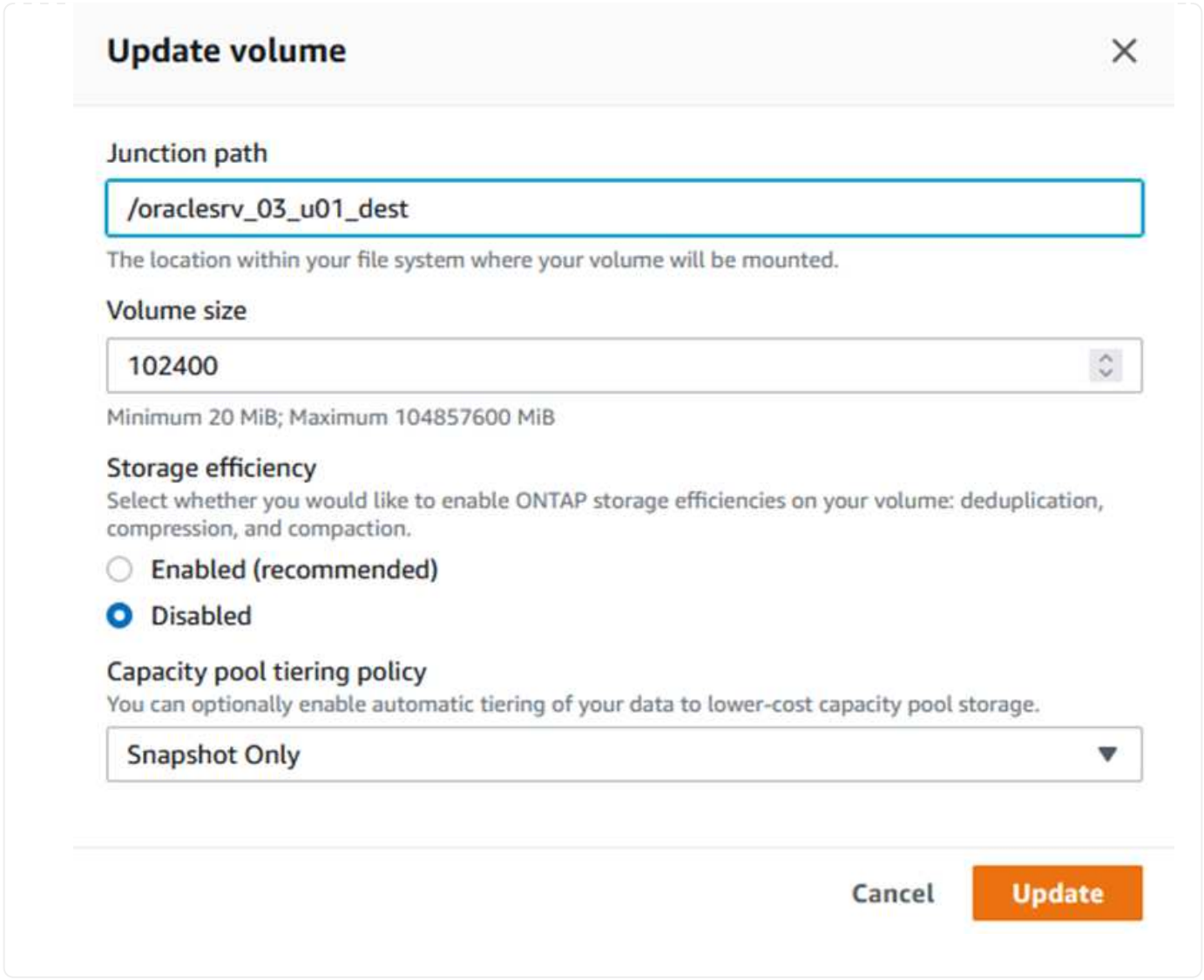
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Actualice la ruta de unión en el cliente web de Amazon FSX:



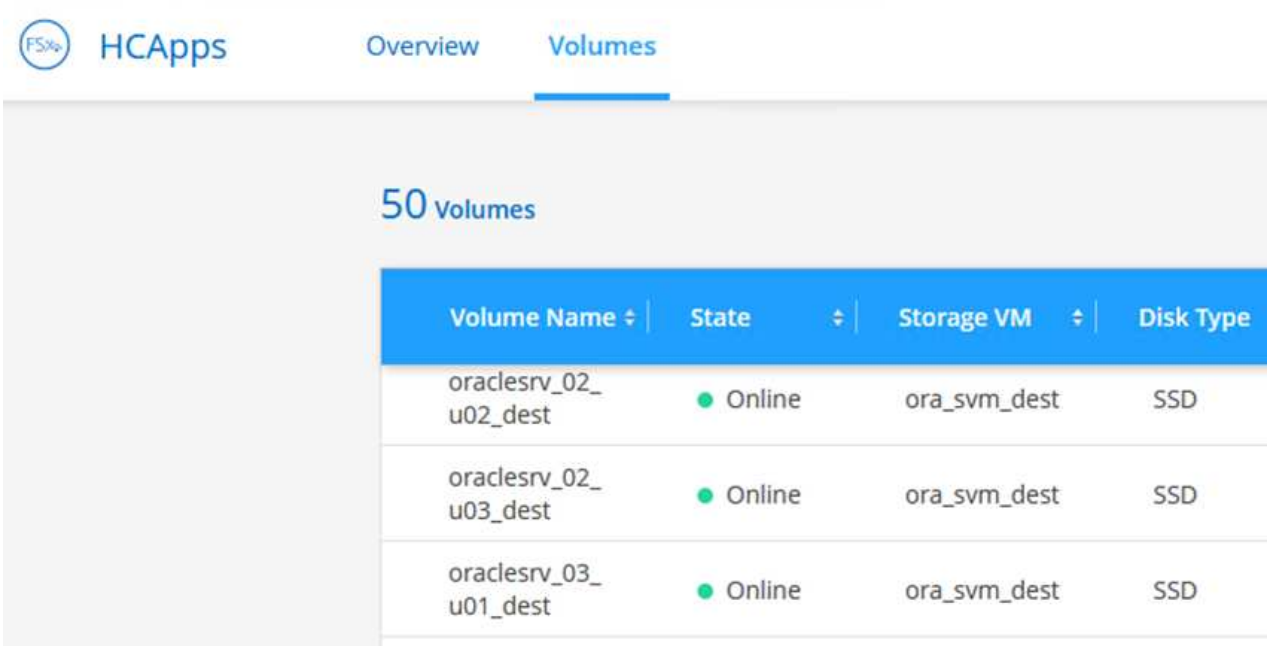
4. Añada el nombre de la ruta de unión y haga clic en Update. Especifique esta ruta de unión cuando monte el volumen NFS desde el servidor de Oracle.


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Snapshot Only
Cancel
Update

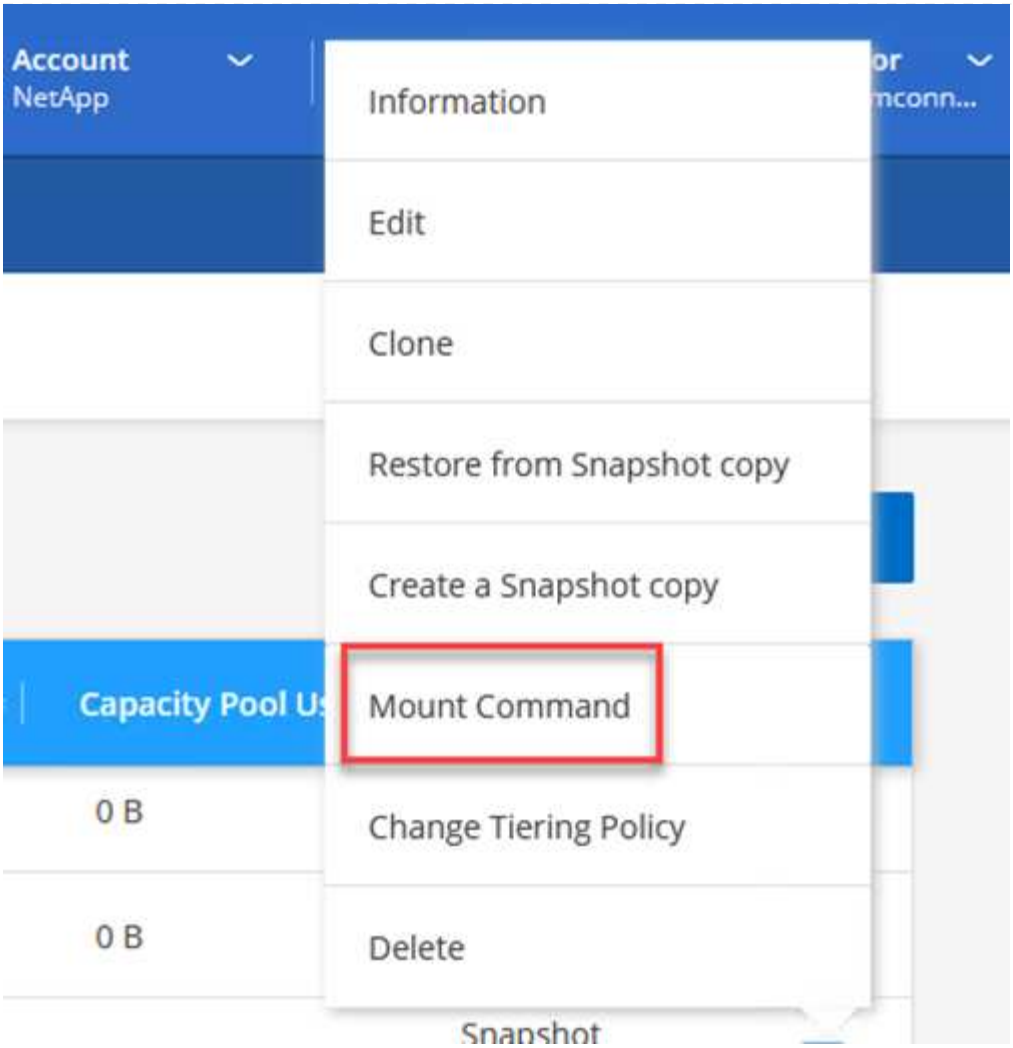
Montar volúmenes de NFS en Oracle Server

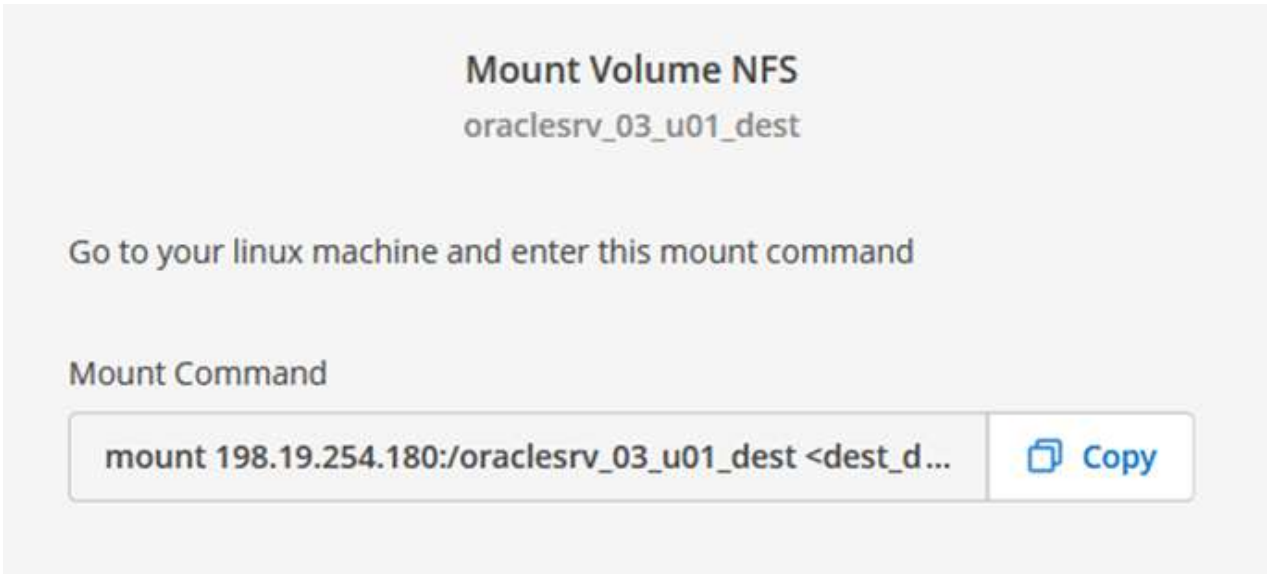
En Cloud Manager, puede obtener el comando de montaje con la dirección IP de LIF NFS correcta para montar los volúmenes NFS que contienen los registros y archivos de la base de datos de Oracle.

1. En Cloud Manager, acceda a la lista de volúmenes para el clúster FSX.



2. En el menú Action, seleccione Mount Command para ver y copiar el comando Mount que se va a utilizar en nuestro servidor Oracle Linux.





3. Monte el sistema de archivos NFS en el servidor Oracle Linux. Los directorios para montar el recurso compartido de NFS ya existen en el host Oracle Linux.
4. Desde el servidor Oracle Linux, utilice el comando Mount para montar los volúmenes NFS.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Repita este paso con cada volumen asociado con las bases de datos de Oracle.

Para que el montaje NFS sea coherente tras reiniciar, edite el `/etc/fstab` archivo para incluir los comandos de montaje.

5. Reinicie el servidor Oracle. Las bases de datos Oracle deben iniciarse normalmente y estar disponibles para su uso.

Conmutación tras recuperación

Una vez completado correctamente el proceso de conmutación al nodo de respaldo descrito en esta solución, SnapCenter y Veeam reanudan sus funciones de backup que se ejecutan en AWS. Además, FSX para ONTAP ahora se designa como almacenamiento principal sin relaciones de SnapMirror existentes con el centro de datos local original. Tras la reanudación de la función normal en las instalaciones, puede utilizar un proceso idéntico al descrito en esta documentación para reflejar los datos de nuevo en el sistema de almacenamiento ONTAP local.

Como también se describe en esta documentación, puede configurar SnapCenter para que refleje los volúmenes de datos de aplicaciones del FSX para ONTAP a un sistema de almacenamiento ONTAP que reside en las instalaciones. Asimismo, Veeam se puede configurar para que replique copias de backup en Amazon S3 utilizando un repositorio de backup de escalado horizontal para que estos backups estén accesibles a través de un servidor de backup de Veeam que se encuentra en el centro de datos local.

La conmutación por recuperación no está dentro del ámbito de esta documentación, pero la conmutación por recuperación difiere poco del proceso detallado que se describe aquí.

Conclusión

El caso de uso que se presenta en esta documentación se centra en tecnologías probadas de recuperación ante desastres que destacan la integración entre NetApp y VMware. Los sistemas de almacenamiento ONTAP de NetApp proporcionan tecnologías contrastadas de mirroring de datos que permiten a las organizaciones diseñar soluciones de recuperación ante desastres que abarcan las tecnologías ONTAP y en las instalaciones que residen con los proveedores de cloud líderes.

FSX para ONTAP en AWS es una solución de este tipo que permite una integración fluida con SnapCenter y SyncMirror para replicar datos de aplicaciones en el cloud. Veeam Backup & Replication es otra tecnología muy conocida que se integra bien con los sistemas de almacenamiento ONTAP de NetApp y puede proporcionar conmutación al nodo de respaldo al almacenamiento nativo de vSphere.

Esta solución presentó una solución de recuperación ante desastres utilizando el almacenamiento «guest connect» en un sistema ONTAP que aloja datos de aplicaciones de SQL Server y Oracle. SnapCenter con SnapMirror proporciona una solución fácil de gestionar para proteger volúmenes de aplicaciones en sistemas ONTAP y replicarlos en FSX o CVO que residen en el cloud. SnapCenter es una solución preparada para recuperación ante desastres que permite conmutar por error todos los datos de aplicaciones al cloud de VMware en AWS.

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios

web:

- Enlaces a la documentación de la solución

  "Multicloud híbrido de NetApp con soluciones de VMware"

  "Soluciones NetApp"

Backup y restauración de Veeam en VMware Cloud, con Amazon FSx para ONTAP

Autor: Josh Powell: Ingeniería de soluciones de NetApp

Descripción general

Veeam Backup & Replication es una solución efectiva y fiable para proteger datos en VMware Cloud. Esta solución demuestra la instalación y la configuración adecuadas para usar Backup and Replication de Veeam para realizar backups y restaurar VM de aplicaciones que residen en almacenes de datos NFS de FSx para ONTAP en VMware Cloud.

VMware Cloud (en AWS) admite el uso de almacenes de datos NFS como almacenamiento complementario, y FSx para ONTAP de NetApp es una solución segura para clientes que necesitan almacenar grandes cantidades de datos para sus aplicaciones en la nube y que pueden escalar independientemente del número de hosts ESXi en el clúster SDDC. Este servicio de almacenamiento integrado de AWS ofrece un almacenamiento altamente eficiente con todas las funcionalidades tradicionales de ONTAP de NetApp.

Casos de uso

Esta solución aborda los siguientes casos prácticos:

- Backup y restauración de máquinas virtuales de Windows y Linux alojadas en VMC usando FSx para NetApp ONTAP como repositorio de backup.
- Backup y restauración de datos de aplicaciones de Microsoft SQL Server mediante FSx para NetApp ONTAP como repositorio de backup.
- Realiza backups y restauraciones de datos de aplicaciones de Oracle usando FSx para NetApp ONTAP como repositorio de backup.

Almacenes de datos NFS mediante Amazon FSx para ONTAP

Todas las máquinas virtuales de esta solución residen en almacenes de datos NFS complementarios de FSx para ONTAP. Usar FSx for ONTAP como almacén de datos NFS complementario tiene varias ventajas. Por ejemplo, le permite:

- Cree un sistema de archivos escalable y de alta disponibilidad en el cloud sin necesidad de una configuración y gestión complejas.
- Se integra con tu entorno de VMware actual y te permite utilizar herramientas y procesos conocidos para gestionar los recursos en la nube.
- Benefíciese de las funciones avanzadas de gestión de datos que ofrece ONTAP, como las copias Snapshot y la replicación, para proteger sus datos y garantizar su disponibilidad.

Descripción general de la puesta en marcha de soluciones

Esta lista ofrece los pasos de alto nivel necesarios para configurar Veeam Backup & Replication, ejecutar tareas de backup y restauración con FSx para ONTAP como repositorio de backup y realizar restauraciones de máquinas virtuales y bases de datos de SQL Server y Oracle:

1. Cree el sistema de archivos FSx para ONTAP que se utilizará como repositorio de backup iSCSI para Veeam Backup & Replication.
2. Pon en marcha Veeam Proxy para distribuir las cargas de trabajo de backup y montar los repositorios de backup de iSCSI alojados en FSx para ONTAP.
3. Configure Veeam Backup Jobs para realizar copias de seguridad de máquinas virtuales de SQL Server, Oracle, Linux y Windows.
4. Restaure máquinas virtuales de SQL Server y bases de datos individuales.
5. Restaurar máquinas virtuales de Oracle y bases de datos individuales.

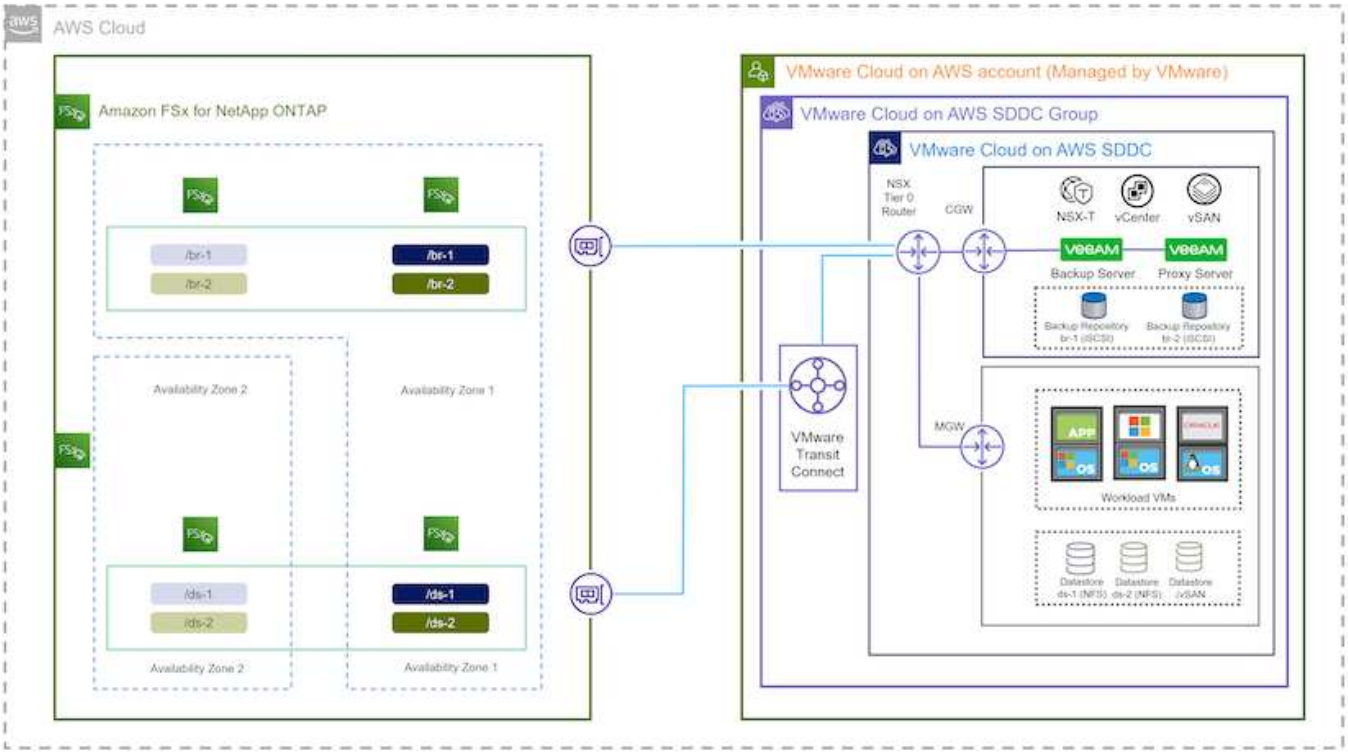
Requisitos previos

El objetivo de esta solución es demostrar la protección de datos de máquinas virtuales que se ejecutan en VMware Cloud y ubicadas en almacenes de datos NFS alojados por FSx for NetApp ONTAP. Esta solución asume que los siguientes componentes están configurados y listos para su uso:

1. FSX para el sistema de archivos ONTAP con uno o varios almacenes de datos NFS conectados a VMware Cloud.
2. Máquina virtual de Microsoft Windows Server con software Veeam Backup & Replication instalado.
    - El servidor Veeam Backup & Replication ha detectado el servidor vCenter con su dirección IP o un nombre de dominio completo.
3. Máquina virtual de Microsoft Windows Server que se instalará con los componentes de Veeam Backup Proxy durante la implementación de la solución.
4. Máquinas virtuales de Microsoft SQL Server con VMDK y datos de aplicaciones que residen en FSx para almacenes de datos NFS de ONTAP. Para esta solución teníamos dos bases de datos de SQL en dos VMDK separados.
    - Nota: Como práctica recomendada, los archivos de registro de transacciones y base de datos se colocan en unidades separadas, ya que esto mejorará el rendimiento y la fiabilidad. Esto se debe en parte al hecho de que los registros de transacciones se escriben de forma secuencial, mientras que los archivos de base de datos se escriben de forma aleatoria.
5. Máquinas virtuales de Oracle Database con VMDK y datos de aplicación que residen en FSx para almacenes de datos NFS de ONTAP.
6. Máquinas virtuales de servidores de archivos Linux y Windows con VMDK que residen en FSx para almacenes de datos NFS de ONTAP.
7. Veeam requiere puertos TCP específicos para la comunicación entre servidores y componentes en el entorno de backup. En los componentes de la infraestructura de copia de seguridad de Veeam, las reglas de firewall necesarias se crean automáticamente. Para ver una lista completa de los requisitos del puerto de red, consulte la sección Puertos de "Guía del usuario de backup y replicación de Veeam para VMware vSphere".

Arquitectura de alto nivel

Las pruebas y la validación de esta solución se llevaron a cabo en un laboratorio que puede o no coincidir con el entorno de puesta en marcha final. Para obtener más información, consulte las siguientes secciones.



Componentes de hardware/software

El objetivo de esta solución es demostrar la protección de datos de máquinas virtuales que se ejecutan en VMware Cloud y ubicadas en almacenes de datos NFS alojados por FSx for NetApp ONTAP. Esta solución asume que los siguientes componentes ya están configurados y listos para su uso:

- VM de Microsoft Windows ubicadas en un almacén de datos NFS de ONTAP FSx
- Equipos virtuales de Linux (CentOS) ubicados en FSx para un almacén de datos NFS de ONTAP
- Máquinas virtuales de Microsoft SQL Server ubicadas en un almacén de datos NFS de FSx para ONTAP
  - Dos bases de datos alojadas en VMDK independientes
- Oracle VM ubicadas en un almacén de datos NFS de ONTAP FSx

Puesta en marcha de la solución

En esta solución proporcionamos instrucciones detalladas para implementar y validar una solución utilizando el software Veeam Backup and Replication para realizar la copia de seguridad y recuperación de máquinas virtuales de servidores de archivos de SQL Server, Oracle, Windows y Linux en un SDDC de VMware Cloud en AWS. Las máquinas virtuales de esta solución residen en un almacén de datos NFS complementario alojado por FSx para ONTAP. Además, se utiliza un sistema de archivos FSx para ONTAP aparte para alojar volúmenes iSCSI que se utilizarán para los repositorios de backup de Veeam.

Repasaremos FSx para la creación del sistema de archivos de ONTAP, el montaje de los volúmenes iSCSI

que se utilizarán como repositorios de backup, la creación y la ejecución de tareas de backup, así como la realización de restauraciones de máquinas virtuales y bases de datos.

Para obtener información detallada sobre FSx para ONTAP de NetApp, consulte la "Guía de usuario de FSx para ONTAP".

Para obtener información detallada sobre Veeam Backup and Replication, consulte la "Documentación técnica del centro de ayuda de Veeam" sitio.

Para conocer las consideraciones y limitaciones al usar Veeam Backup and Replication con VMware Cloud en AWS, consulte "VMware Cloud en AWS y VMware Cloud en soporte de Dell EMC. Consideraciones y limitaciones".

Implemente el servidor proxy de Veeam

Un servidor proxy de Veeam es un componente del software Veeam Backup & Replication que actúa como intermediario entre el origen y el destino de backup o replicación. El servidor proxy ayuda a optimizar y acelerar la transferencia de datos durante los trabajos de copia de seguridad mediante el procesamiento local de los datos y puede utilizar diferentes modos de transporte para acceder a los datos mediante las API de VMware vStorage para la protección de datos o mediante el acceso directo al almacenamiento.

Al elegir un diseño de servidor proxy de Veeam, es importante tener en cuenta el número de tareas simultáneas y el modo de transporte o el tipo de acceso de almacenamiento deseado.

Para determinar el tamaño del número de servidores proxy y los requisitos de su sistema, consulte la "Guía de prácticas recomendadas de Veeam VMware vSphere".

Veeam Data Mover es un componente del servidor proxy de Veeam y utiliza un modo de transporte como método para obtener datos de VM del origen y transferirlos al destino. El modo de transporte se especifica durante la configuración del trabajo de copia de seguridad. Es posible aumentar la eficiencia de los backups de los almacenes de datos NFS utilizando el acceso directo al almacenamiento.

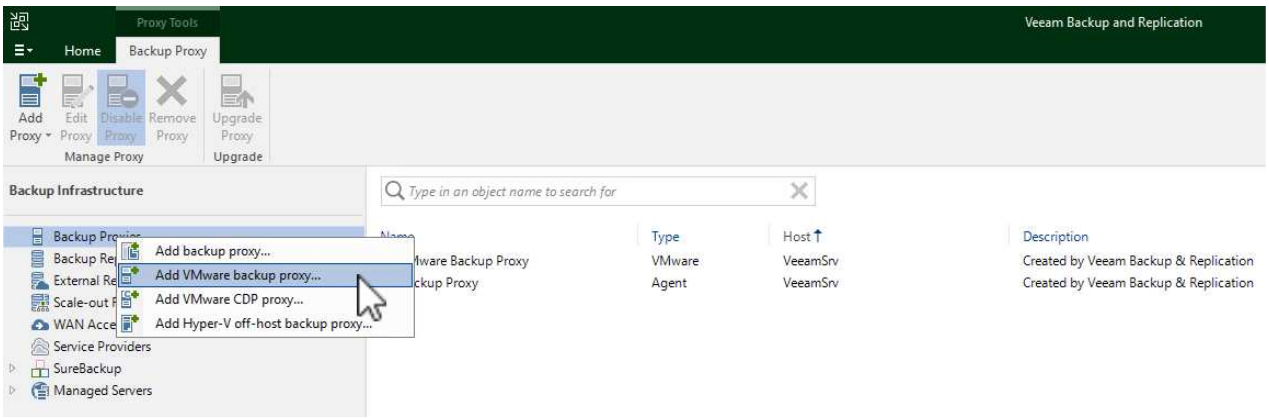
Para obtener más información sobre los modos de transporte, consulte la "Guía del usuario de backup y replicación de Veeam para VMware vSphere".

En el siguiente paso, cubrimos la implementación del Veeam Proxy Server en una VM de Windows en el SDDC de VMware Cloud.

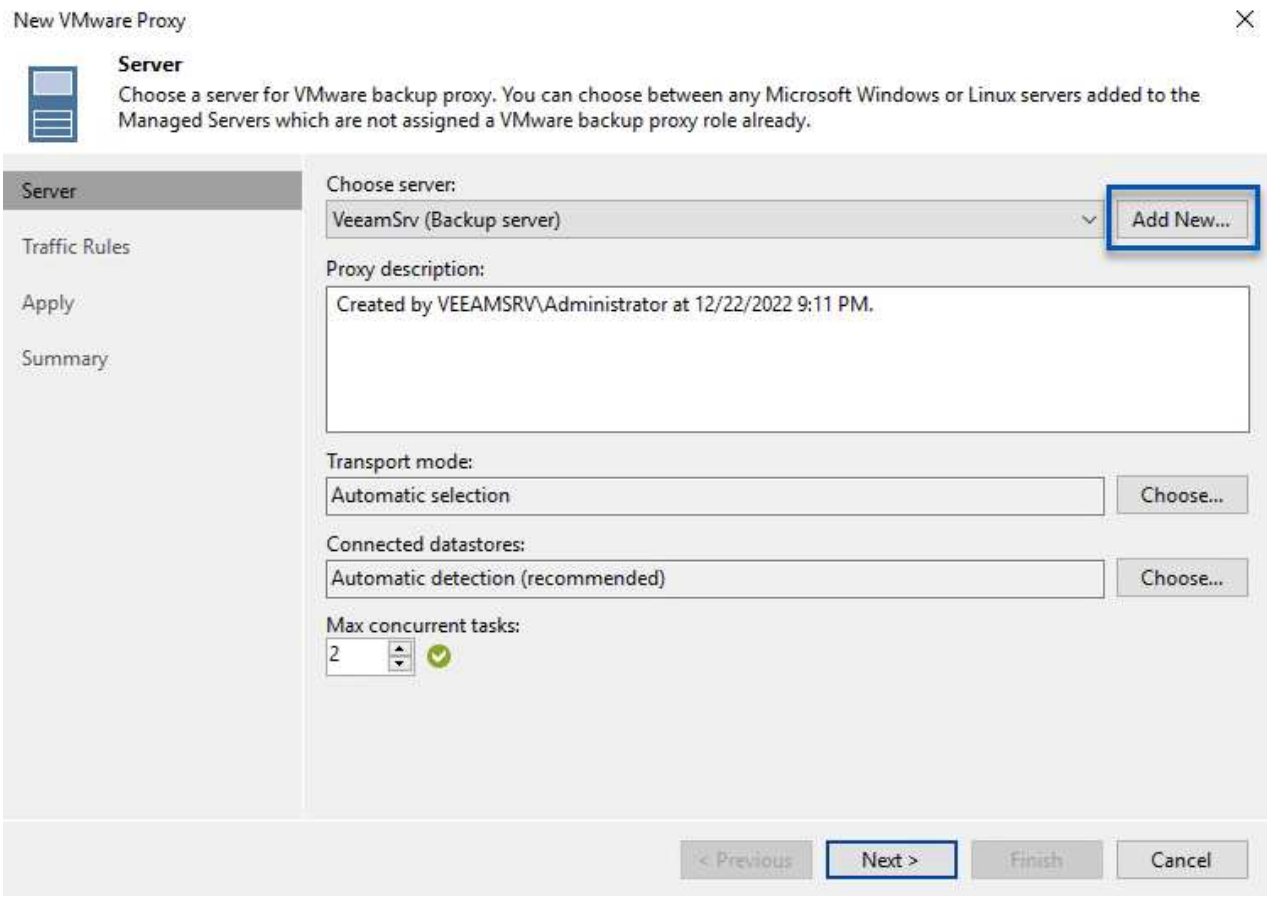
Implemente Veeam Proxy para distribuir las cargas de trabajo de backup

En este paso, Veeam Proxy se implementa en una VM de Windows existente. Esto permite que los trabajos de backup se distribuyan entre el Veeam Backup Server principal y Veeam Proxy.

1. En el servidor Veeam Backup and Replication, abra la consola de administración y seleccione **Infraestructura de copia de seguridad** en el menú inferior izquierdo.
2. Haga clic derecho en **Proxies de copia de seguridad** y haga clic en **Agregar proxy de copia de seguridad de VMware…** para abrir el asistente.

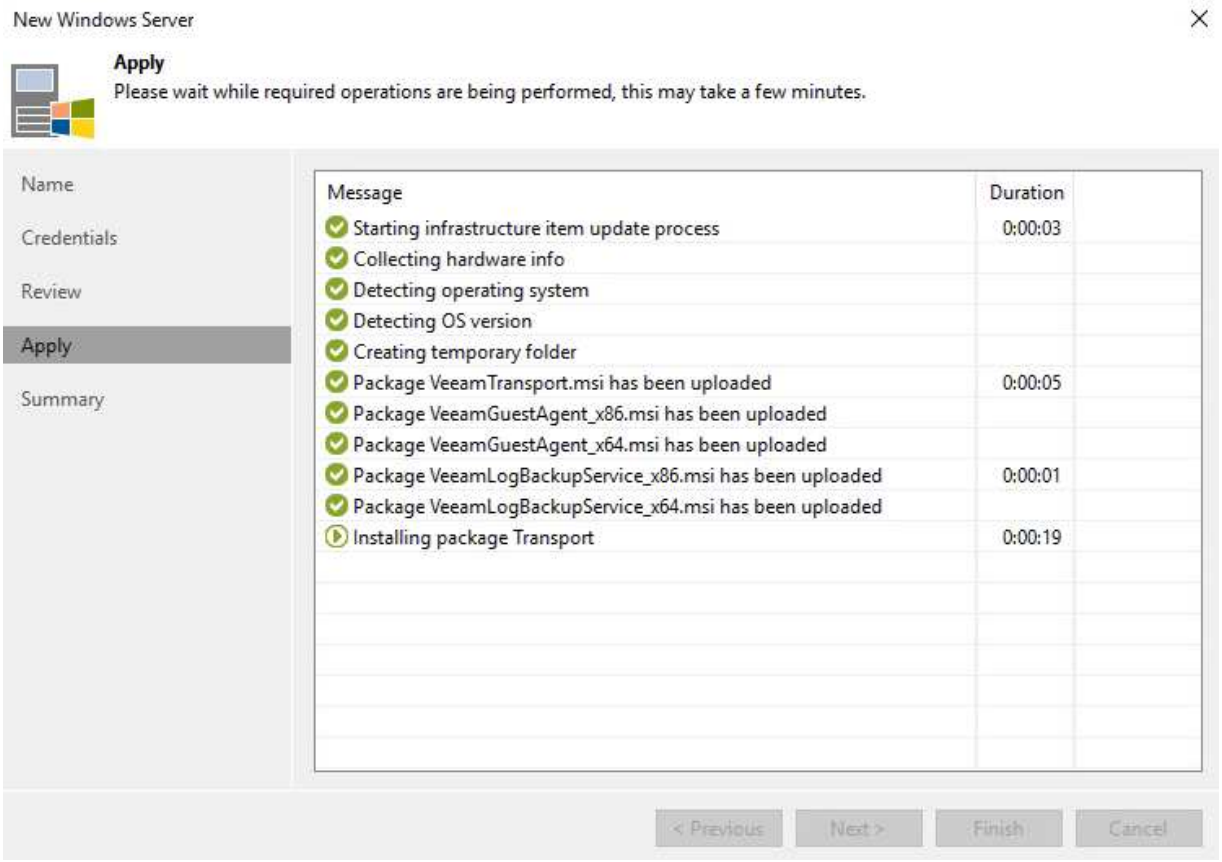


3. En el asistente de **Agregar proxy VMware**, haga clic en el botón **Agregar nuevo…** para agregar un nuevo servidor proxy.

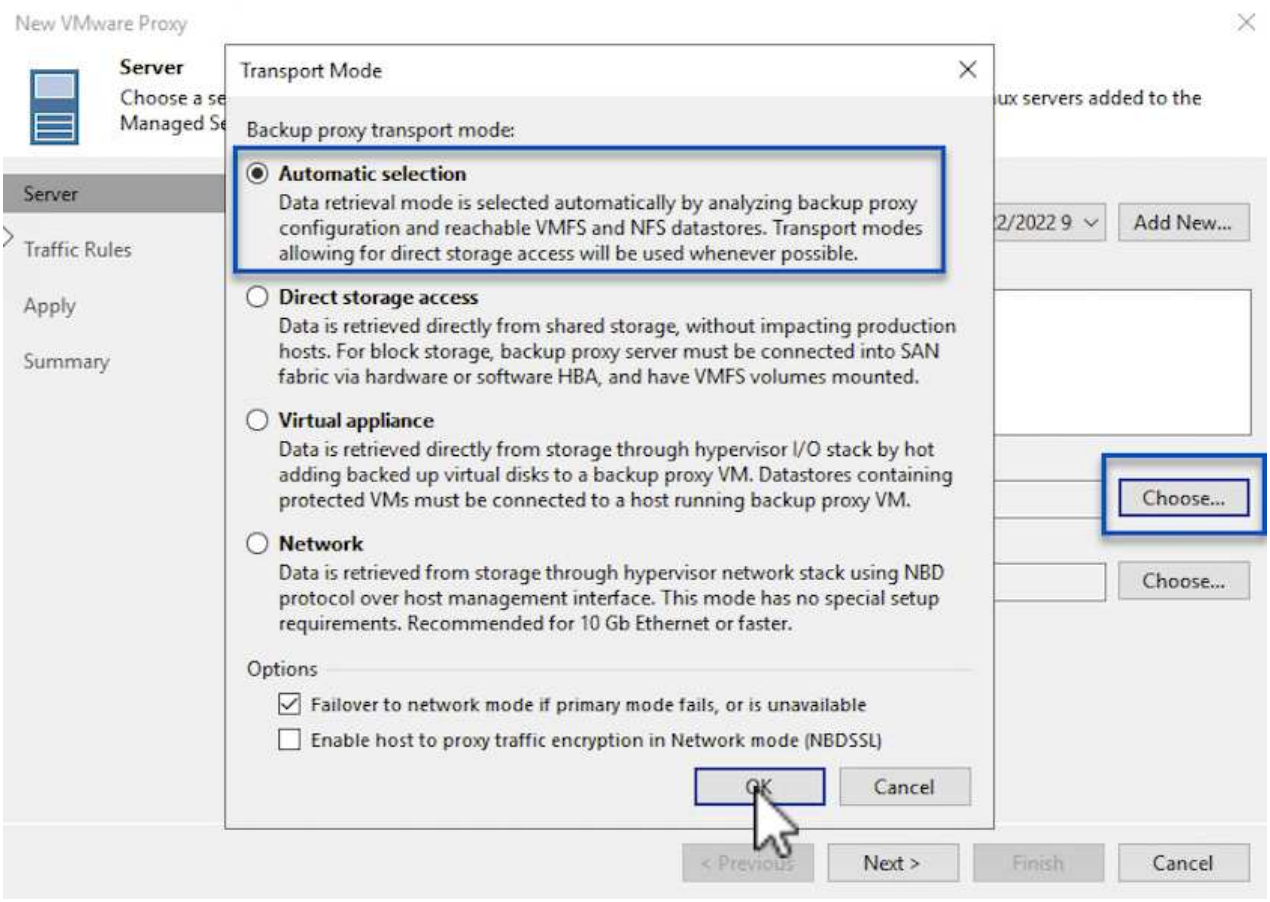


4. Seleccione para agregar Microsoft Windows y siga las indicaciones para agregar el servidor:

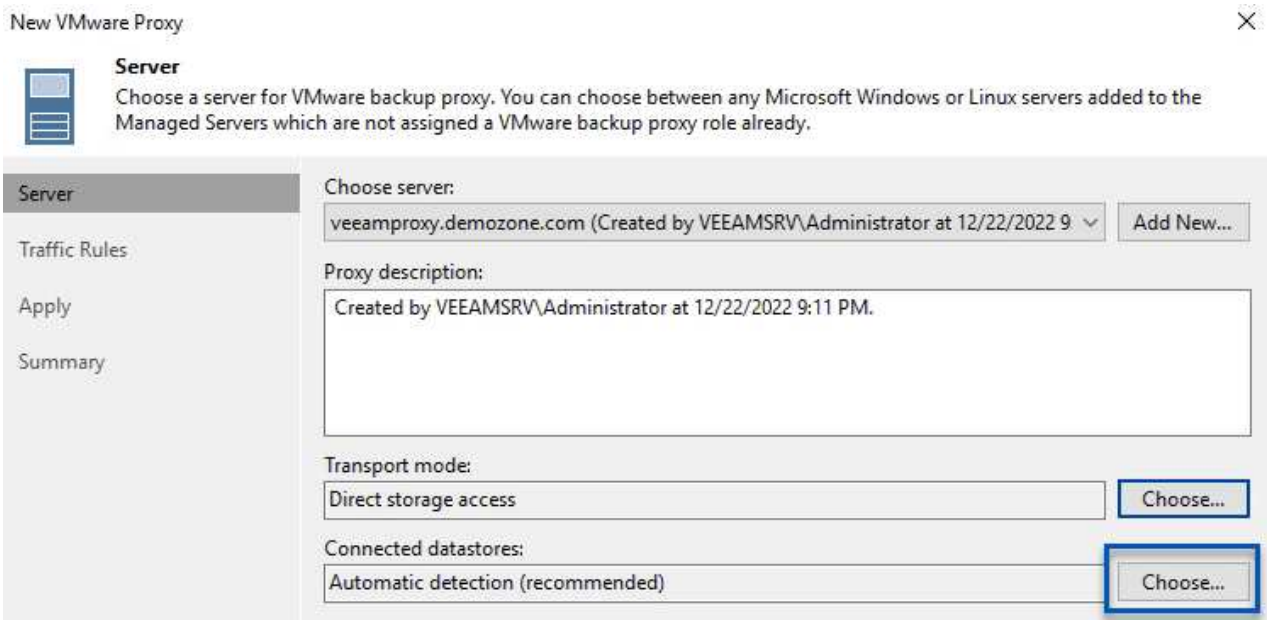
- Rellene el nombre DNS o la dirección IP
- Seleccione una cuenta para utilizar las credenciales en el nuevo sistema o agregue nuevas credenciales
- Revise los componentes que se van a instalar y luego haga clic en **Aplicar** para comenzar la implementación

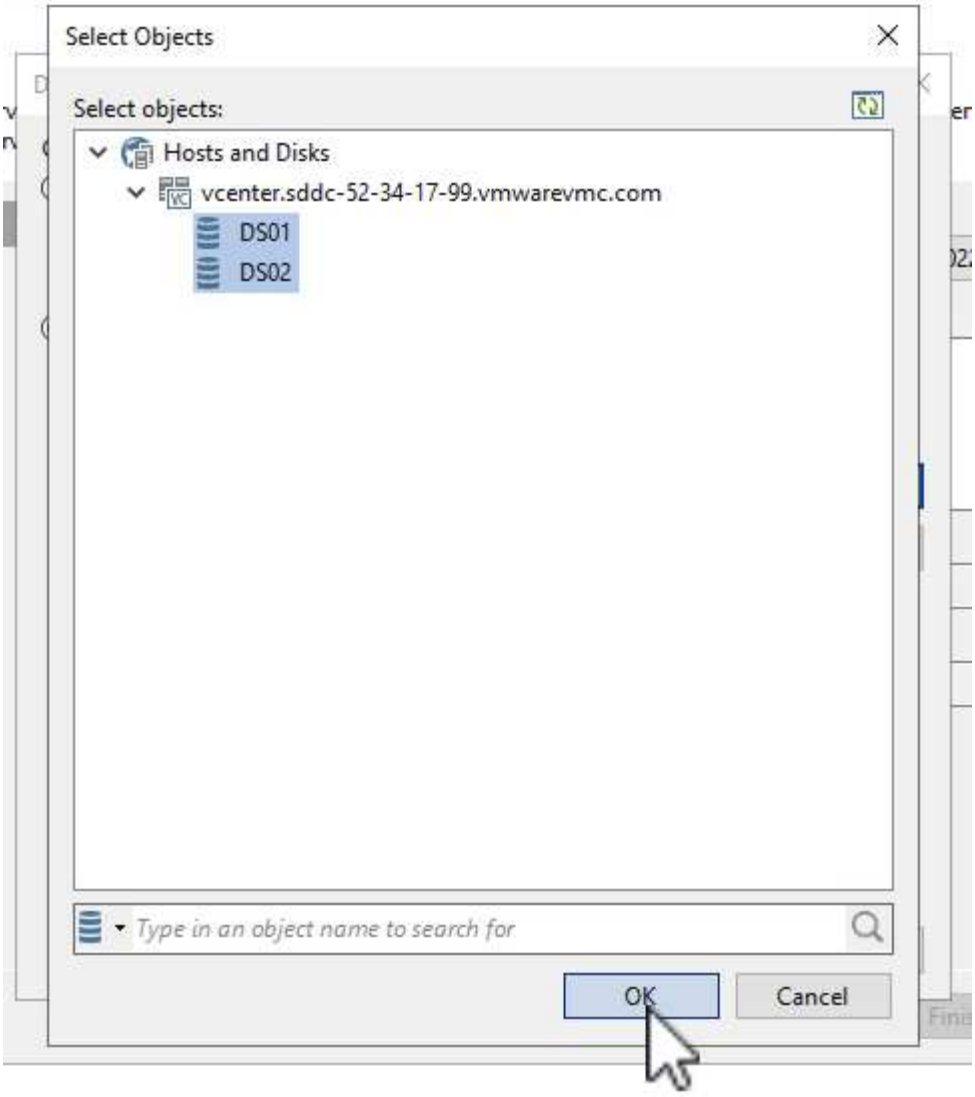


5. De nuevo en el asistente de **New VMware Proxy**, elija un modo de transporte. En nuestro caso elegimos **Selección Automática**.

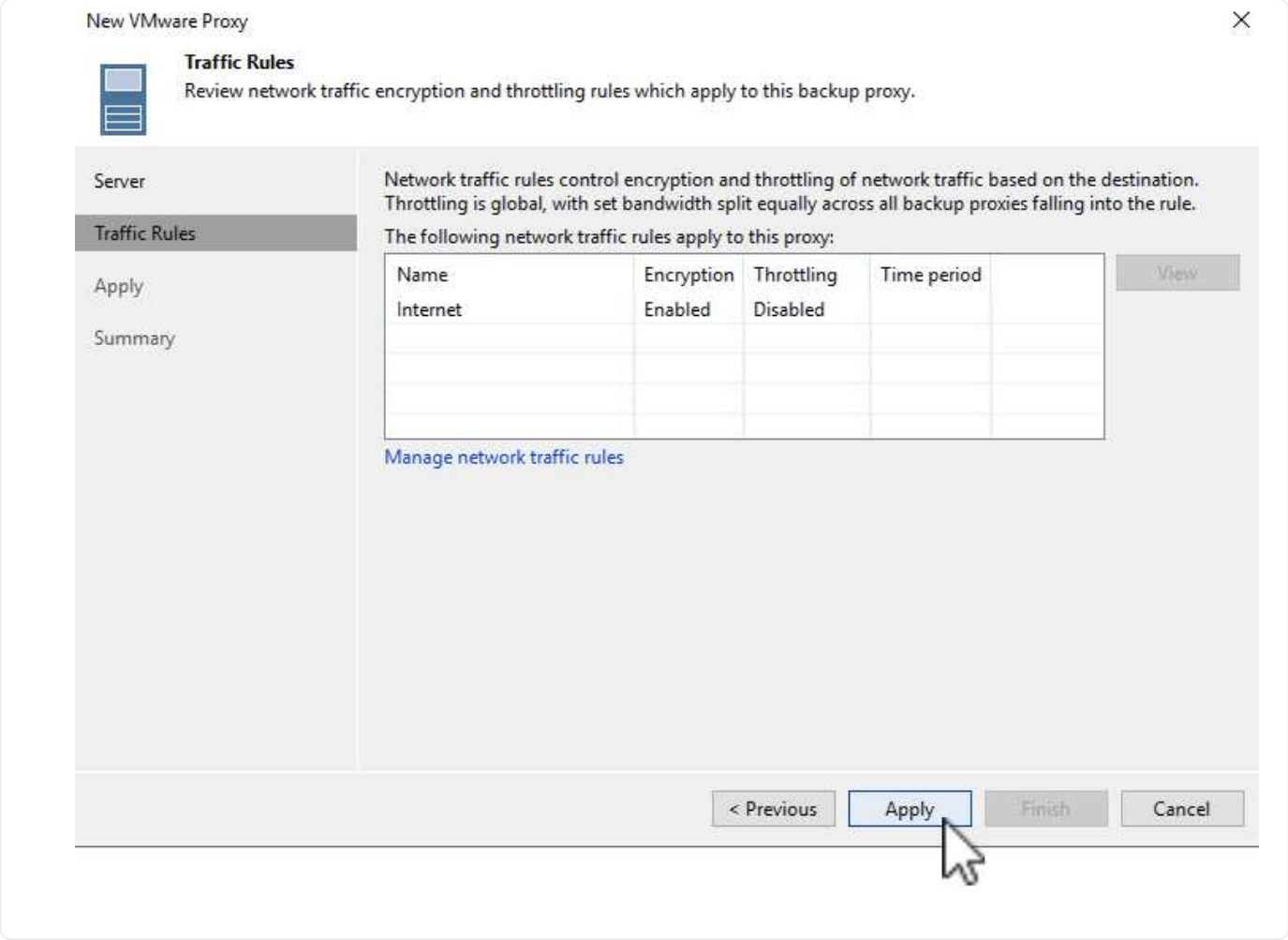


6. Seleccione los almacenes de datos conectados a los que desea que VMware Proxy tenga acceso directo.





7. Configure y aplique las reglas de tráfico de red específicas, como el cifrado o la limitación que desee. Cuando termine, haga clic en el botón **Aplicar** para completar la implementación.



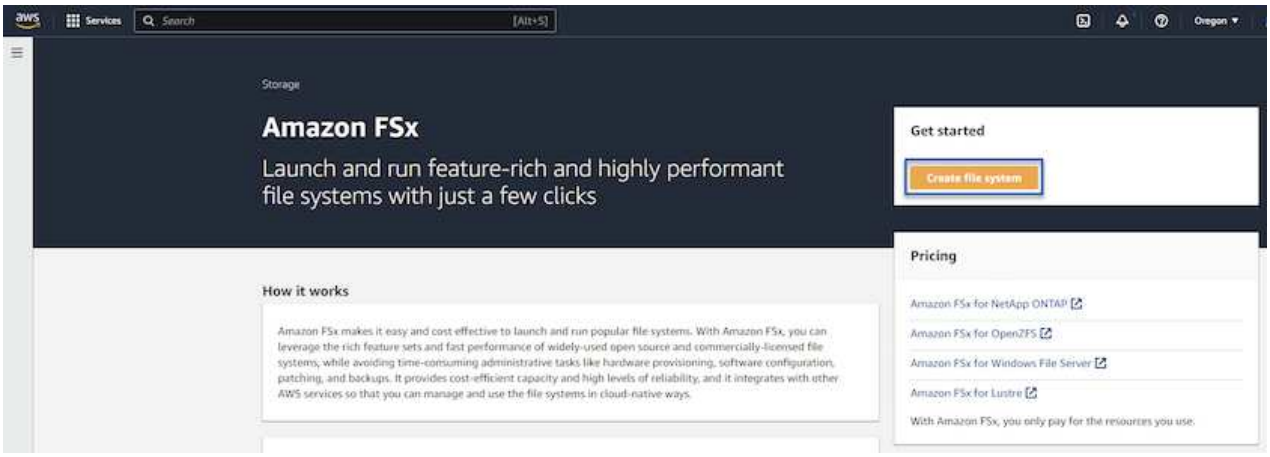
Configurar Repositorios de Almacenamiento y Copia de Seguridad

El servidor principal de Veeam Backup y el servidor Veeam Proxy tienen acceso a un repositorio de respaldo en forma de almacenamiento conectado directamente. En esta sección trataremos la creación de un sistema de archivos FSx for ONTAP, el montaje de LUN iSCSI en los servidores de Veeam y la creación de repositorios de backup.

Crear FSX para el sistema de archivos ONTAP

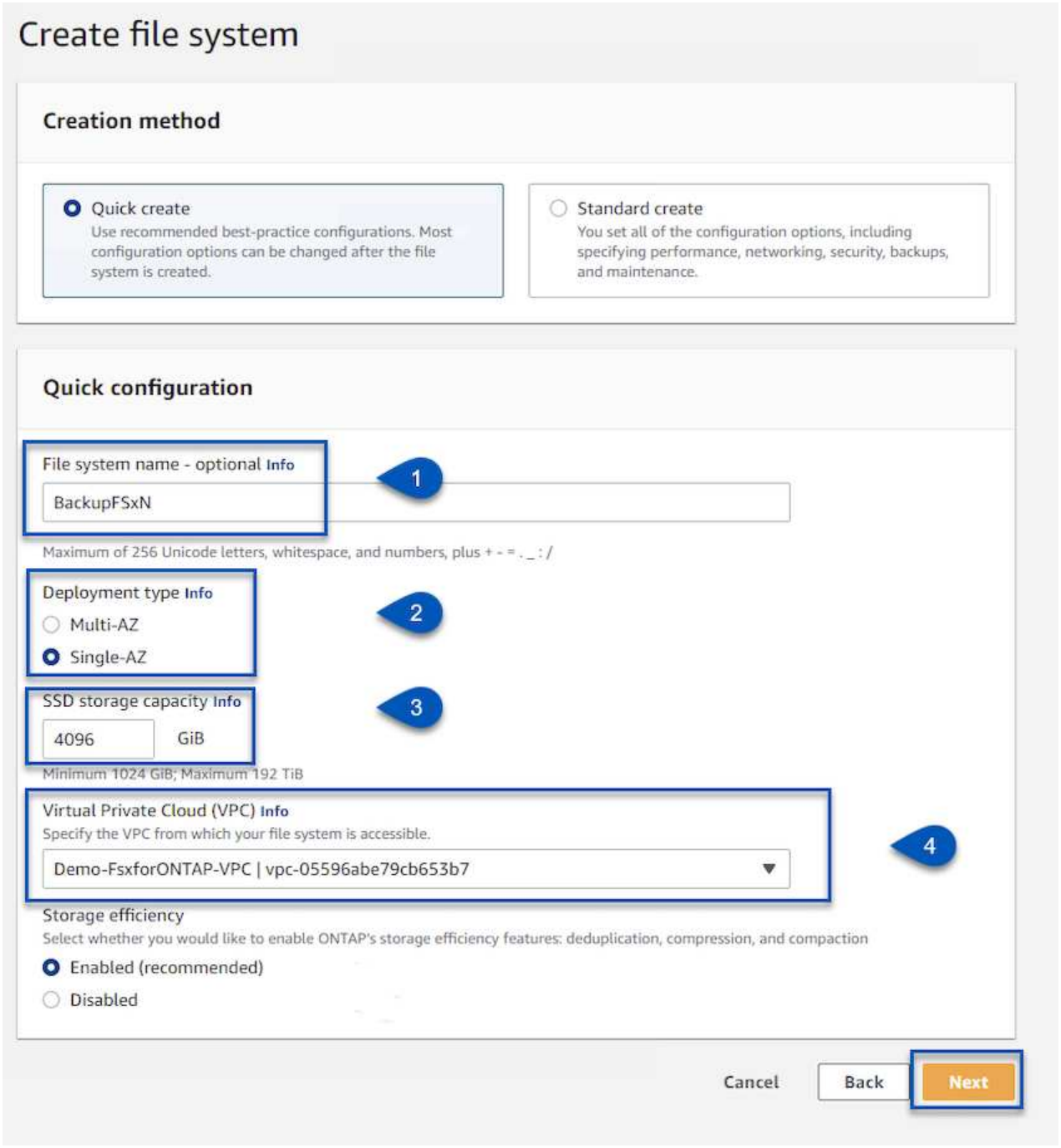
Cree un sistema de archivos FSx para ONTAP que se utilizará para alojar los volúmenes iSCSI para los repositorios de backup de Veeam.

1. En la consola de AWS, vaya a FSX y luego a **Crear sistema de archivos**



2. Selecciona **Amazon FSx para ONTAP de NetApp** y, a continuación, **Siguiente** para continuar.

3. Rellene el nombre del sistema de archivos, el tipo de puesta en marcha, la capacidad de almacenamiento SSD y la VPC en la que residirá el clúster de FSx para ONTAP. Debe ser una VPC configurada para comunicarse con la red de máquina virtual en VMware Cloud. Haga clic en **Siguiente**.



4. Revise los pasos de implementación y haga clic en **Crear sistema de archivos** para comenzar el proceso de creación del sistema de archivos.

Configuración y montaje de LUN iSCSI

Crear y configurar los LUN iSCSI en FSx para ONTAP y montarlos en los servidores proxy y de backup de Veeam. Estos LUN se usarán más adelante para crear repositorios de backup de Veeam.

> La creación de una LUN iSCSI en FSx para ONTAP es un proceso de varios pasos. El primer paso de creación de los volúmenes puede realizarse en la consola de Amazon FSx o con la CLI de ONTAP de NetApp.

> Para obtener más información sobre cómo usar FSx para ONTAP, consulta la "Guía de usuario de FSx para ONTAP".

1. En la CLI de ONTAP de NetApp, cree los volúmenes iniciales mediante el siguiente comando:

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. Cree LUN con los volúmenes que se crearon en el paso anterior:

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Conceda acceso a las LUN creando un iGroup que contenga el IQN iSCSI de los servidores proxy y de backup de Veeam:

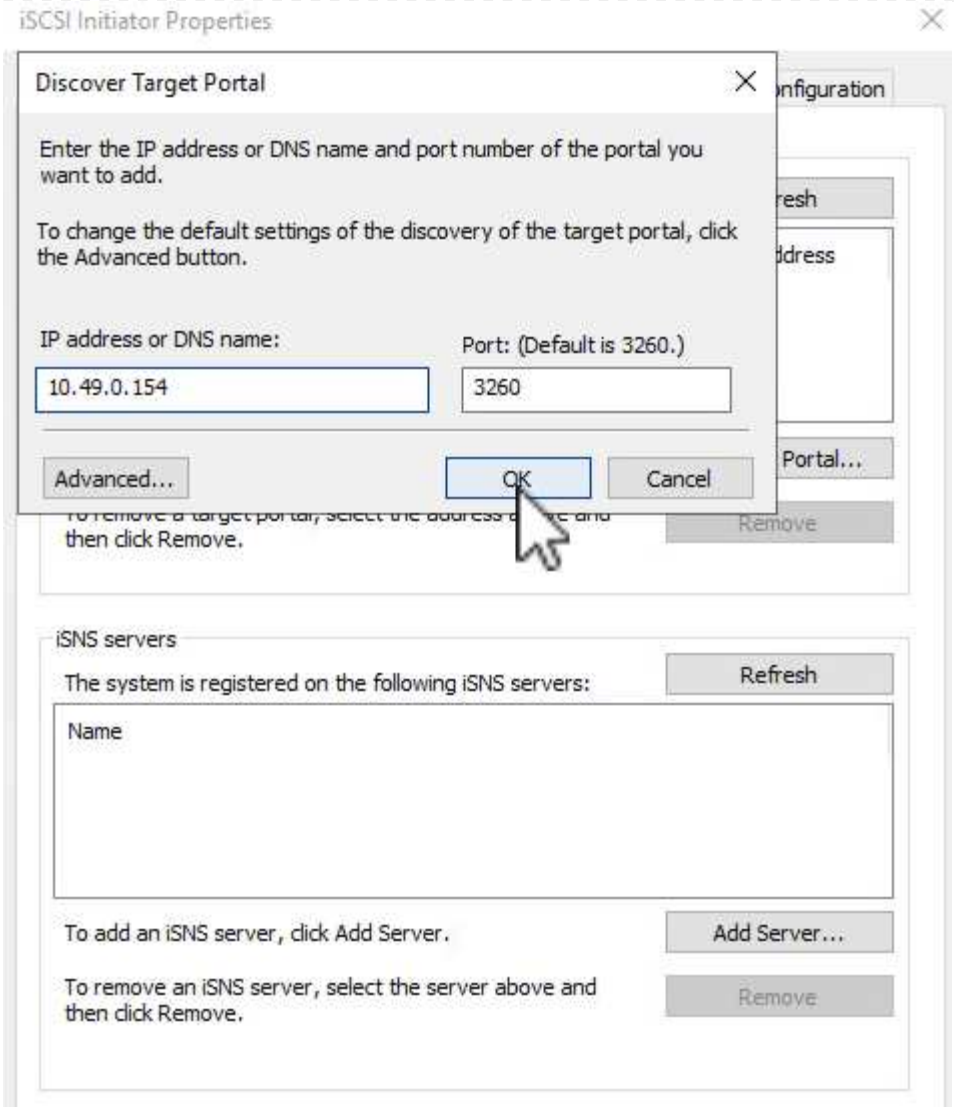
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

> Para completar el paso anterior, primero deberá recuperar el IQN de las propiedades del iniciador iSCSI en los servidores Windows.

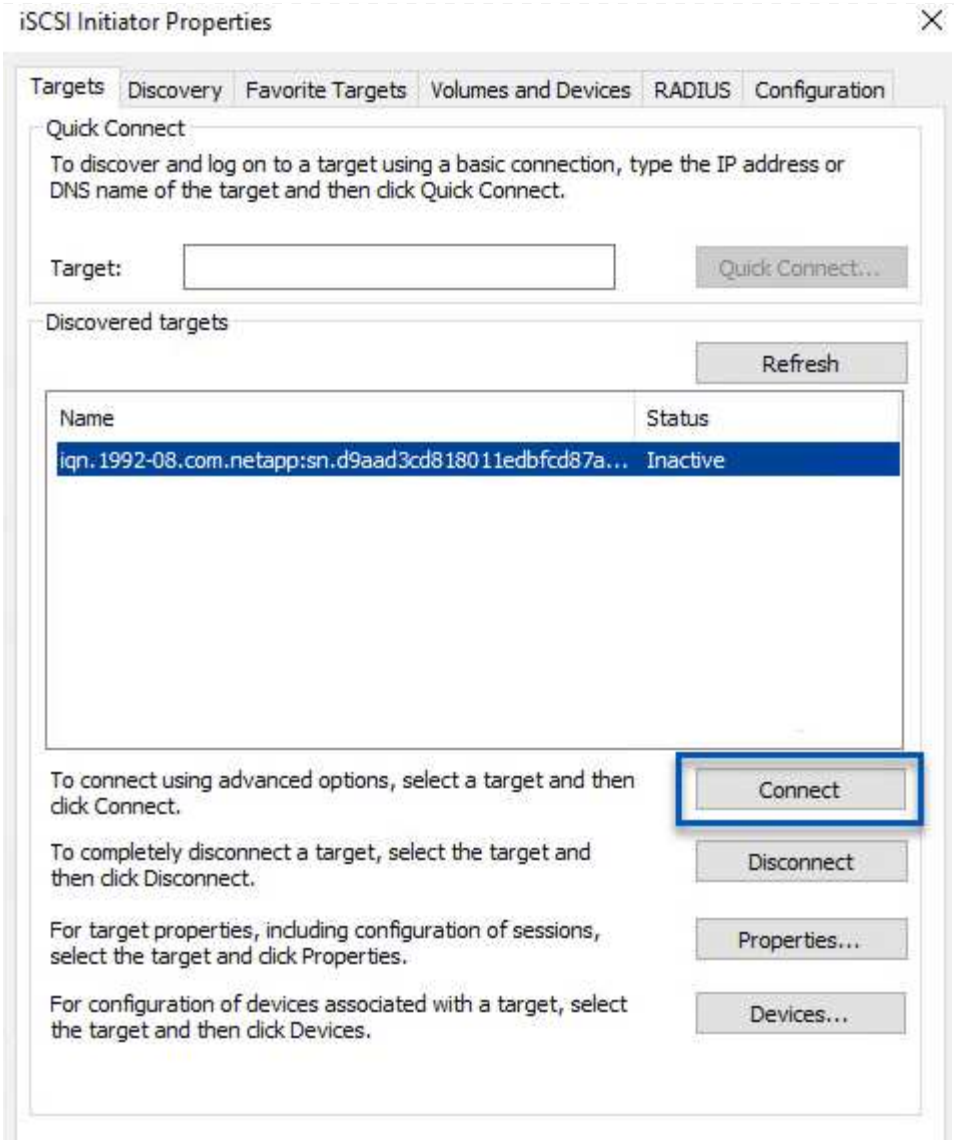
4. Finalmente, asigne las LUN al iGroup que acaba de crear:

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

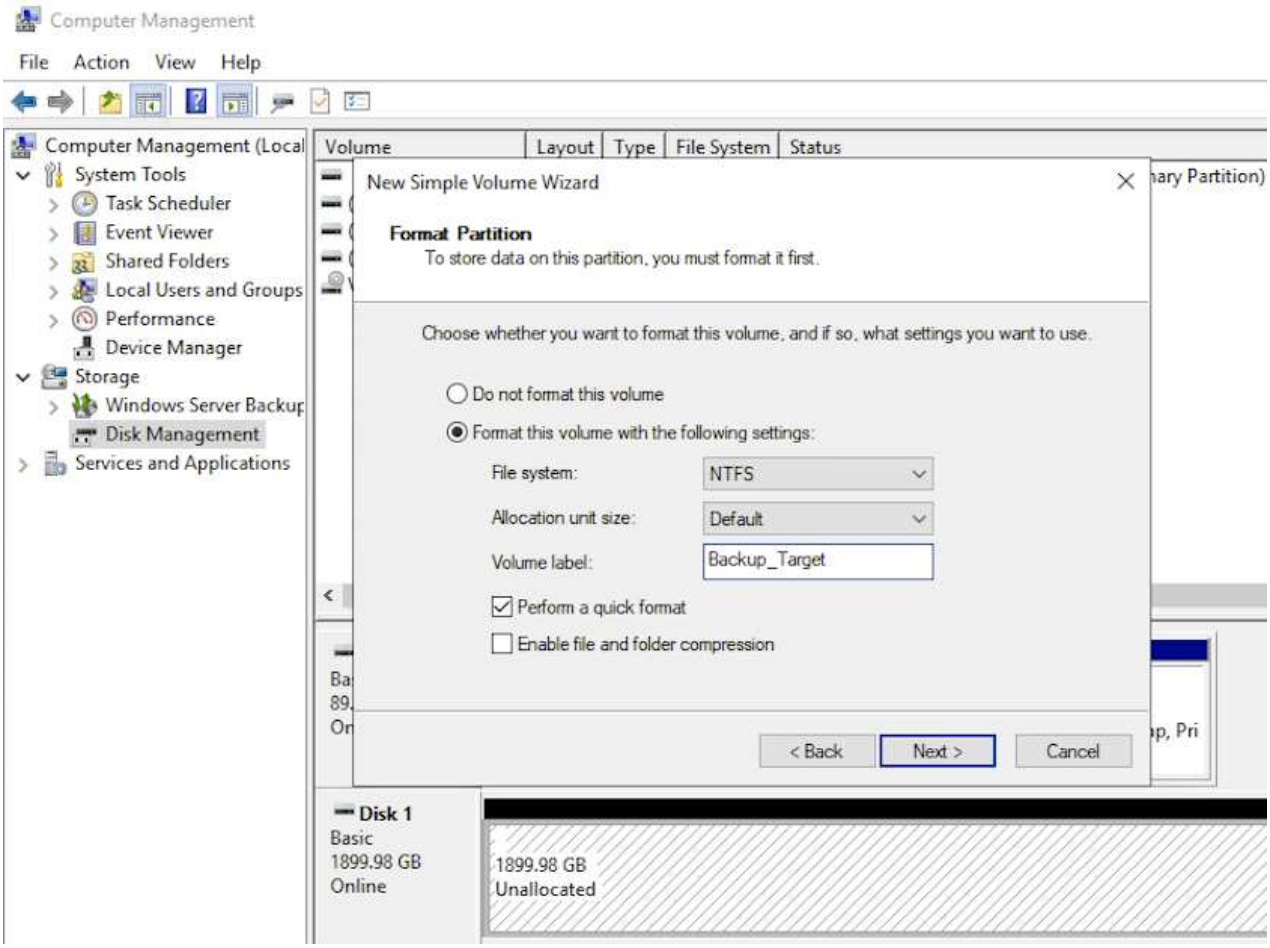
5. Para montar los LUN iSCSI, inicie sesión en Veeam Backup & Replication Server y abra Propiedades del iniciador iSCSI. Vaya a la pestaña **Discover** e introduzca la dirección IP de destino iSCSI.



6. En la pestaña **Targets**, resalte la LUN inactiva y haga clic en **Connect**. Marque la casilla **Enable multi-path** y haga clic en **OK** para conectarse a la LUN.



7. En la utilidad Administración de discos, inicialice el nuevo LUN y cree un volumen con el nombre y la letra de unidad deseados. Marque la casilla **Enable multi-path** y haga clic en **OK** para conectarse a la LUN.

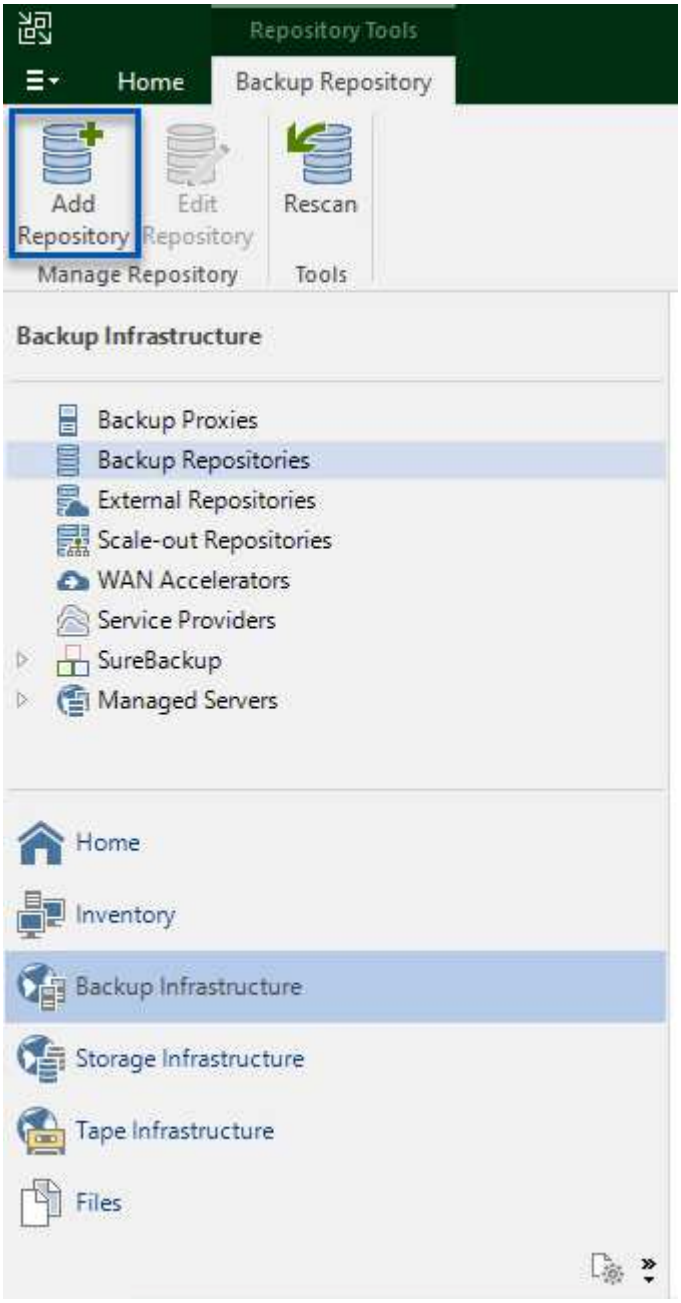


8. Repita estos pasos para montar los volúmenes iSCSI en el servidor proxy de Veeam.

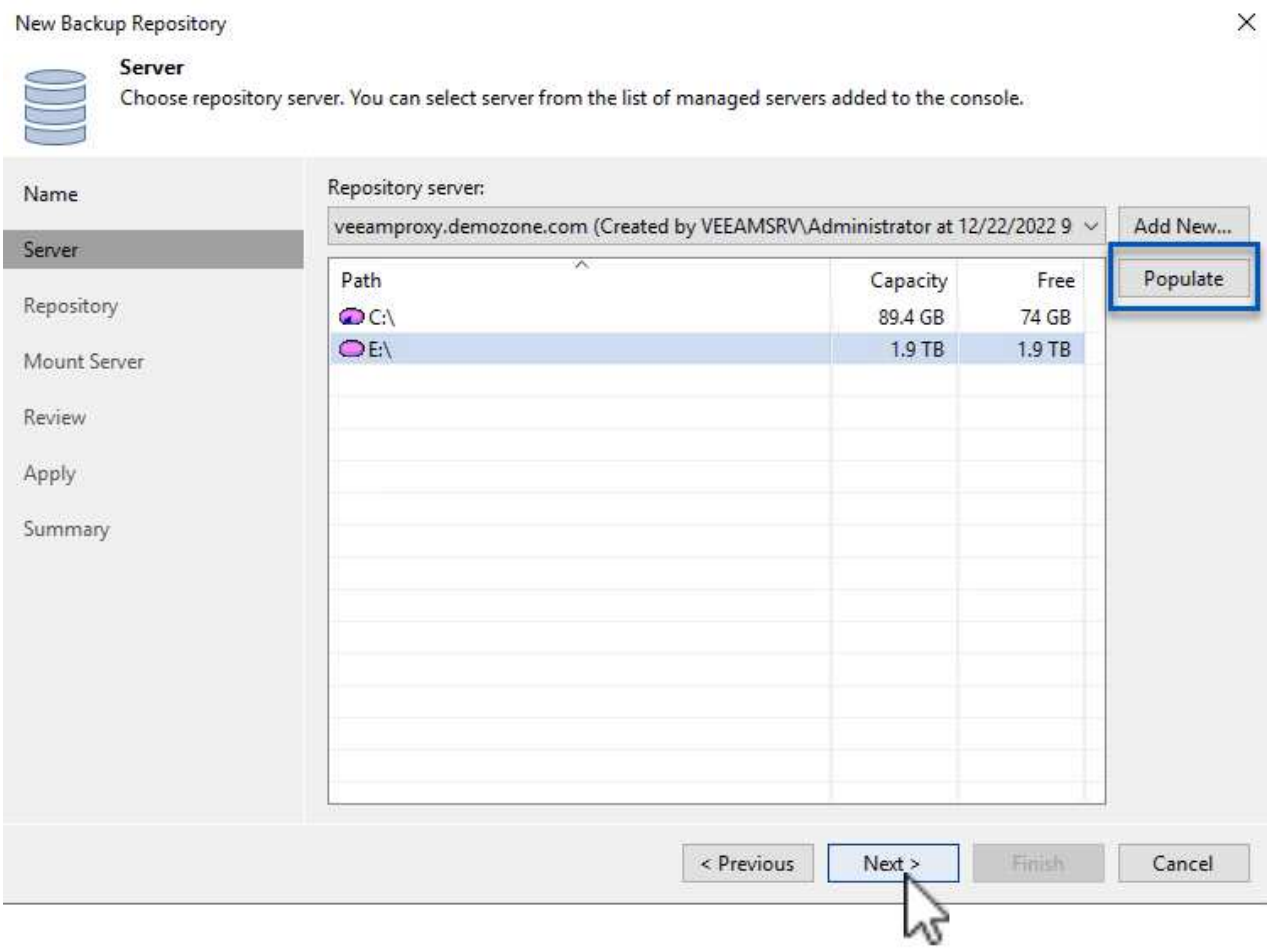
Crear repositorios de Veeam Backup

En la consola Veeam Backup and Replication, cree repositorios de backup para los servidores Veeam Backup y Veeam Proxy. Estos repositorios se utilizarán como destinos de copia de seguridad para las copias de seguridad de máquinas virtuales.

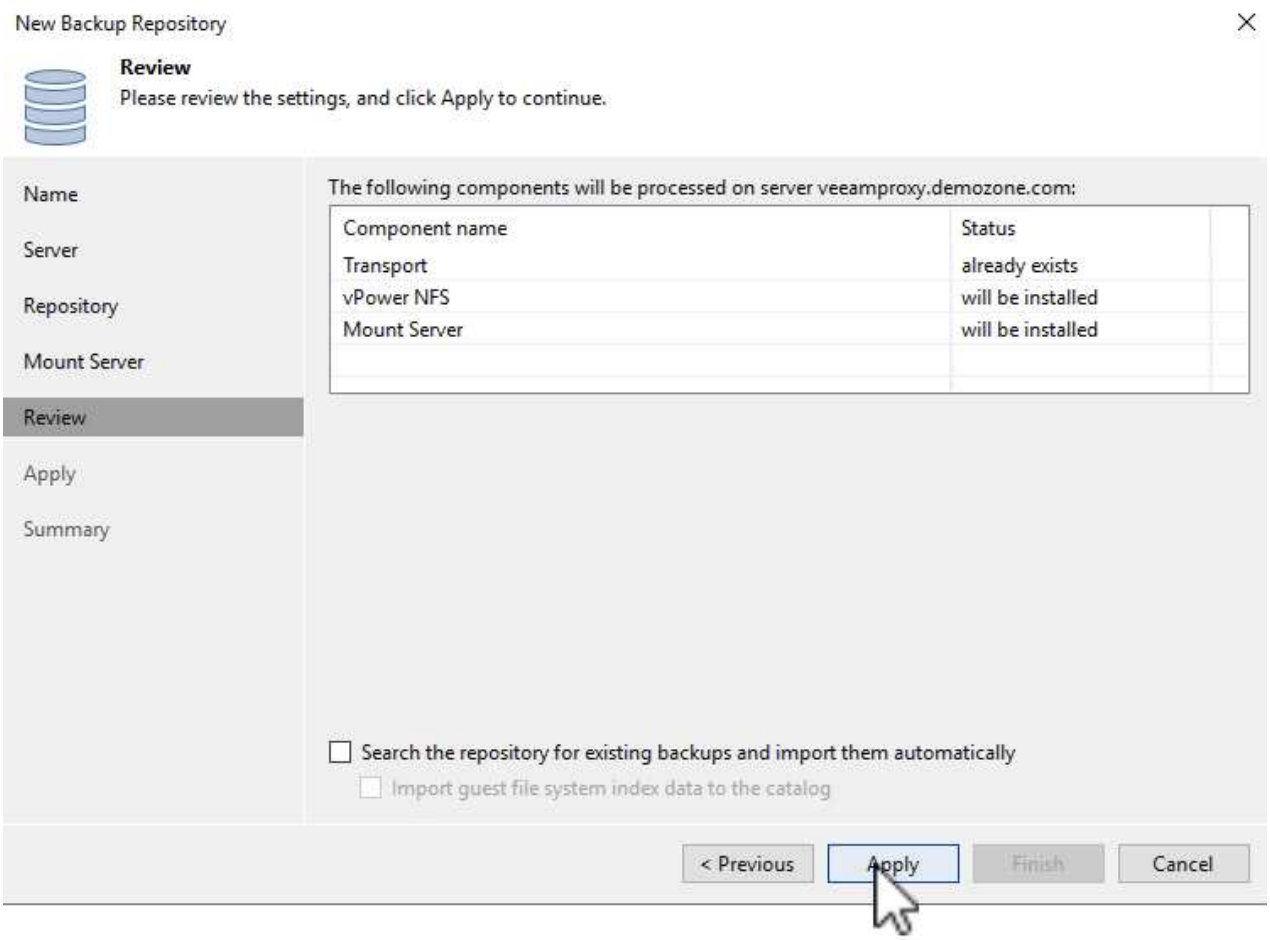
1. En la consola Veeam Backup and Replication, haga clic en **Backup Infrastructure** en la parte inferior izquierda y luego seleccione **Add Repository**



2. En el asistente New Backup Repository, introduzca un nombre para el repositorio y, a continuación, seleccione el servidor de la lista desplegable y haga clic en el botón **Llenar** para elegir el volumen NTFS que se utilizará.



3. En la página siguiente, elija el servidor de montaje que se utilizará para montar backups en la realización de restauraciones avanzadas. Por defecto, este es el mismo servidor que tiene conectado el almacenamiento del repositorio.
4. Revise sus selecciones y haga clic en **Aplicar** para iniciar la creación del repositorio de copia de seguridad.



5. Repita estos pasos para cualquier servidor proxy adicional.

Configurar los trabajos de backup de Veeam

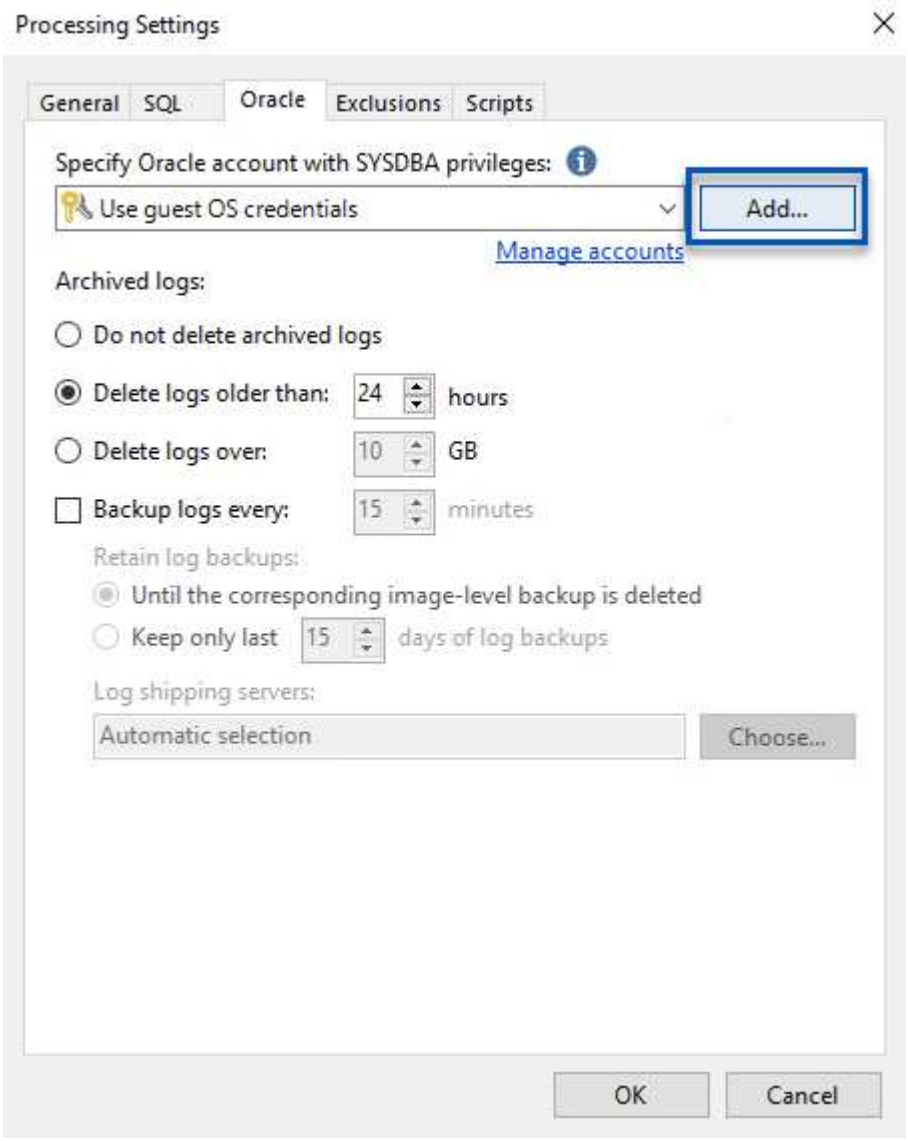
Los trabajos de copia de seguridad se deben crear utilizando los repositorios de copia de seguridad de la sección anterior. La creación de tareas de backup forma parte normal del repertorio de cualquier administrador de almacenamiento y no cubrimos todos los pasos aquí. Si desea obtener más información acerca de la creación de trabajos de backup en Veeam, consulte "Documentación técnica del centro de ayuda de Veeam".

En esta solución se crearon tareas de backup independientes para:

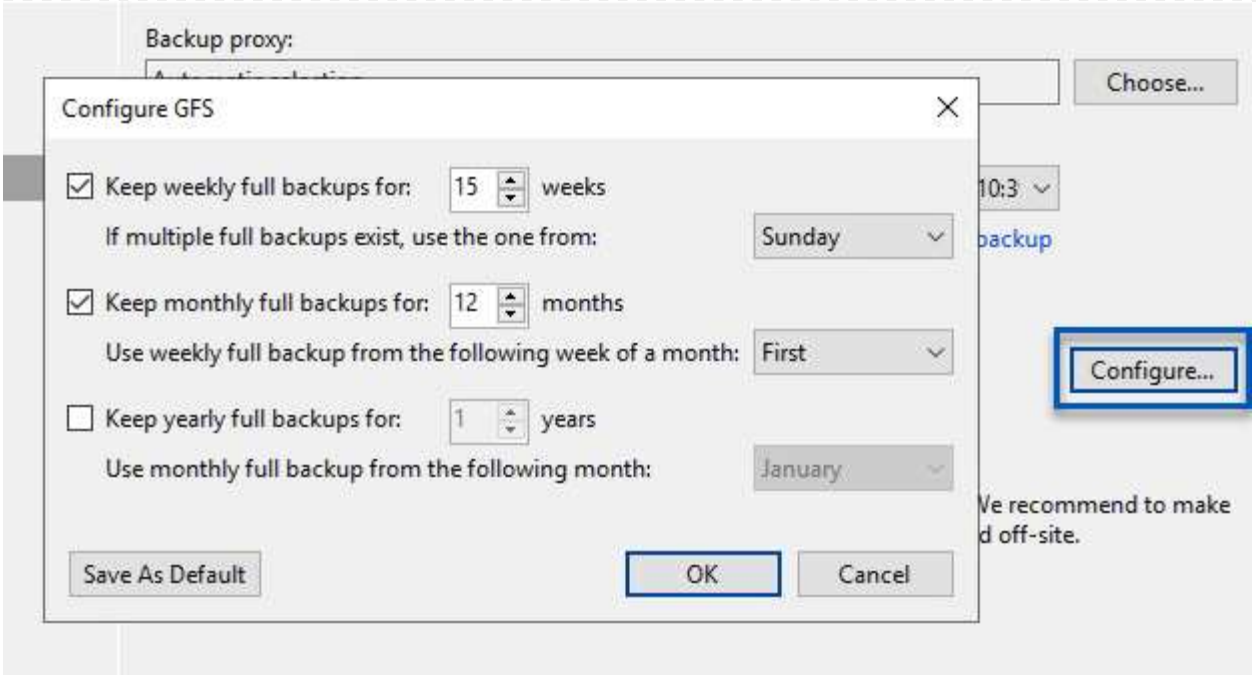
- Servidores Microsoft Windows SQL Server
- Servidores Oracle Database
- Servidores de archivo Windows
- Servidores de archivos Linux

Consideraciones generales al configurar trabajos de backup de Veeam

1. Permitir el procesamiento con reconocimiento de aplicaciones para crear copias de seguridad coherentes y realizar el procesamiento de registros de transacciones.
2. Después de activar el procesamiento que tenga en cuenta la aplicación, agregue las credenciales correctas con privilegios de administrador a la aplicación, ya que puede ser diferente de las credenciales del sistema operativo invitado.



3. Para administrar la política de retención para la copia de seguridad, verifique el **Mantenga ciertas copias de seguridad completas durante más tiempo para fines de archivado** y haga clic en el botón **Configurar…** para configurar la política.



Restaure VMs de aplicaciones con la restauración completa de Veeam

Realizar una restauración completa con Veeam es el primer paso de la restauración de una aplicación. Validamos que todas las restauraciones de nuestras máquinas virtuales encendidas y que todos los servicios se ejecutaban con normalidad.

La restauración de servidores es una parte normal del repertorio de administradores de almacenamiento y no cubrimos todos los pasos aquí. Para obtener información más completa sobre cómo realizar restauraciones completas en Veeam, consulte la "Documentación técnica del centro de ayuda de Veeam".

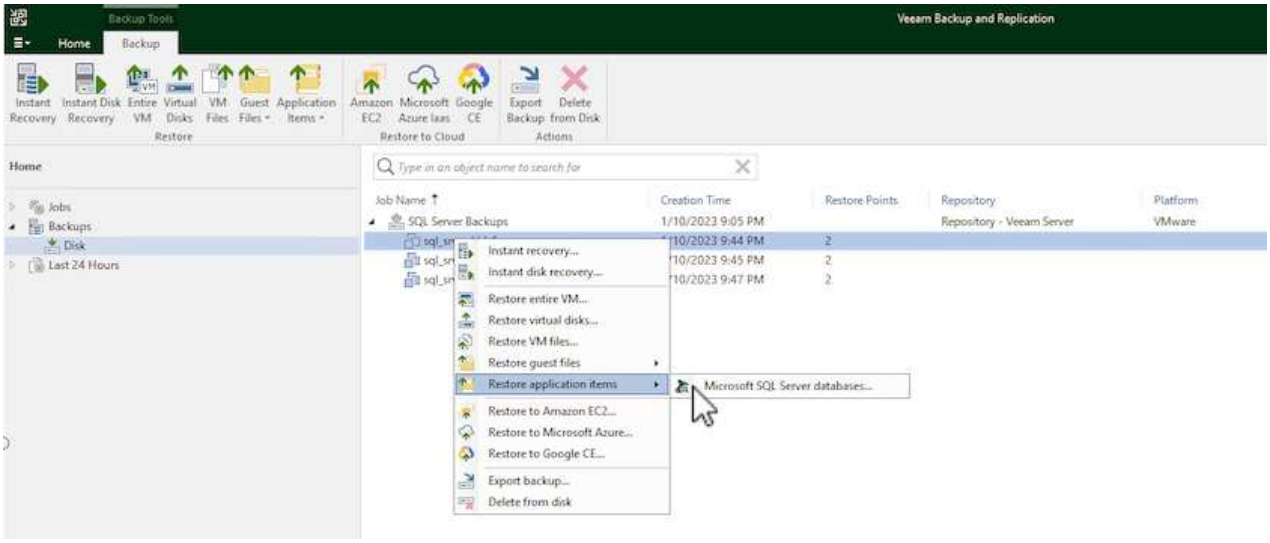
Restaure las bases de datos de SQL Server

Veeam Backup & Replication ofrece varias opciones para restaurar bases de datos de SQL Server. Para esta validación utilizamos Veeam Explorer for SQL Server with Instant Recovery para ejecutar restauraciones de nuestras bases de datos SQL Server. SQL Server Instant Recovery es una función que le permite restaurar rápidamente bases de datos de SQL Server sin tener que esperar a que se restaure la base de datos completa. Este rápido proceso de recuperación minimiza el tiempo de inactividad y garantiza la continuidad del negocio. Así es como funciona:

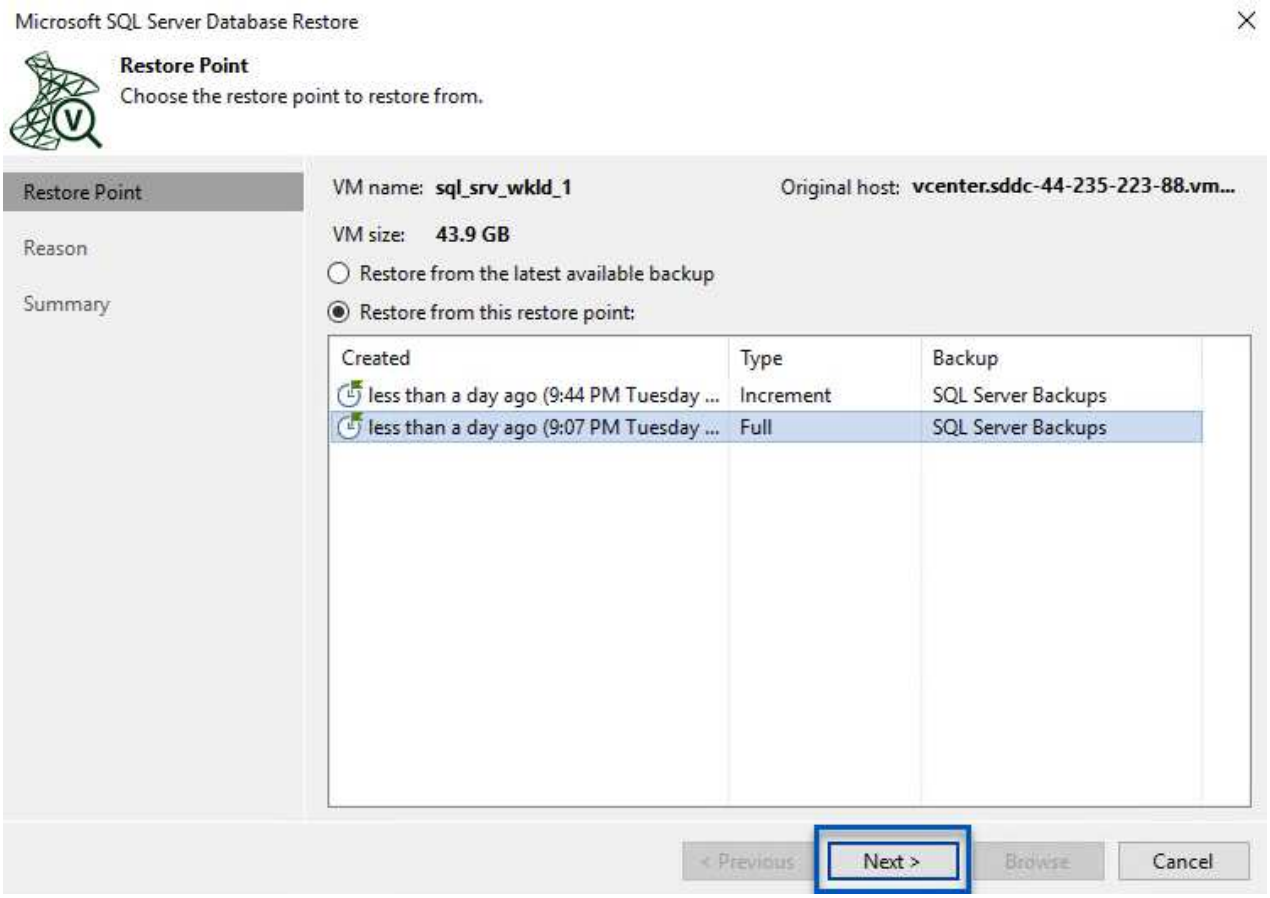
- Veeam Explorer **monta la copia de seguridad** que contiene la base de datos de SQL Server que se va a restaurar.
- El software **publica la base de datos** directamente desde los archivos montados, haciéndola accesible como base de datos temporal en la instancia de SQL Server de destino.
- Mientras la base de datos temporal está en uso, Veeam Explorer **redirige las consultas de los usuarios** a esta base de datos, asegurando que los usuarios puedan seguir accediendo y trabajando con los datos.
- En segundo plano, Veeam **realiza una restauración completa de la base de datos**, transfiriendo datos de la base de datos temporal a la ubicación original de la base de datos.
- Una vez completada la restauración completa de la base de datos, Veeam Explorer * cambia las consultas de los usuarios a la base de datos original* y elimina la base de datos temporal.

Restaure la base de datos de SQL Server con Veeam Explorer Instant Recovery

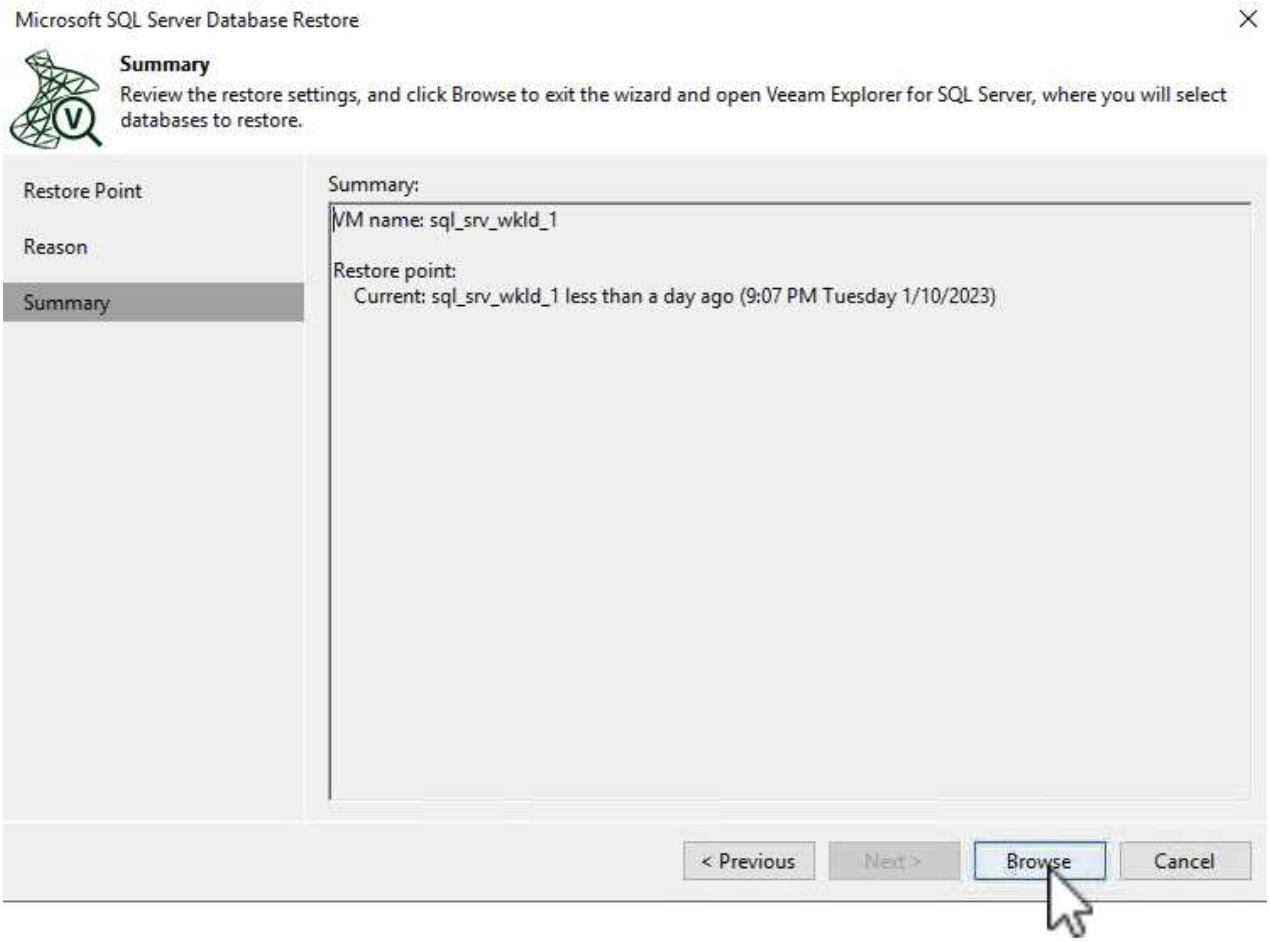
1. En la consola de Veeam Backup and Replication, navegue a la lista de copias de seguridad de SQL Server, haga clic con el botón derecho en un servidor y seleccione **Restaurar elementos de aplicación** y luego **Bases de datos de Microsoft SQL Server…**.



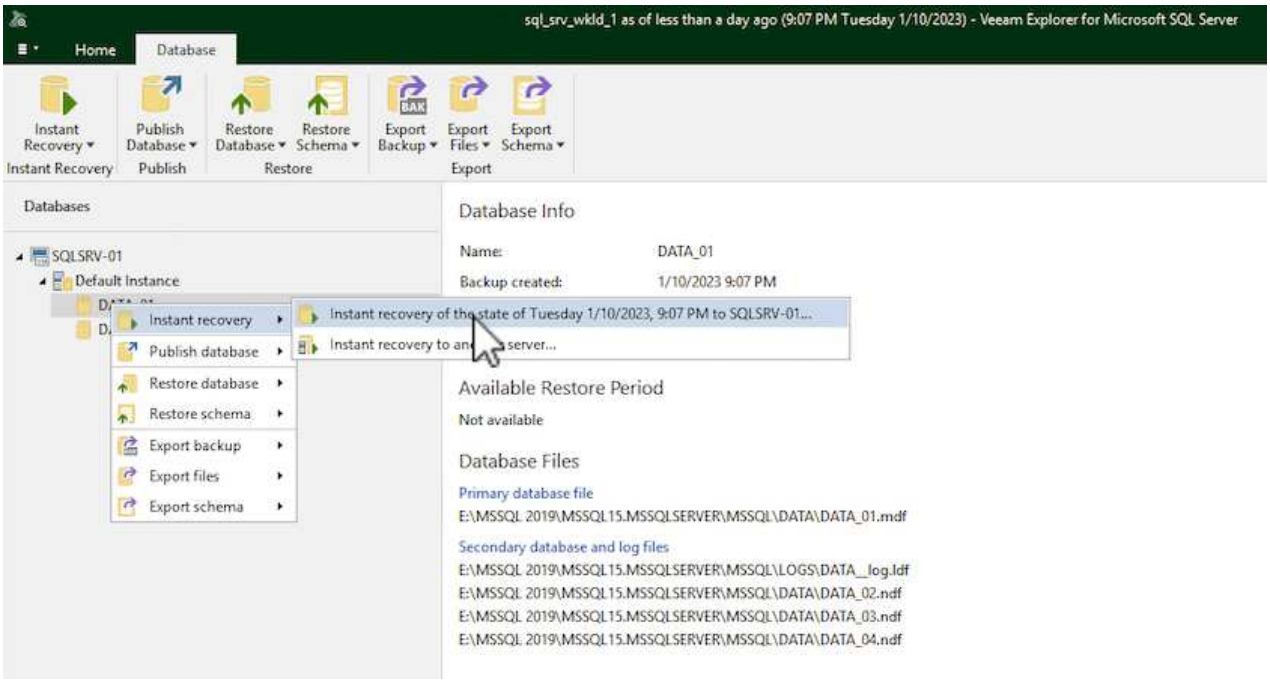
2. En el Asistente de restauración de bases de datos de Microsoft SQL Server, seleccione un punto de restauración de la lista y haga clic en **Siguiente**.



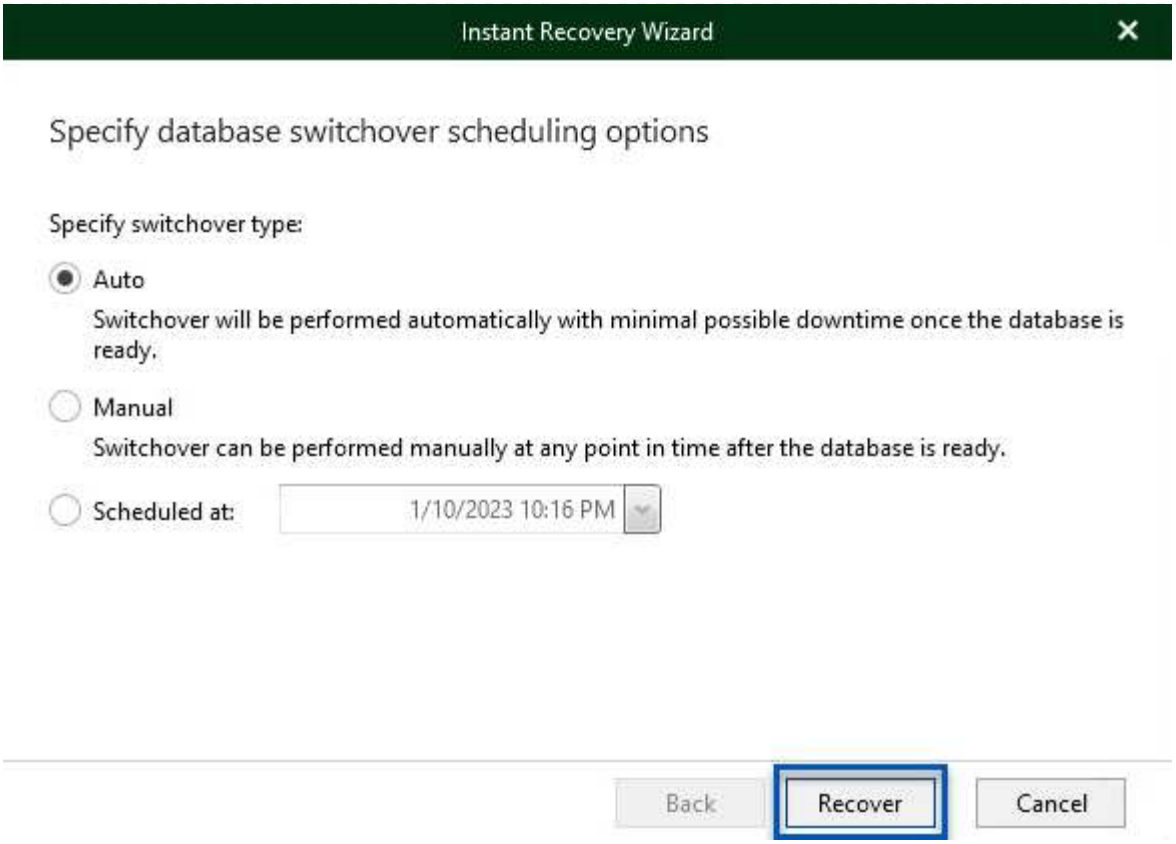
3. Introduzca un **Razón de restauración** si lo desea y, a continuación, en la página Resumen, haga clic en el botón **Examinar** para iniciar Veeam Explorer para Microsoft SQL Server.



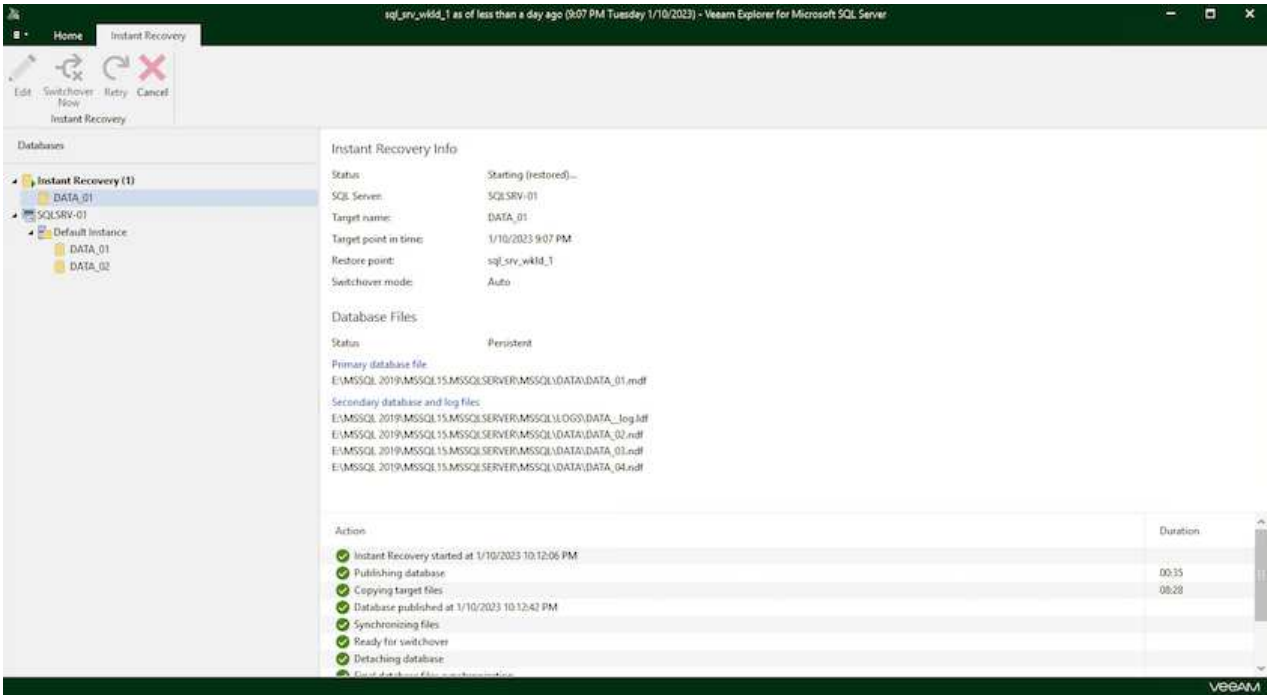
4. En Veeam Explorer expanda la lista de instancias de base de datos, haga clic derecho y seleccione **Recuperación instantánea** y luego el punto de restauración específico para recuperar.



5. En el Asistente de Recuperación Instantánea, especifique el tipo de switchover. Esto puede realizarse automáticamente con un tiempo de inactividad mínimo, manualmente o en un momento determinado. Luego haga clic en el botón **Recuperar** para comenzar el proceso de restauración.



6. El proceso de recuperación se puede supervisar desde Veeam Explorer.



Para obtener información más detallada sobre cómo realizar operaciones de restauración de SQL Server con Veeam Explorer, consulte la sección Microsoft SQL Server en la "Guía del usuario de Veeam Explorers".

Restaurar bases de datos de Oracle con Veeam Explorer

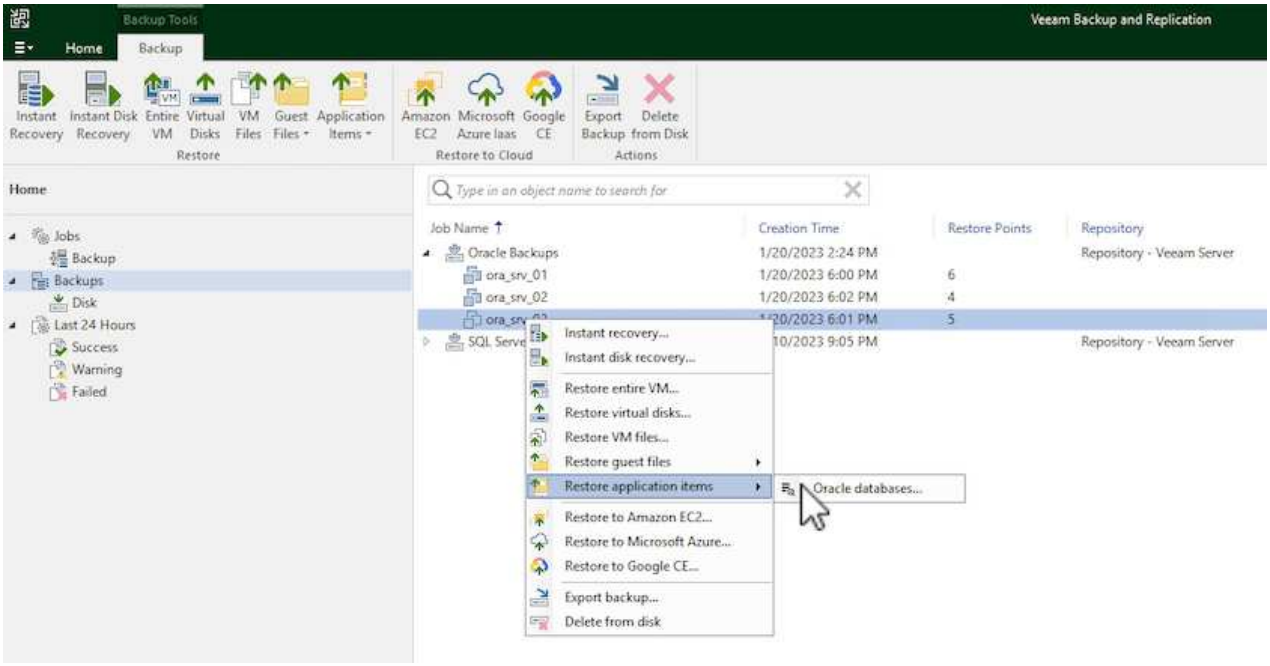
Veeam Explorer para la base de datos Oracle permite realizar una restauración estándar de la base de datos Oracle o una restauración sin interrupciones con Instant Recovery. También admite la publicación de bases de datos para un acceso rápido, la recuperación de bases de datos de Data Guard y las restauraciones a partir de copias de seguridad de RMAN.

Para obtener información más detallada sobre cómo realizar operaciones de restauración de bases de datos de Oracle con Veeam Explorer, consulte la sección Oracle en la "Guía del usuario de Veeam Explorers".

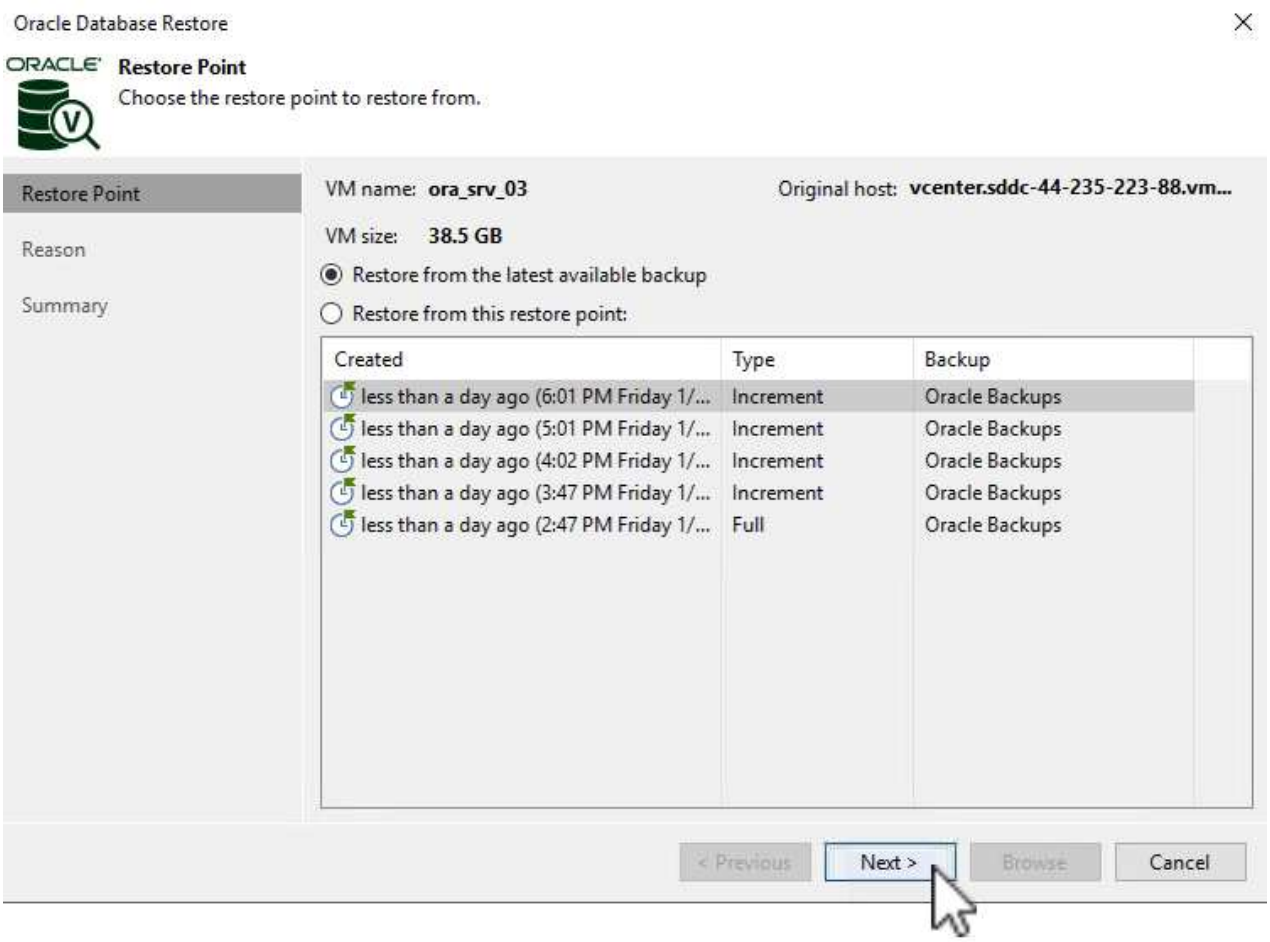
Restaurar base de datos de Oracle con Veeam Explorer

En esta sección, se trata una restauración de la base de datos Oracle en un servidor diferente mediante Veeam Explorer.

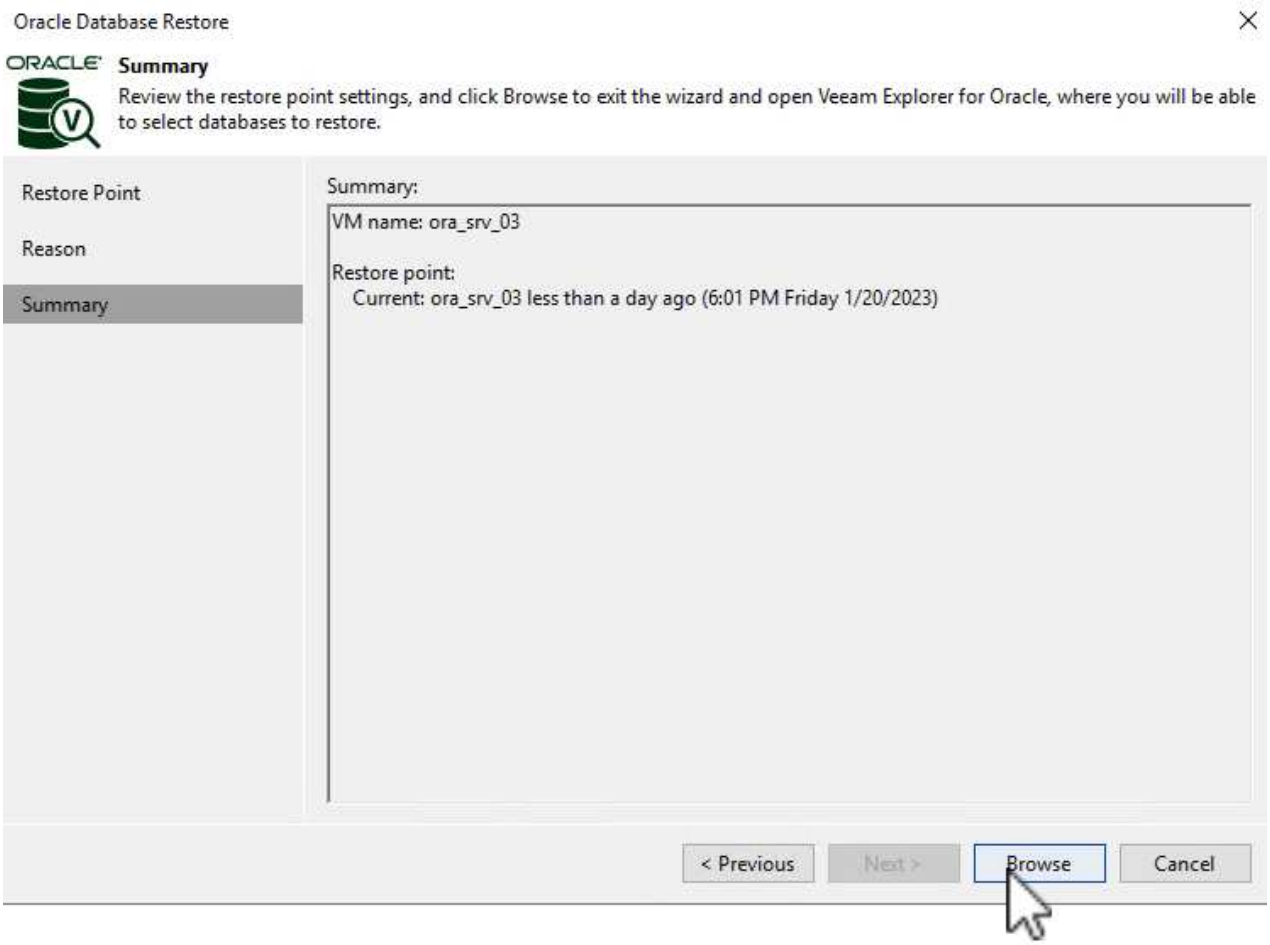
1. En la consola de Veeam Backup and Replication, navegue a la lista de copias de seguridad de Oracle, haga clic con el botón derecho en un servidor y seleccione **Restaurar elementos de aplicación** y luego **Bases de datos Oracle…**.



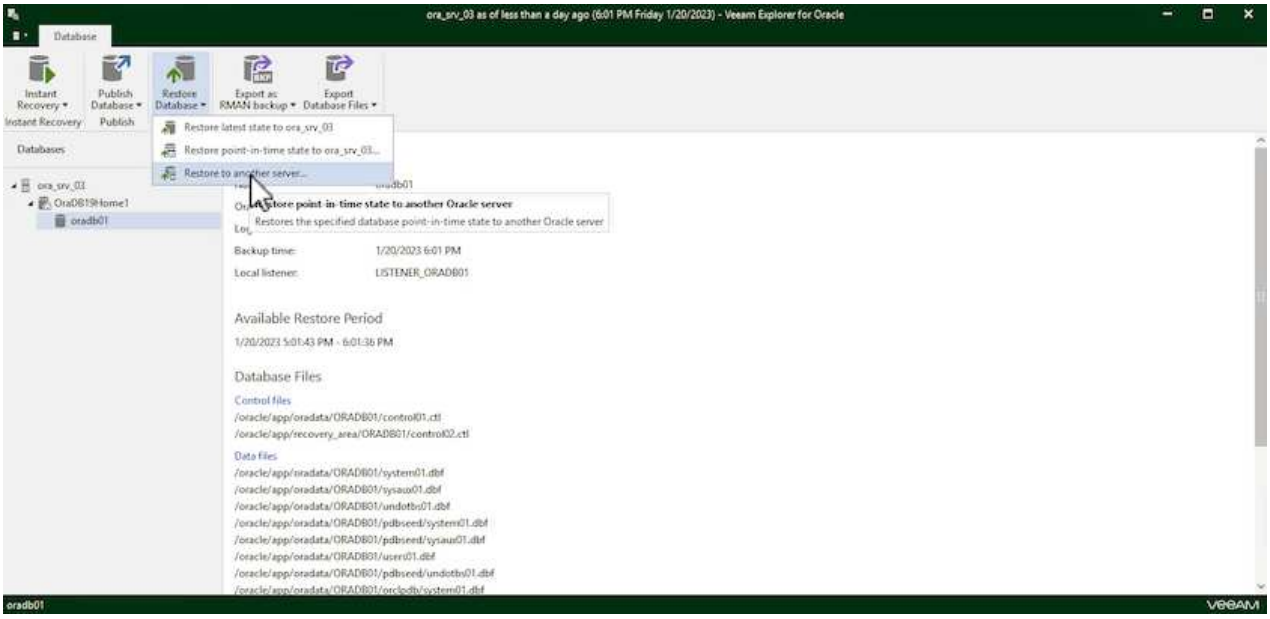
2. En el Asistente de restauración de bases de datos Oracle, seleccione un punto de restauración de la lista y haga clic en **Siguiente**.



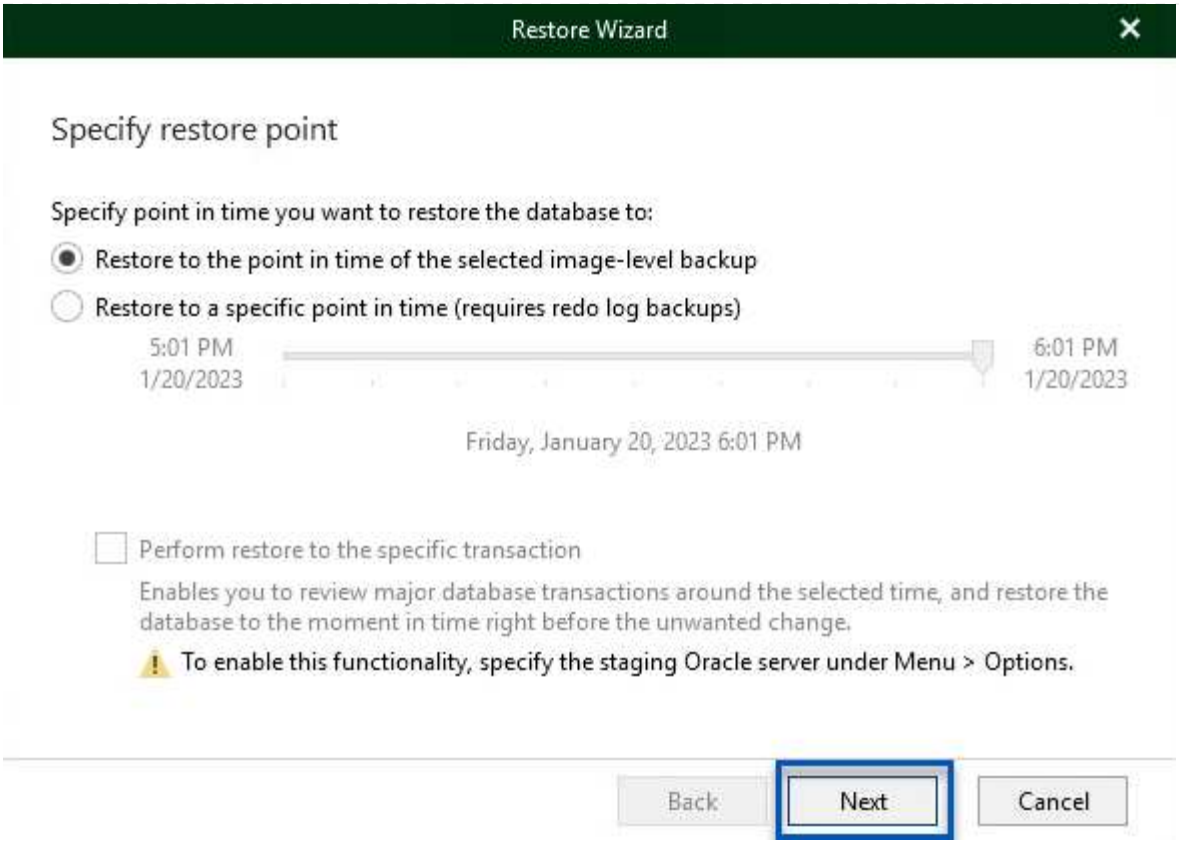
3. Introduzca un **Razón de restauración** si lo desea y, a continuación, en la página Resumen, haga clic en el botón **Examinar** para iniciar Veeam Explorer para Oracle.



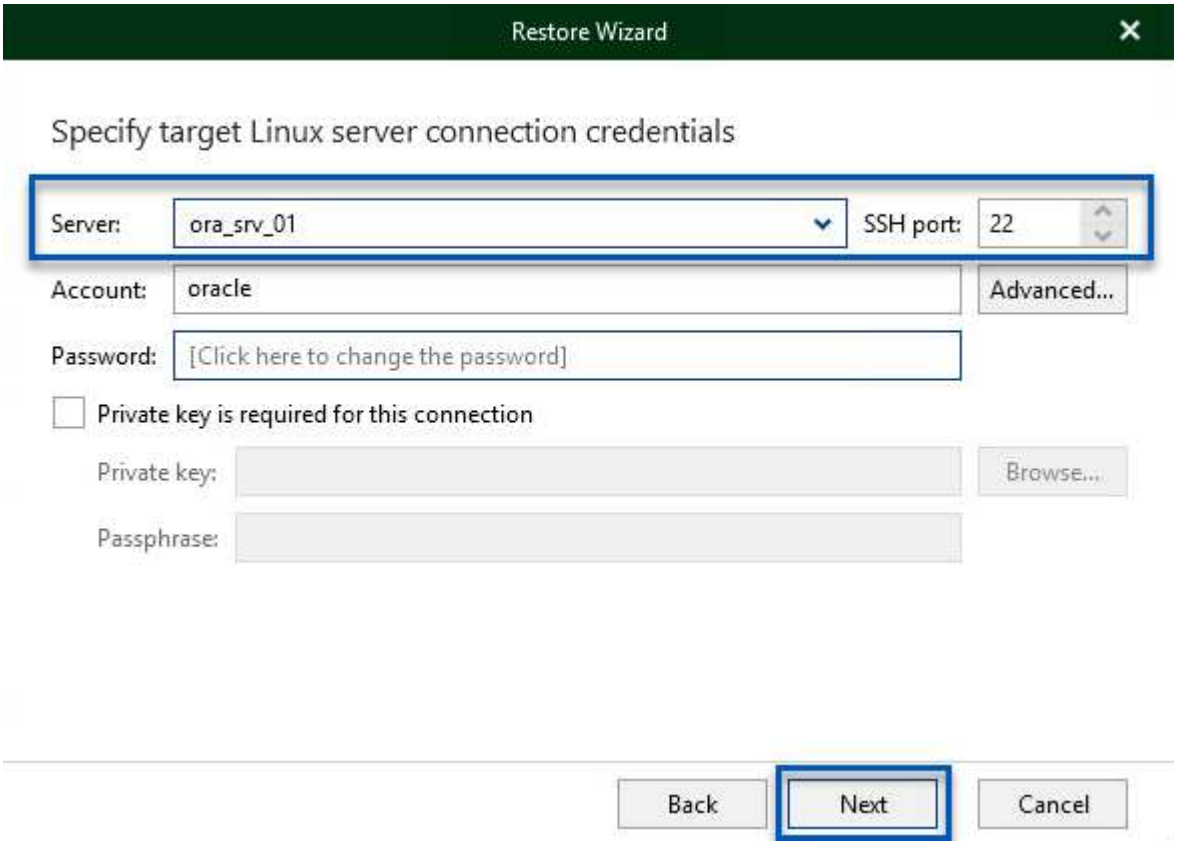
4. En Veeam Explorer expanda la lista de instancias de base de datos, haga clic en la base de datos que desea restaurar y luego en el menú desplegable **Restaurar base de datos** en la parte superior seleccione **Restaurar a otro servidor…**.



5. En el Asistente de restauración, especifique el punto de restauración desde el que desea restaurar y haga clic en **Siguiente**.

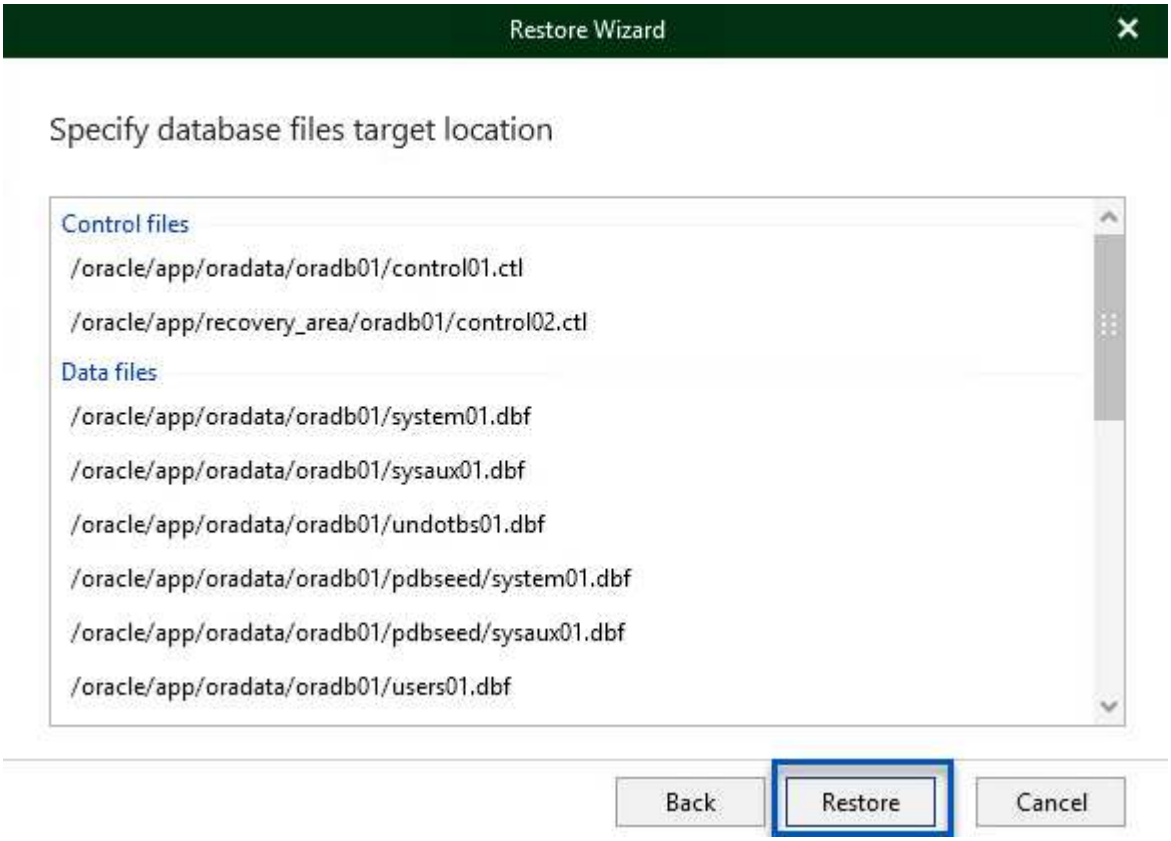


6. Especifique el servidor de destino al que se restaurará la base de datos y las credenciales de la cuenta y haga clic en **Siguiente**.



7. Por último, especifique la ubicación de destino de los archivos de base de datos y haga clic en el

botón **Restaurar** para iniciar el proceso de restauración.

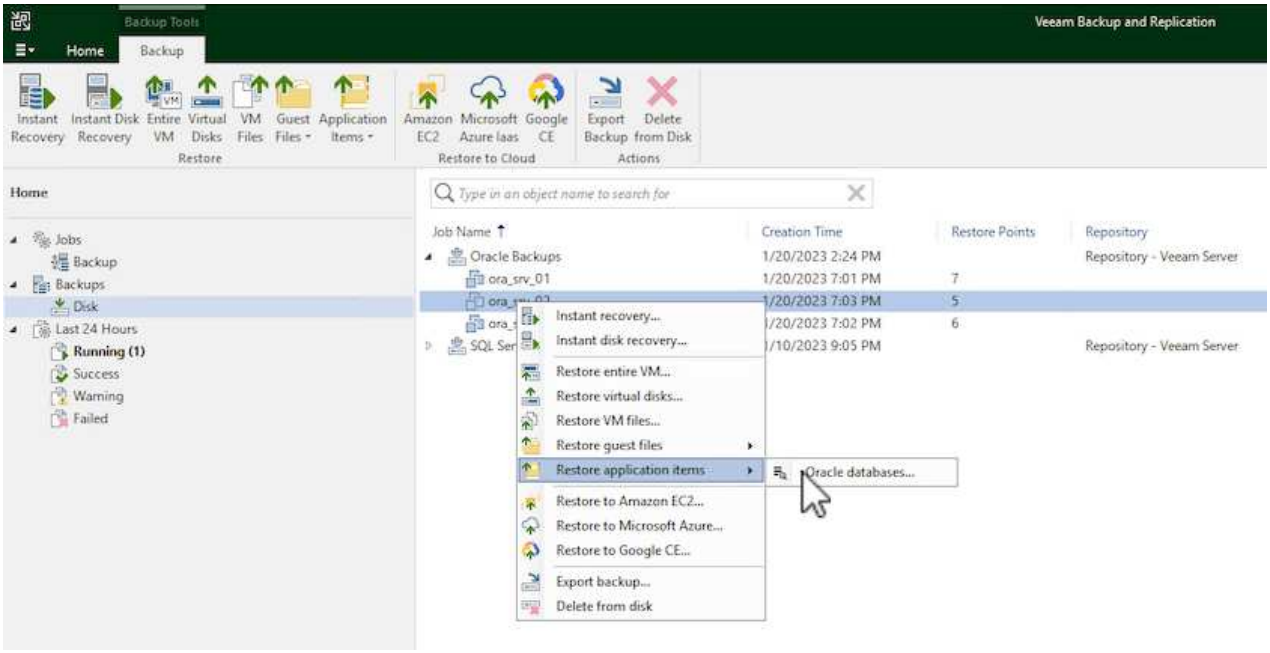


8. Una vez finalizada la recuperación de la base de datos, compruebe que la base de datos Oracle se inicia correctamente en el servidor.

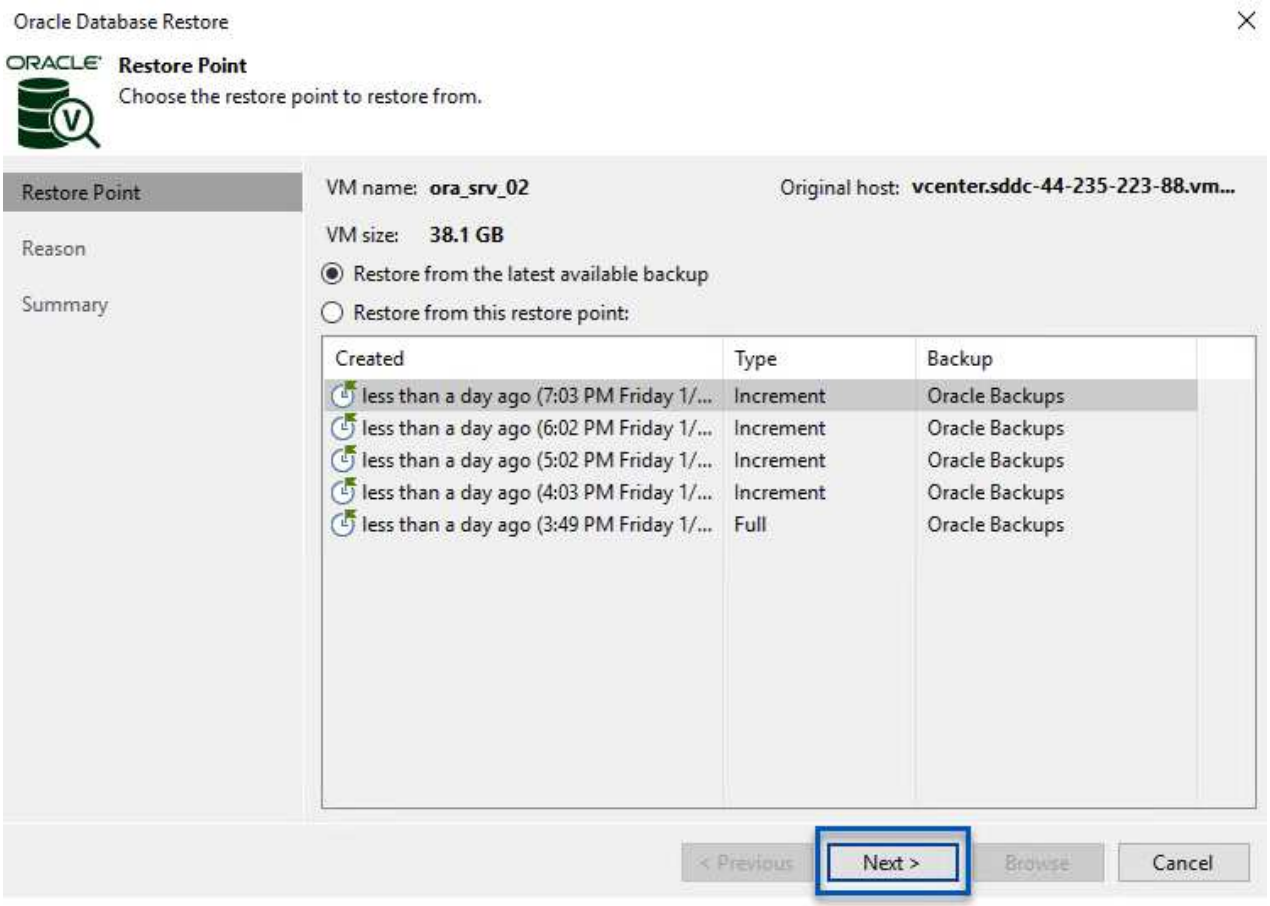
Publicar la base de datos Oracle en un servidor alternativo

En esta sección se publica una base de datos en un servidor alternativo para obtener un acceso rápido sin iniciar una restauración completa.

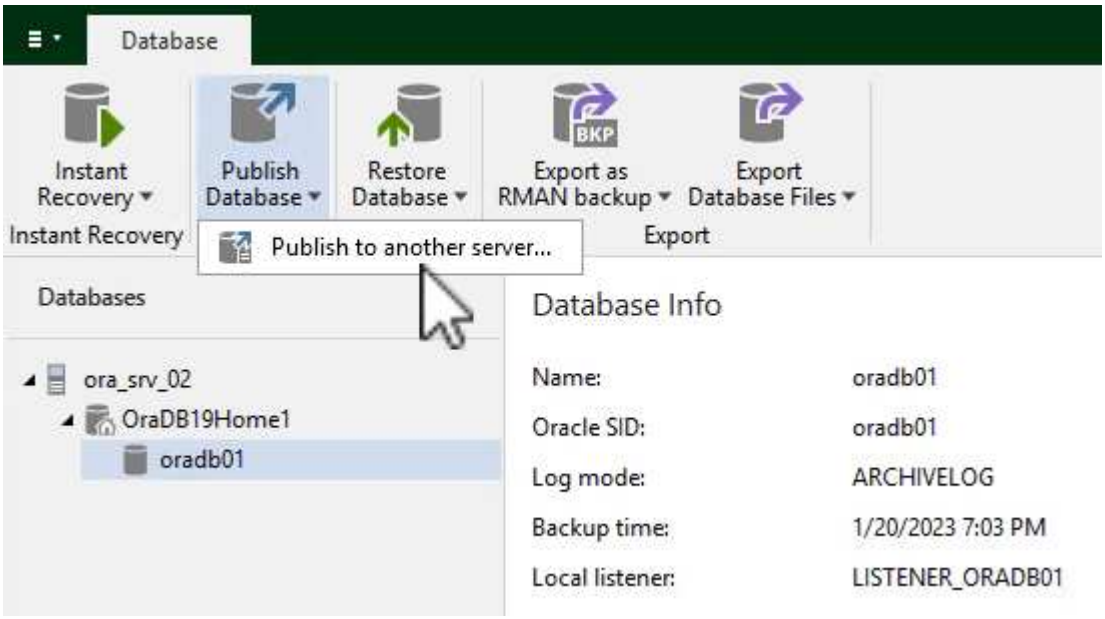
1. En la consola de Veeam Backup and Replication, navegue a la lista de copias de seguridad de Oracle, haga clic con el botón derecho en un servidor y seleccione **Restaurar elementos de aplicación** y luego **Bases de datos Oracle…**.



2. En el Asistente de restauración de bases de datos Oracle, seleccione un punto de restauración de la lista y haga clic en **Siguiente**.

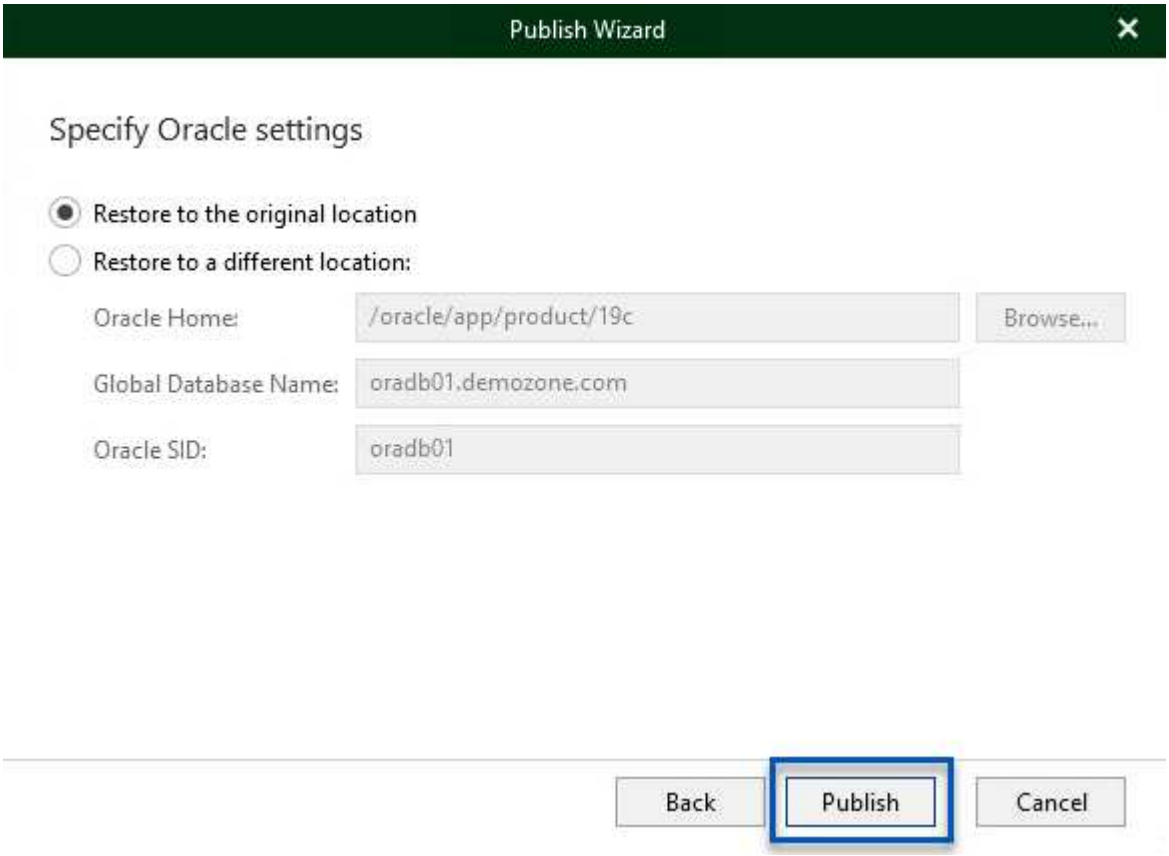


3. Introduzca un **Razón de restauración** si lo desea y, a continuación, en la página Resumen, haga clic en el botón **Examinar** para iniciar Veeam Explorer para Oracle.
4. En Veeam Explorer expanda la lista de instancias de base de datos, haga clic en la base de datos que desea restaurar y luego en el menú desplegable **Publicar base de datos** en la parte superior seleccione **Publicar en otro servidor…**.



5. En el asistente Publicar, especifique el punto de restauración desde el que publicar la base de datos y haga clic en **Siguiente**.

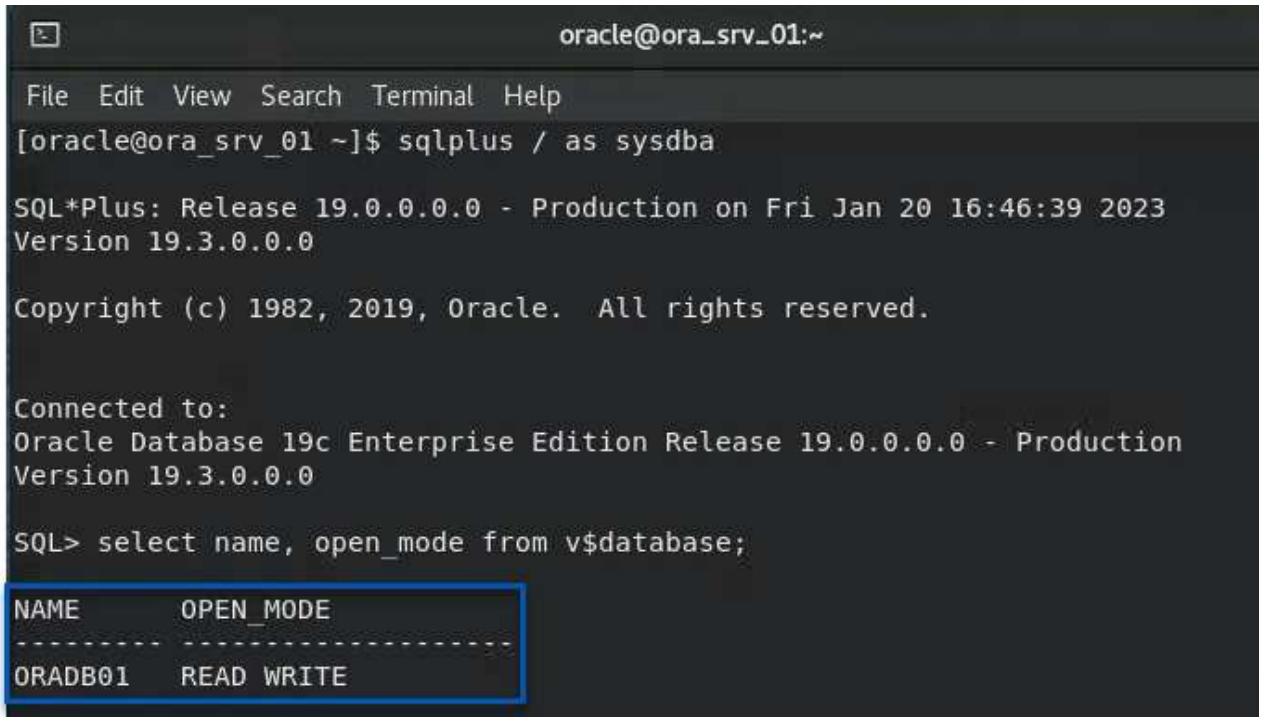
6. Por último, especifique la ubicación del sistema de archivos linux de destino y haga clic en **Publicar** para comenzar el proceso de restauración.



7. Una vez finalizada la publicación, conéctese al servidor de destino y ejecute los siguientes comandos para asegurarse de que la base de datos se está ejecutando:

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



Conclusión

VMware Cloud es una plataforma potente para ejecutar aplicaciones vitales para el negocio y almacenar datos confidenciales. Una solución de protección de datos segura es esencial para las empresas que confían en VMware Cloud para garantizar la continuidad del negocio y protegerse contra las amenazas cibernéticas y la pérdida de datos. Al elegir una solución de protección de datos sólida y fiable, las empresas pueden estar seguras de que sus datos esenciales están a salvo, independientemente de qué suceda.

El caso de uso que se presenta en esta documentación se centra en las tecnologías de protección de datos demostradas que destacan la integración entre NetApp, VMware y Veeam. FSX para ONTAP es compatible como almacenes de datos NFS complementarios para VMware Cloud en AWS y se utiliza para todos los datos de aplicaciones y máquinas virtuales. Veeam Backup & Replication es una completa solución de protección de datos diseñada para ayudar a las empresas a mejorar, automatizar y agilizar sus procesos de backup y recuperación. Veeam se utiliza en combinación con volúmenes de destino de backup iSCSI, alojados en FSx para ONTAP, para proporcionar una solución de protección de datos segura y fácil de gestionar para los datos de aplicaciones que residen en VMware Cloud.

Información adicional

Para obtener más información sobre las tecnologías presentadas en esta solución, consulte la siguiente información adicional.

- "Guía de usuario de FSx para ONTAP"
- "Documentación técnica del centro de ayuda de Veeam"
- "Soporte de VMware Cloud en AWS. Consideraciones y limitaciones"

TR-4955: Recuperación ante desastres con FSX para ONTAP y VMC (cloud VMware de AWS)

Niyaz Mohamed, NetApp

Descripción general

La recuperación ante desastres en el cloud es un método resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos dañados por los datos (por ejemplo, ransomware). Con la tecnología SnapMirror de NetApp, las cargas de trabajo de VMware en las instalaciones se pueden replicar en FSX para ONTAP ejecutándose en AWS.

Disaster Recovery Orchestrator (DRO, una solución basada en scripts con la interfaz de usuario) se puede usar para recuperar sin problemas las cargas de trabajo replicadas desde las instalaciones a FSX para ONTAP. DRO automatiza la recuperación del nivel de SnapMirror, mediante el registro de VM en VMC, hasta las asignaciones de red directamente en NSX-T. Esta función está incluida en todos los entornos VMC.

Primeros pasos

Implemente y configure VMware Cloud en AWS

"VMware Cloud en AWS" Proporciona una experiencia nativa del cloud para cargas de trabajo basadas en VMware en el ecosistema de AWS. Cada centro de datos definido por software (SDDC) de VMware se ejecuta en un cloud privado virtual de Amazon (VPC) y proporciona una pila completa de VMware (incluido vCenter Server), las redes definidas por software NSX-T, el almacenamiento definido por software VSAN y uno o más hosts ESXi que proporcionan recursos informáticos y de almacenamiento a las cargas de trabajo. Para configurar un entorno VMC en AWS, siga estos pasos "enlace". También se puede utilizar un clúster de luz piloto para la recuperación ante desastres.

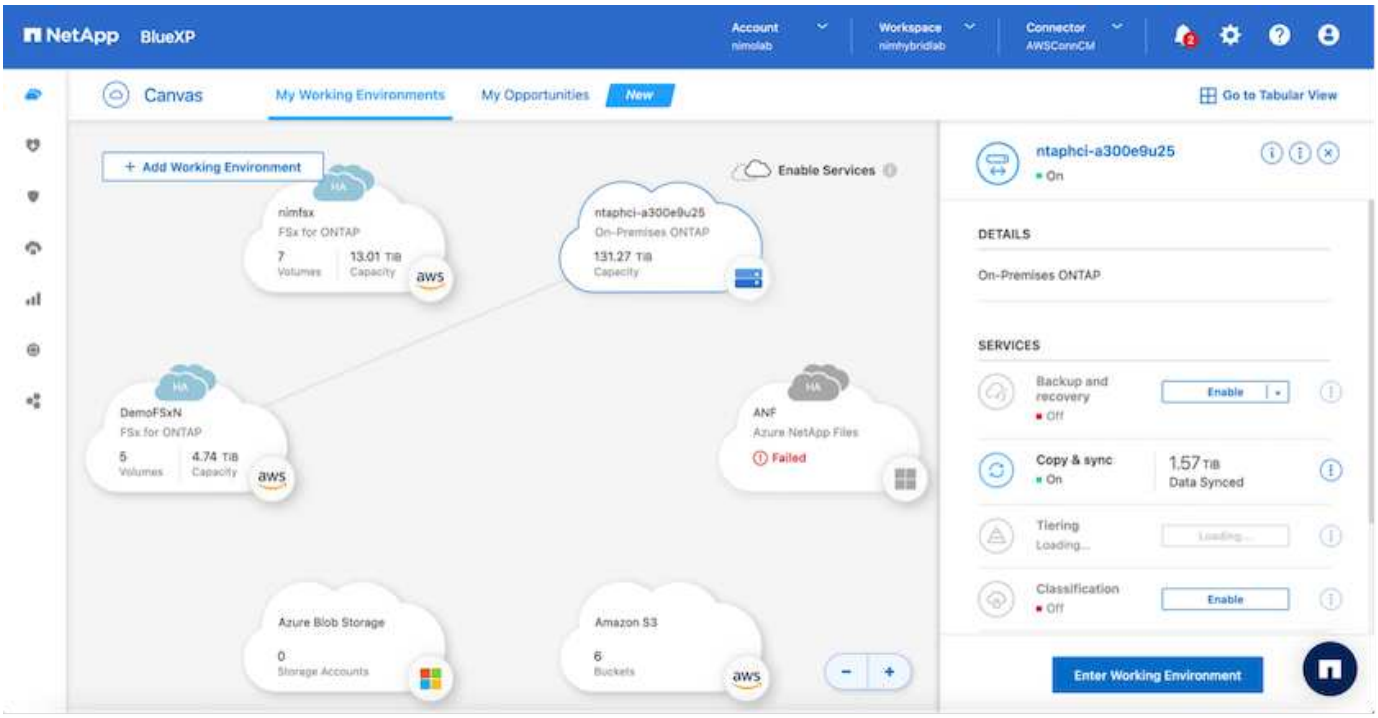
> En la versión inicial, DRO admite un clúster de luces piloto existente. La creación bajo demanda de SDDC estará disponible en una próxima versión.

Aprovisionar y configurar FSX para ONTAP

Amazon FSX para ONTAP de NetApp es un servicio totalmente gestionado que ofrece un almacenamiento de archivos altamente fiable, escalable, de alto rendimiento y con numerosas funciones incorporado en el popular sistema de archivos ONTAP de NetApp. Siga estos pasos "enlace" Para aprovisionar y configurar FSX para ONTAP.

Poner en marcha y configurar SnapMirror a FSX para ONTAP

El siguiente paso consiste en utilizar NetApp BlueXP y descubrir la instancia de FSX aprovisionada para ONTAP en AWS y replicar los volúmenes de almacenes de datos deseados de un entorno local a FSX para ONTAP con la frecuencia adecuada y la retención de copias Snapshot de NetApp:



Siga los pasos de este enlace para configurar BlueXP. También puede utilizar la CLI de ONTAP de NetApp para programar la replicación a continuación de este enlace.

Una relación de SnapMirror es un requisito previo y debe crearse previamente.

Instalación DE DRO

Para empezar con DRO, utilice el sistema operativo Ubuntu en una instancia EC2 o máquina virtual designada para asegurarse de que cumple los requisitos previos. A continuación, instale el paquete.

Requisitos previos

- Asegúrese de que existe conectividad con la instancia de vCenter y los sistemas de almacenamiento de origen y de destino.
- La resolución DNS debe estar en su lugar si está utilizando nombres DNS. De lo contrario, se deben usar direcciones IP para las instancias de vCenter y los sistemas de almacenamiento.
- Crear un usuario con permisos raíz. También puede usar sudo con una instancia de EC2.

Requisitos de SO

- Ubuntu 20.04 (LTS) con un mínimo de 2 GB y 4 vCPU
- Se deben instalar los siguientes paquetes en el equipo virtual del agente designado:
  - Docker
  - Composición de Docker
  - JQ

Cambiar permisos en `docker.sock`: `sudo chmod 666 /var/run/docker.sock`.

La `deploy.sh` el script ejecuta todos los requisitos previos necesarios.

Instale el paquete

1. Descargue el paquete de instalación en la máquina virtual designada:

```
git clone https://github.com/NetApp/DRO-AWS.git
```

El agente se puede instalar localmente o dentro de un VPC de AWS.

2. Descomprima el paquete, ejecute el script de implementación e introduzca la IP del host (por ejemplo, 10.10.10.10).

```
tar xvf DRO-prereq.tar
```

3. Desplácese al directorio y ejecute el script de despliegue de la siguiente manera:

```
sudo sh deploy.sh
```

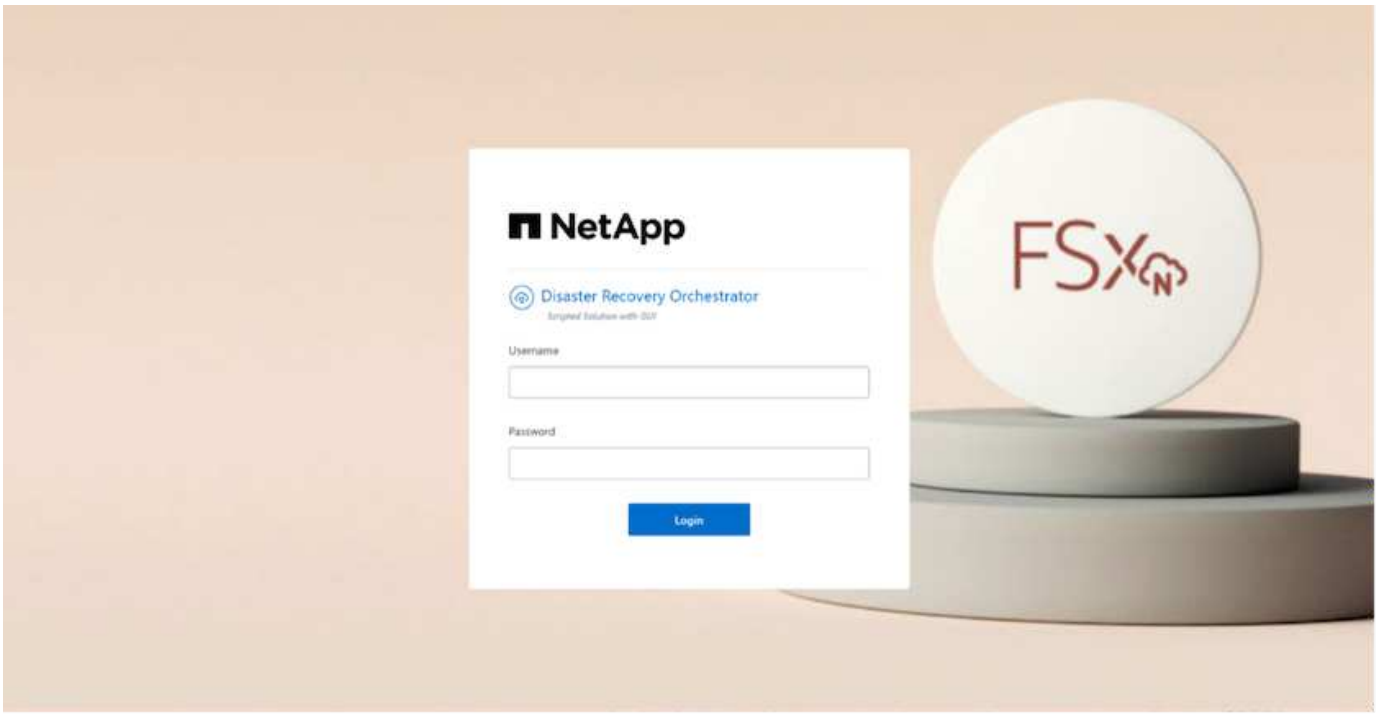
4. Acceda a la interfaz de usuario mediante:

```
https://<host-ip-address>
```

con las siguientes credenciales predeterminadas:

```
Username: admin
Password: admin
```

La contraseña se puede cambiar con la opción "Cambiar contraseña".



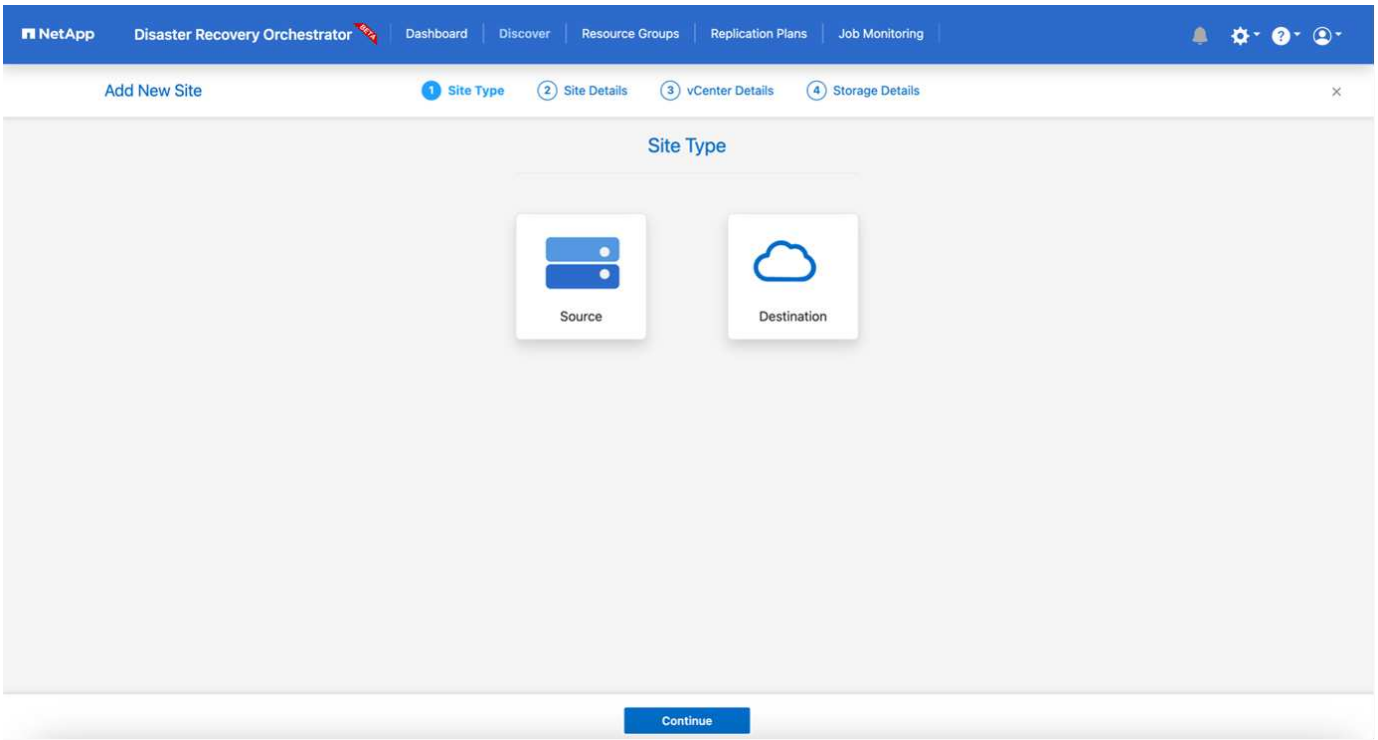
Configuración DE DRO

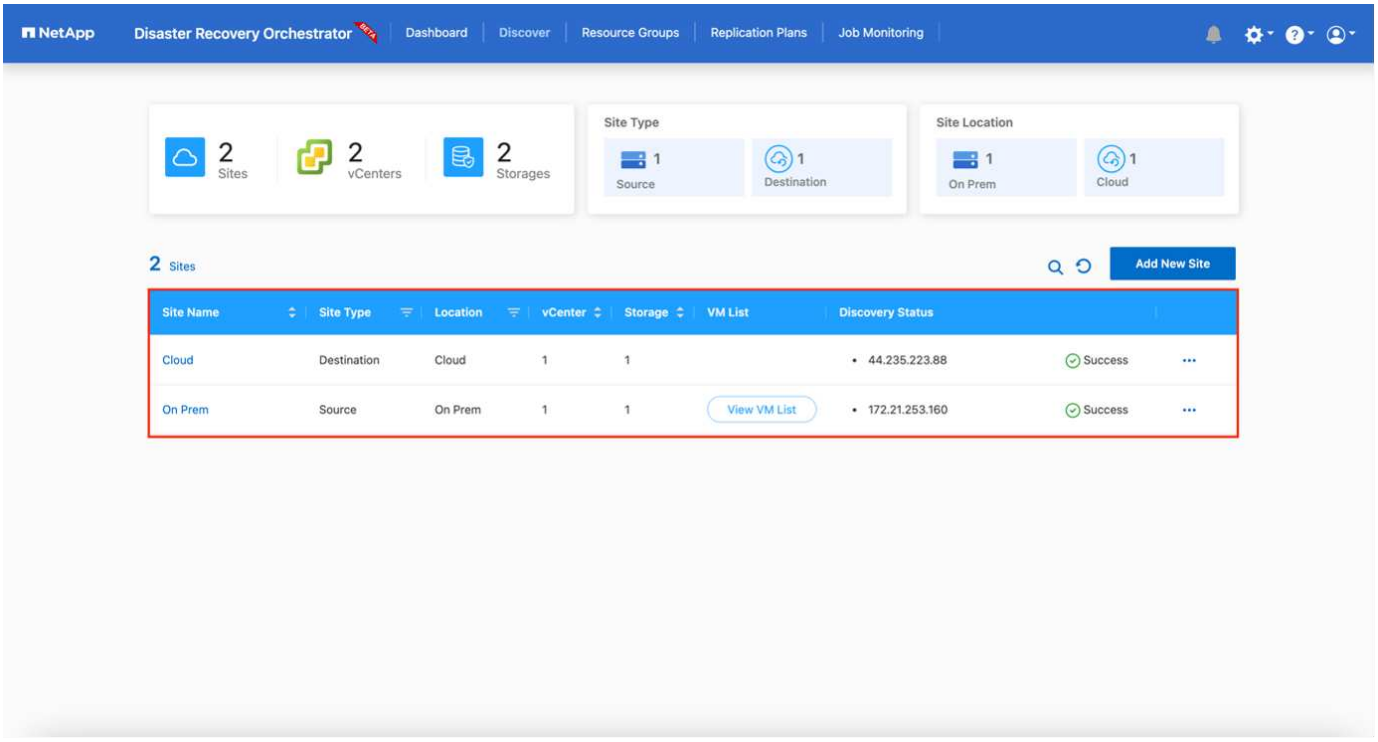
Después de que los FSX para ONTAP y VMC se hayan configurado correctamente, puede empezar a configurar DRO para automatizar la recuperación de las cargas de trabajo en las instalaciones a VMC usando las copias SnapMirror de solo lectura en FSX para ONTAP.

NetApp recomienda la puesta en marcha del agente DRO en AWS y también en el mismo VPC, en el que se ponga en marcha FSX para ONTAP (también puede estar conectado por la misma paridad), Para que el agente DRO pueda comunicarse a través de la red con sus componentes locales, así como con los recursos FSX para ONTAP y VMC.

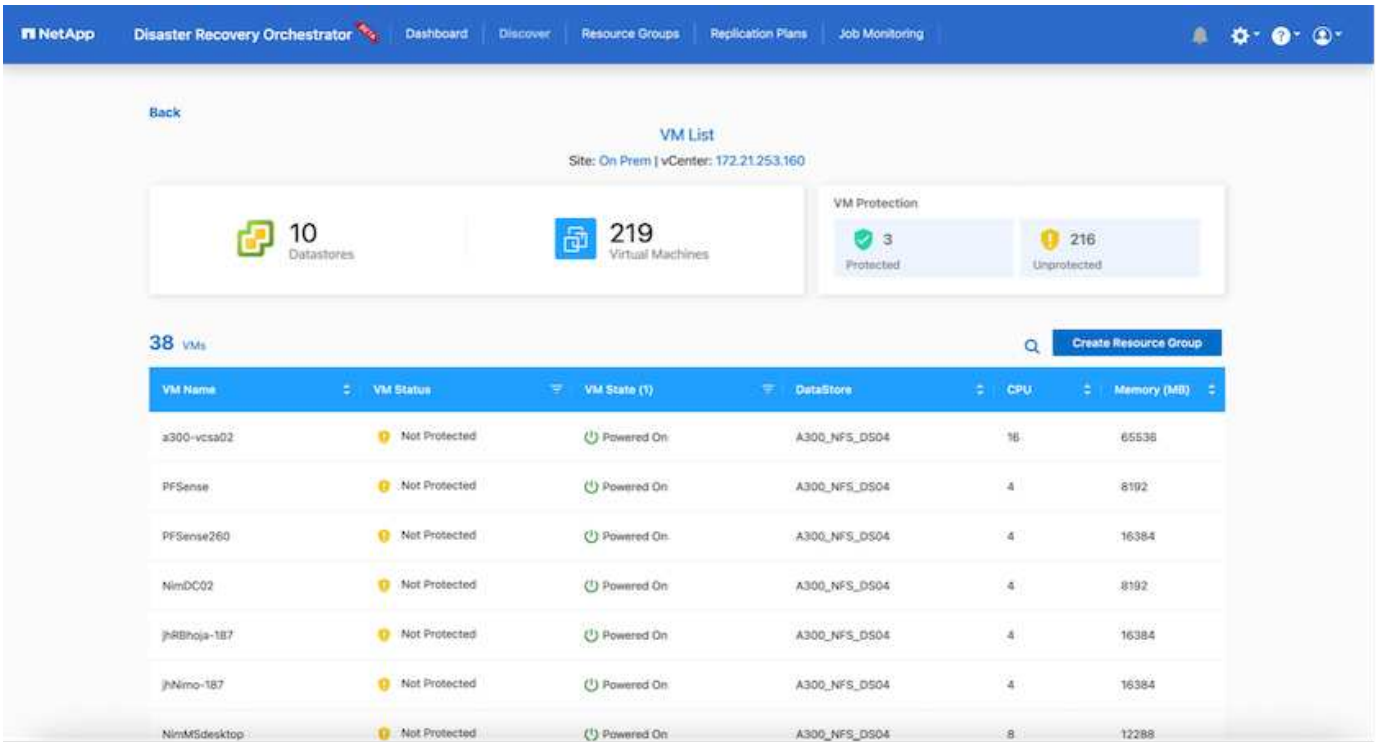
El primer paso es descubrir y añadir los recursos locales y cloud (tanto vCenter como almacenamiento) a la DRO. Abra DRO en un navegador compatible y utilice el nombre de usuario y la contraseña predeterminados (admin/admin) y Add Sites. También se pueden añadir sitios mediante la opción detectar. Añada las siguientes plataformas:

- Localmente
  - En las instalaciones de vCenter
  - Sistema de almacenamiento ONTAP
- Cloud
  - VCenter de VMC
  - FSX para ONTAP





Una vez añadida, DRO realiza la detección automática y muestra las máquinas virtuales con las réplicas de SnapMirror correspondientes desde el almacenamiento de origen a FSX para ONTAP. DRO detecta automáticamente las redes y los grupos de puertos utilizados por los equipos virtuales y los rellena.



El siguiente paso es agrupar los equipos virtuales necesarios en grupos funcionales para servir como grupos de recursos.

Agrupaciones de recursos

Después de añadir las plataformas, puede agrupar las máquinas virtuales que desea recuperar en grupos de recursos. LOS grupos de recursos DE DRO permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque, retrasos de arranque y validaciones de aplicaciones opcionales que se pueden ejecutar tras la recuperación.

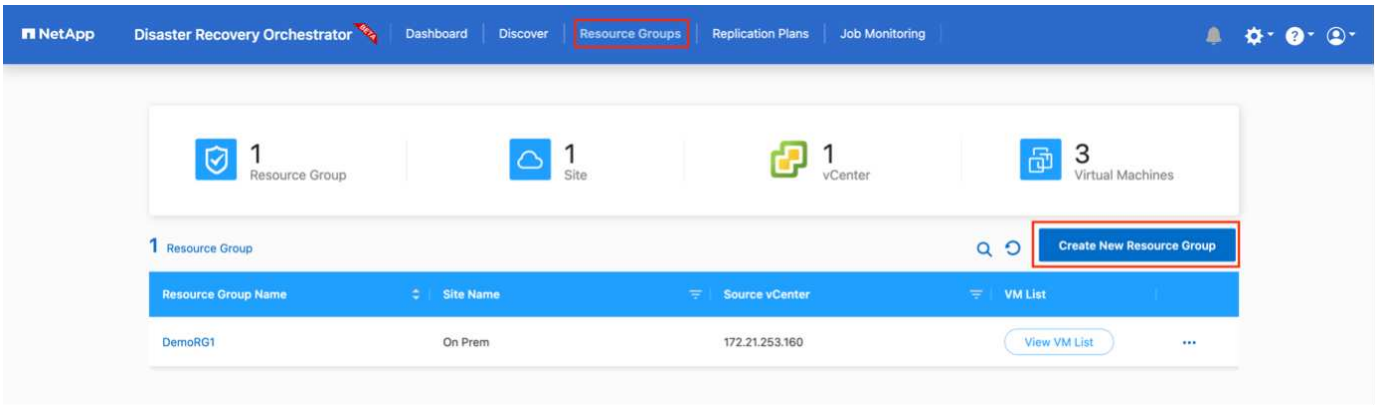
Para comenzar a crear grupos de recursos, complete los siguientes pasos:

1. Acceda a **grupos de recursos** y haga clic en **Crear nuevo grupo de recursos**.
2. En **Nuevo grupo de recursos**, seleccione el sitio de origen en la lista desplegable y haga clic en **Crear**.
3. Proporcione **Detalles del grupo de recursos** y haga clic en **continuar**.
4. Seleccione los equipos virtuales adecuados con la opción de búsqueda.
5. Seleccione el orden de arranque y el retraso de arranque (segundos) para las máquinas virtuales seleccionadas. Para establecer el orden de encendido, seleccione cada máquina virtual y configure la prioridad para ella. Tres es el valor predeterminado para todas las máquinas virtuales.

   Las opciones son estas:

   1 – la primera máquina virtual que se enciende 3 – valor predeterminado 5 – la última máquina virtual que se enciende

6. Haga clic en **Crear grupo de recursos**.

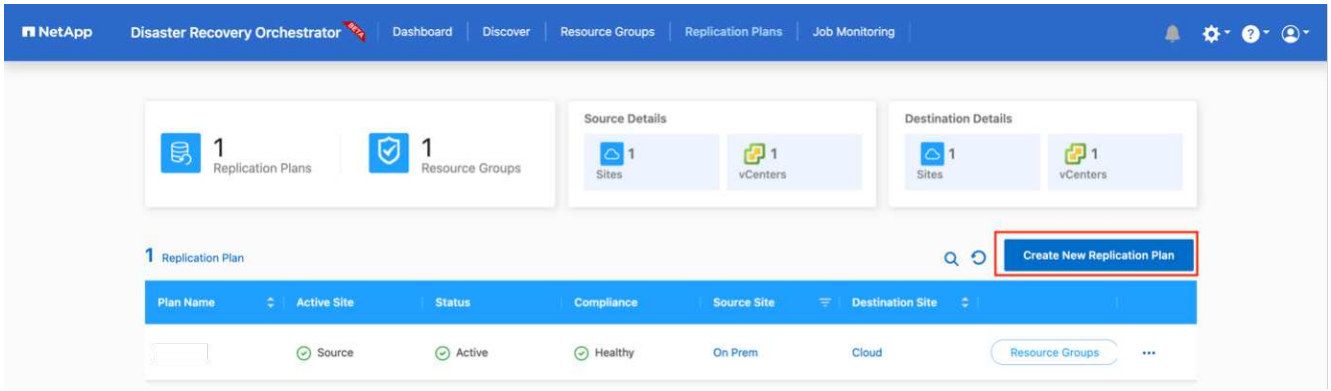


Planes de replicación

Necesita un plan para recuperar las aplicaciones en caso de un desastre. Seleccione las plataformas de vCenter de origen y destino del menú desplegable y seleccione los grupos de recursos que se incluirán en este plan, junto con la agrupación de cómo deben restaurarse y encenderse las aplicaciones (por ejemplo, controladoras de dominio, después nivel 1, después nivel 2, etc.). Tales planes a veces también se denominan modelos. Para definir el plan de recuperación, vaya a la ficha **Plan de replicación** y haga clic en **Nuevo Plan de replicación**.

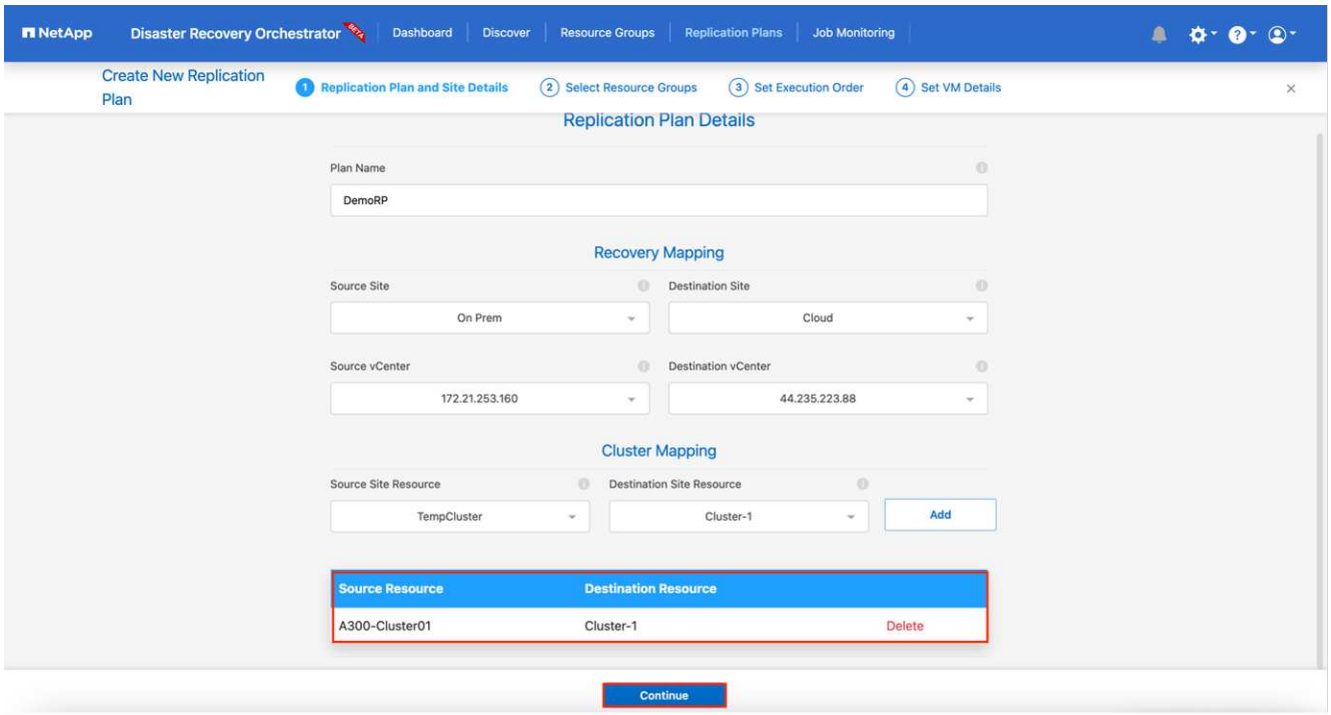
Para comenzar a crear un plan de replicación, lleve a cabo los siguientes pasos:

1. Acceda a **planes de replicación** y haga clic en **Crear nuevo plan de replicación**.



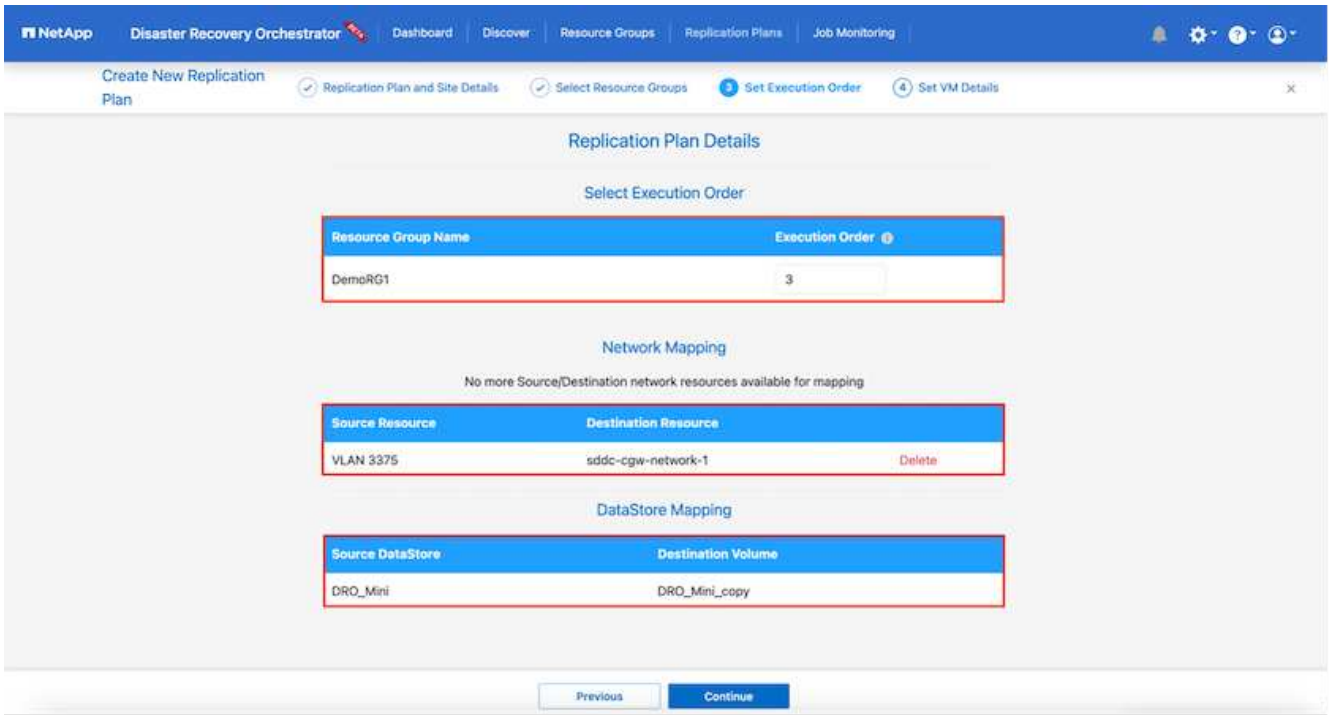
2. En **Nuevo Plan de replicación**, proporcione un nombre para el plan y agregue asignaciones de recuperación seleccionando el sitio de origen, vCenter asociada, sitio de destino y vCenter asociada.

3. Después de completar la asignación de recuperación, seleccione la asignación de clústeres.

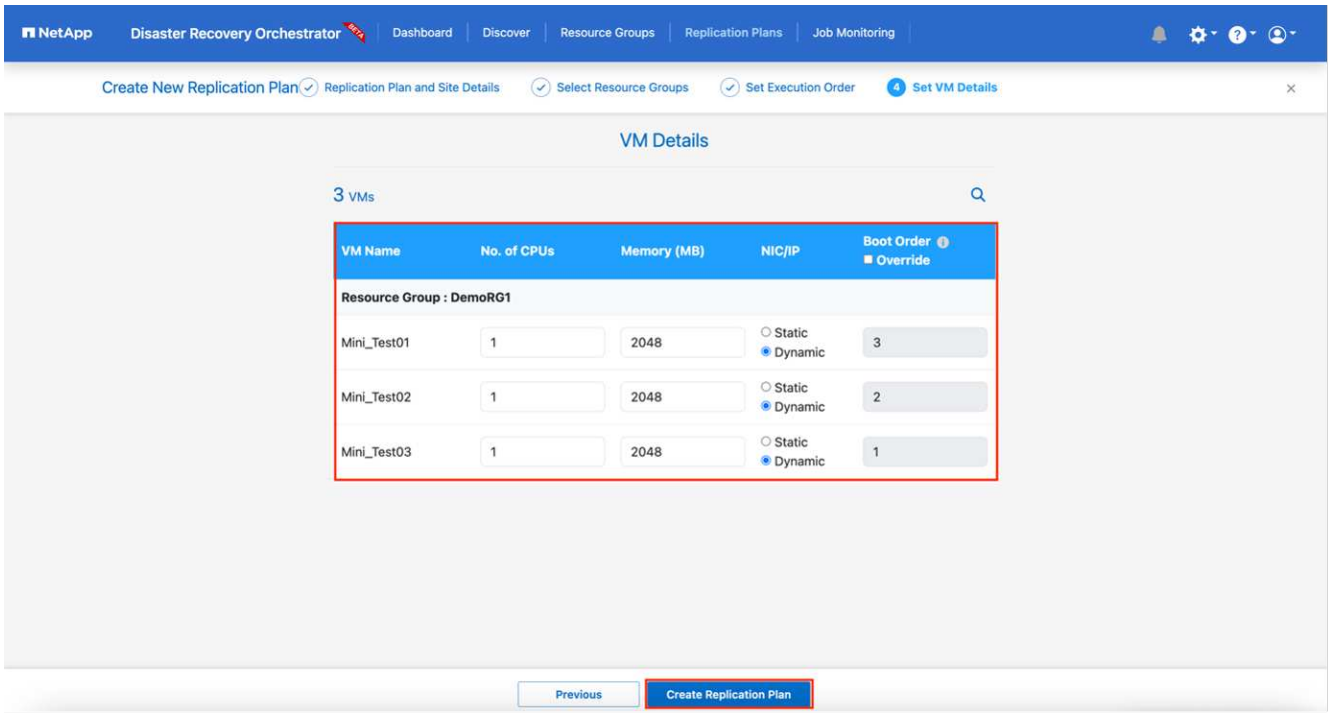


4. Seleccione **Detalles del grupo de recursos** y haga clic en **continuar**.
5. Establezca el orden de ejecución del grupo de recursos. Esta opción permite seleccionar la secuencia de operaciones cuando existen varios grupos de recursos.
6. Una vez que haya terminado, seleccione la asignación de red al segmento apropiado. Los segmentos ya se deben aprovisionar dentro de VMC, así que seleccione el segmento adecuado para asignar la VM.
7. Según la selección de las máquinas virtuales, las asignaciones de almacenes de datos se seleccionan automáticamente.

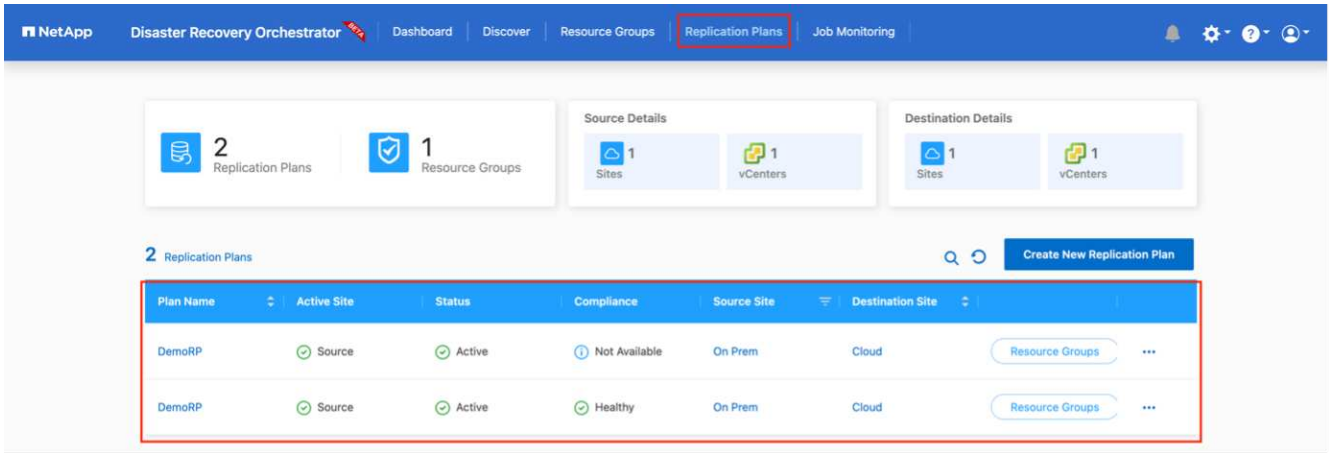
> SnapMirror se encuentra en el nivel de volumen. Por lo tanto, todas las máquinas virtuales se replican en el destino de replicación. Asegúrese de seleccionar todas las máquinas virtuales que forman parte del almacén de datos. Si no se seleccionan, solo se procesan las máquinas virtuales que forman parte del plan de replicación.



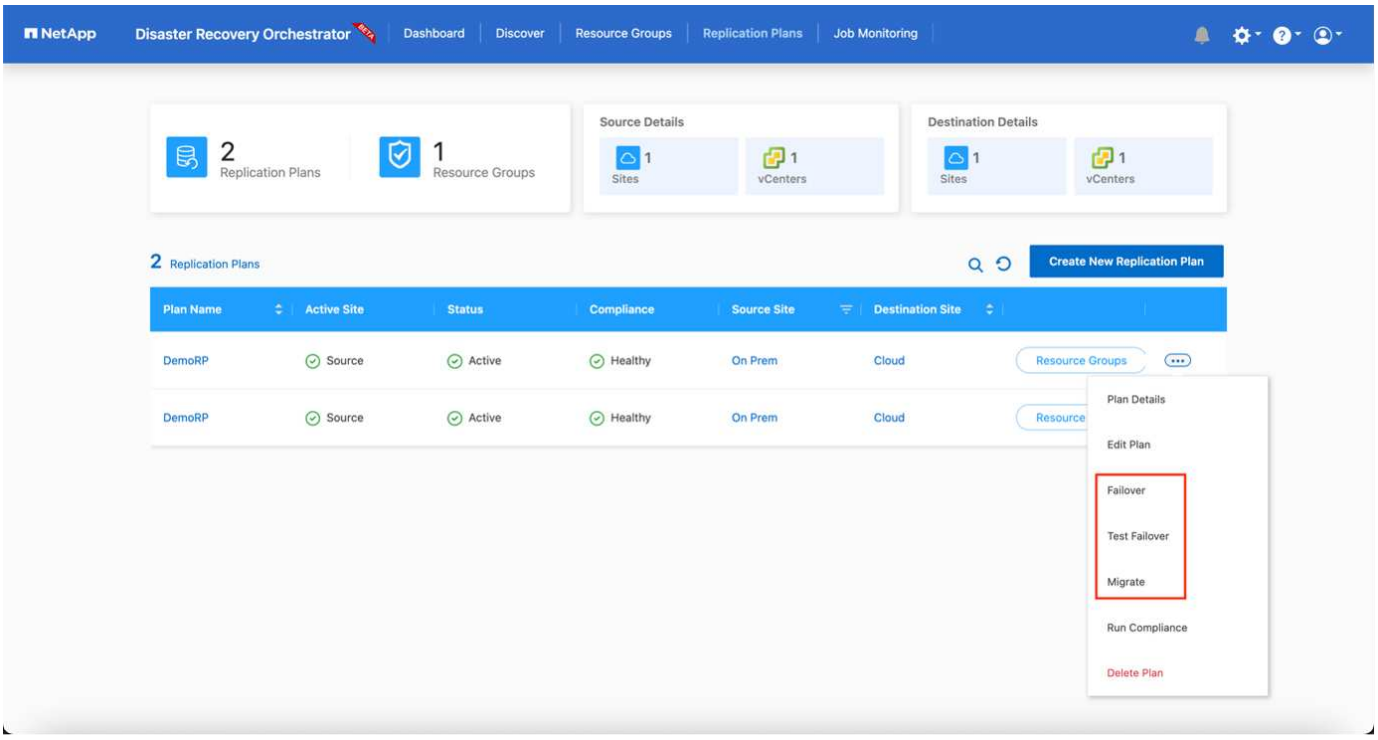
8. Si se especifican los datos del equipo virtual, se puede modificar de forma opcional el tamaño de los parámetros de RAM y CPU del equipo virtual; esto puede resultar muy útil a la hora de recuperar entornos de gran tamaño en clústeres de destino más pequeños o realizar pruebas de recuperación ante desastres sin tener que aprovisionar una infraestructura de VMware física única. Además, puede modificar el orden de arranque y el retraso de arranque (segundos) para todas las máquinas virtuales seleccionadas entre los grupos de recursos. Existe una opción adicional para modificar el orden de arranque si se requieren cambios de los seleccionados durante la selección de orden de arranque del grupo de recursos. De forma predeterminada, se utiliza el orden de arranque seleccionado durante la selección de grupos de recursos; sin embargo, se pueden realizar modificaciones en esta fase.



9. Haga clic en **Crear plan de replicación**.

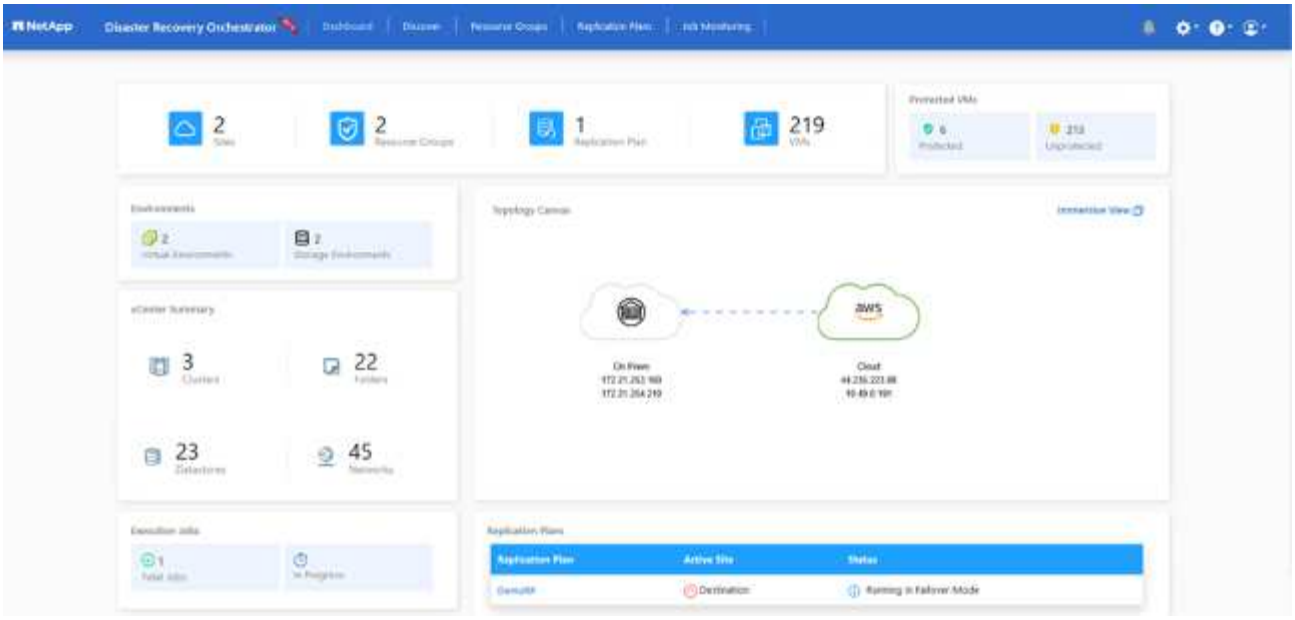


Una vez creado el plan de replicación, la opción de conmutación por error, la opción de conmutación por error de prueba o la opción de migración se pueden ejercer en función de los requisitos. Durante las opciones de conmutación por error y conmutación al nodo de respaldo, se utiliza la copia Snapshot de SnapMirror más reciente o se puede seleccionar una copia Snapshot específica de una copia Snapshot puntual (según la política de retención de SnapMirror). La opción de momento específico puede ser muy útil si se enfrenta a un evento de corrupción como ransomware, donde las réplicas más recientes ya están comprometidas o cifradas. DRO muestra todos los puntos disponibles en el tiempo. Para activar la conmutación por error o la conmutación por error de prueba con la configuración especificada en el plan de replicación, puede hacer clic en **failover** o **Prueba de conmutación por error**.

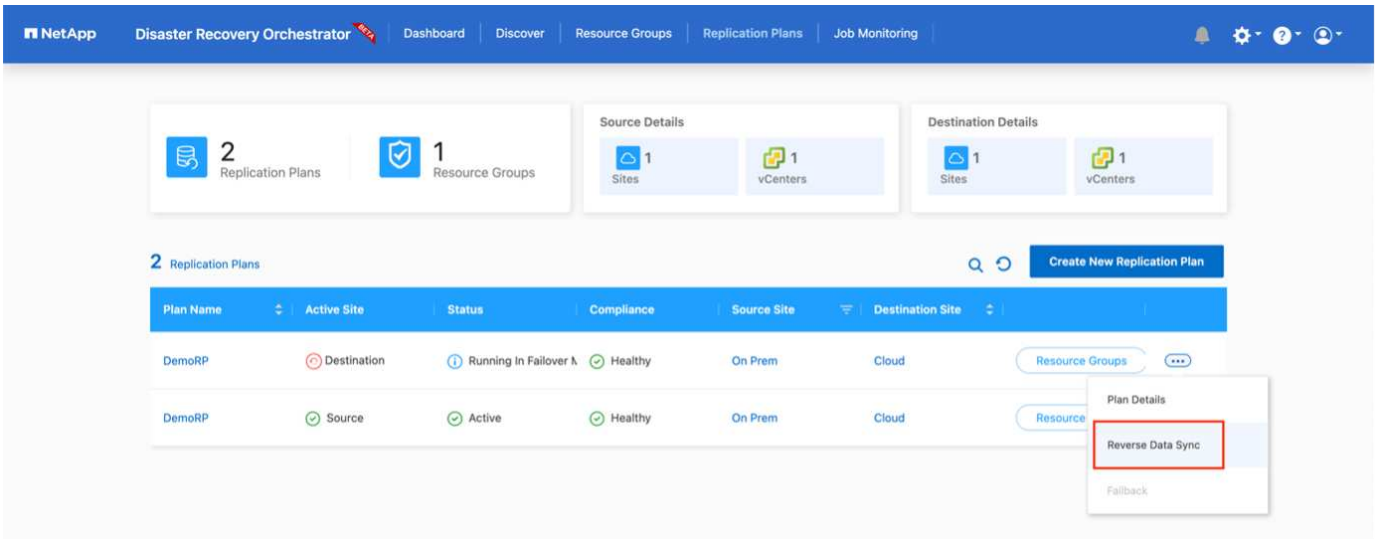


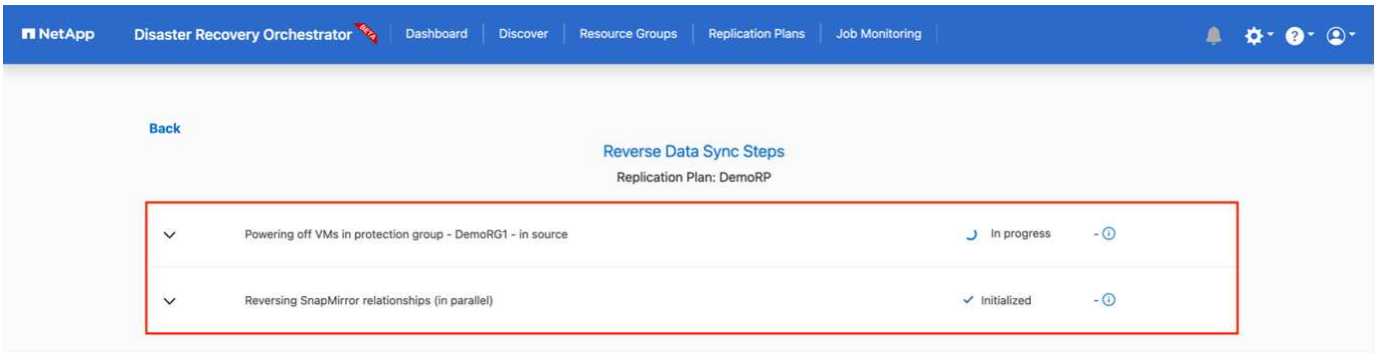
El plan de replicación se puede supervisar en el menú de tareas:

Después de activar la conmutación por error, los elementos recuperados pueden verse en el VMC vCenter (máquinas virtuales, redes y almacenes de datos). De forma predeterminada, las máquinas virtuales se recuperan en la carpeta de carga de trabajo.

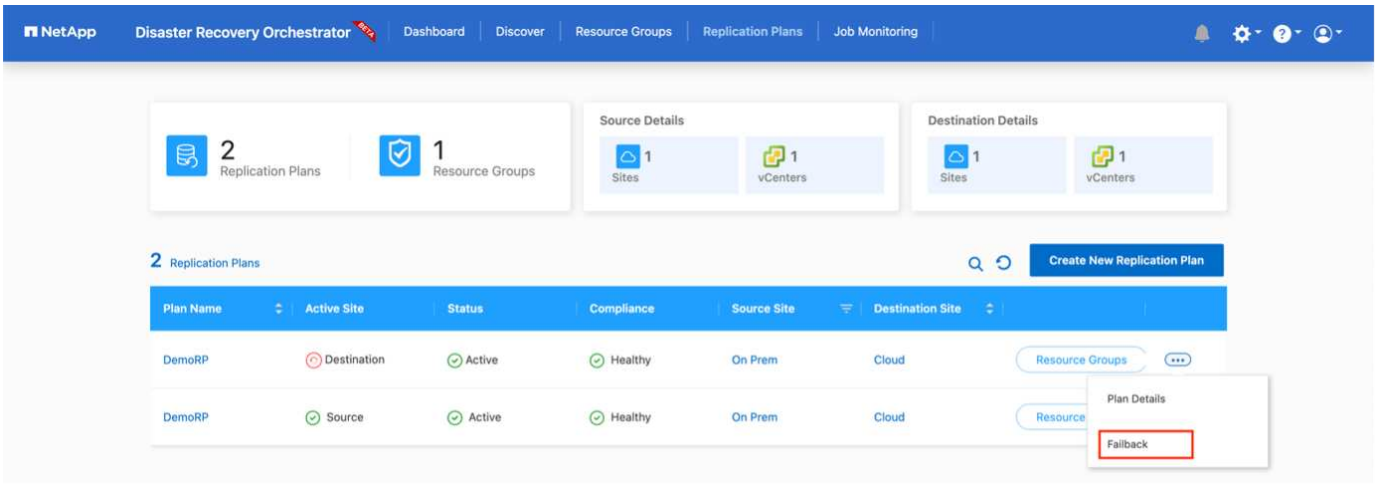


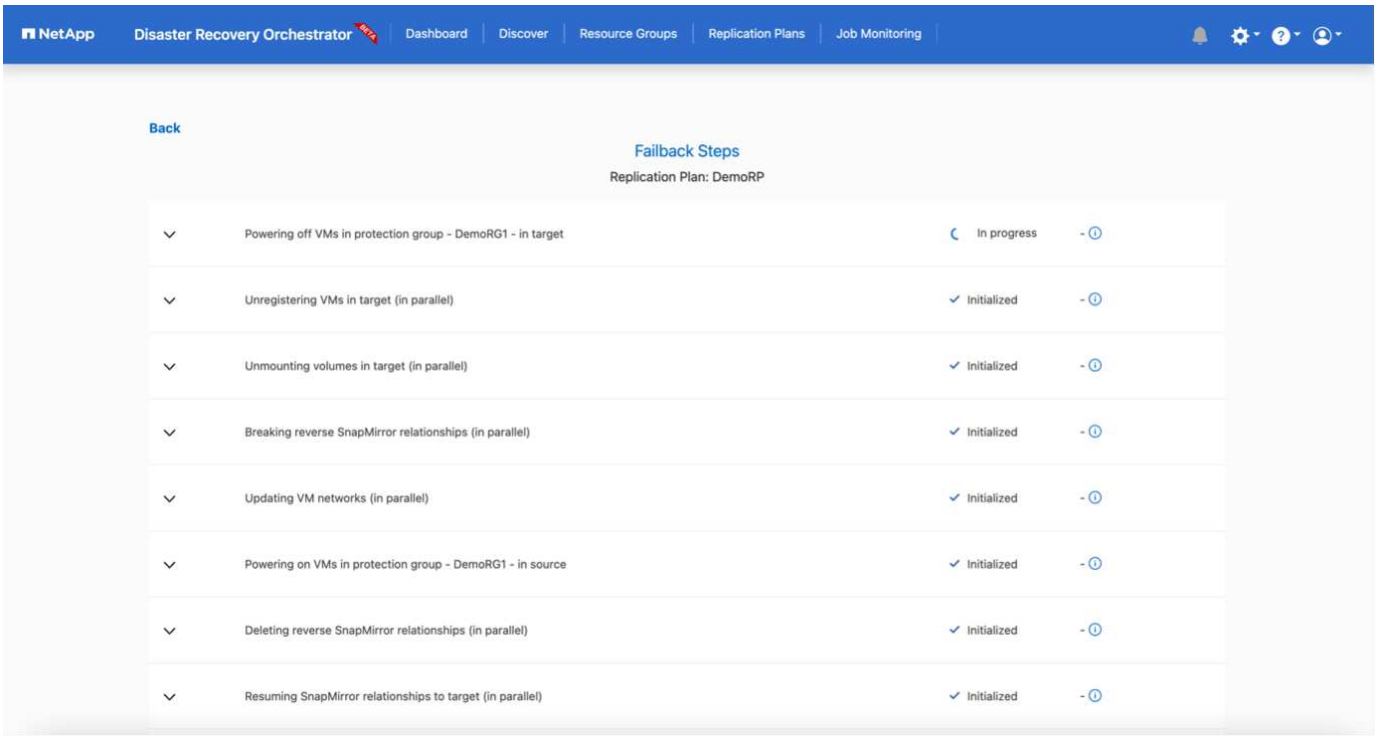
La conmutación por recuperación se puede activar en el nivel de plan de replicación. En el caso de una conmutación por error de prueba, se puede utilizar la opción de eliminación para revertir los cambios y eliminar la relación de FlexClone. La conmutación por recuperación relacionada con la conmutación por error es un proceso de dos pasos. Seleccione el plan de replicación y seleccione **sincronización inversa de datos**.



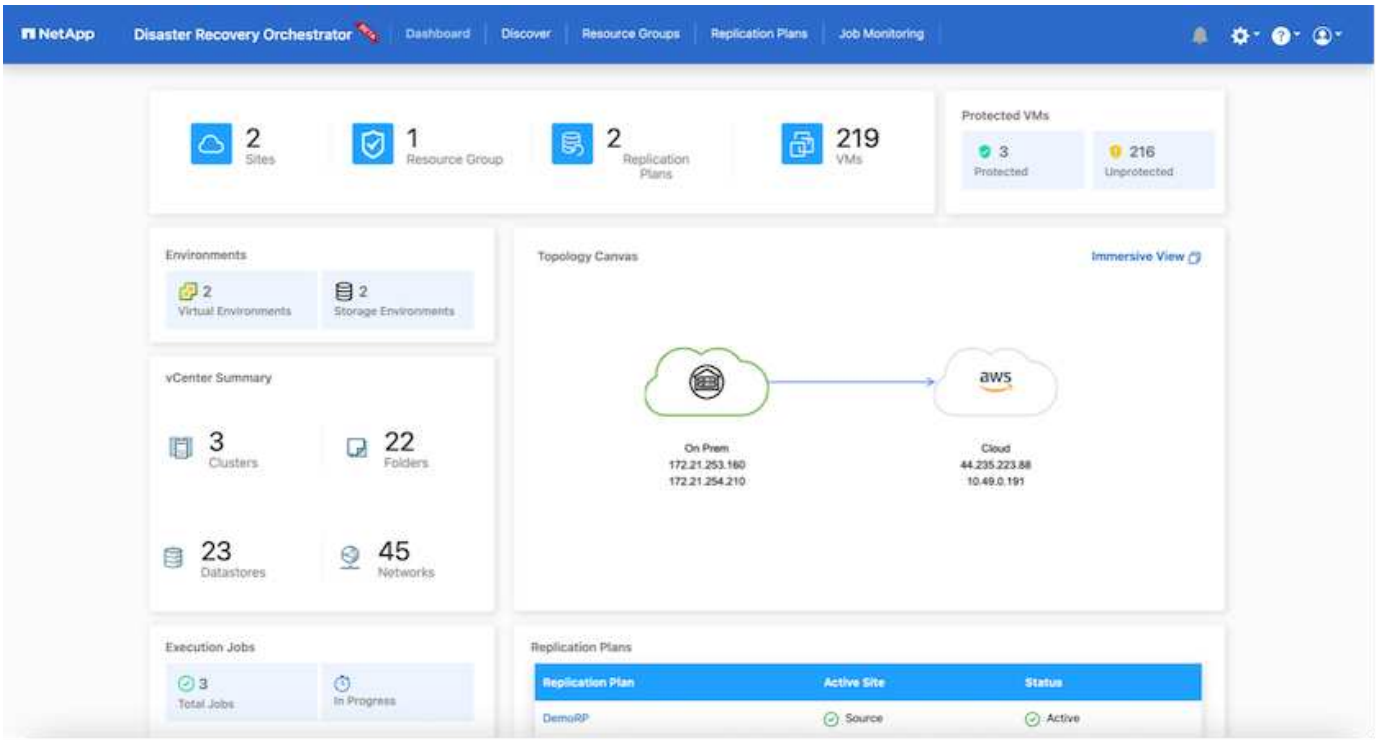


Una vez finalizada, puede activar la conmutación tras recuperación para volver a la instalación de producción original.





Desde BlueXP de NetApp vemos que el estado de la replicación se ha roto para los volúmenes adecuados (los asignados a VMC como volúmenes de lectura y escritura). Durante la conmutación al nodo de respaldo de prueba, DRO no asigna el volumen de destino o de réplica. En su lugar, realiza una copia FlexClone de la instancia de SnapMirror (o Snapshot) necesaria y expone la instancia de FlexClone, que no consume capacidad física adicional para FSX para ONTAP. Este proceso garantiza que el volumen no se modifique y que los trabajos de réplica puedan continuar incluso durante las pruebas de recuperación ante desastres o los flujos de trabajo de clasificación. Además, este proceso garantiza que, si se producen errores o se recuperan los datos dañados, la recuperación se puede limpiar sin riesgo de destrucción de la réplica.



Recuperación de ransomware

Recuperarse del ransomware puede ser una tarea abrumadora. En concreto, a las organizaciones DE TI les puede resultar complicado identificar el punto de retorno seguro y, una vez determinado, proteger las cargas de trabajo recuperadas de ataques recurrentes, por ejemplo, de malware en suspensión o aplicaciones vulnerables.

DRO aborda estas preocupaciones al permitirle recuperar su sistema desde cualquier momento disponible. También puede recuperar cargas de trabajo en redes funcionales pero aisladas, de tal modo que las aplicaciones puedan funcionar y comunicarse entre sí en una ubicación en la que no estén expuestas al tráfico del norte al sur. Esto le da a su equipo de seguridad un lugar seguro para llevar a cabo los análisis forenses y asegurarse de que no hay malware oculto o dormido.

Beneficios

- El uso de la replicación SnapMirror eficiente y resiliente.
- Recuperación en cualquier momento disponible con la retención de copias de Snapshot.
- Automatización completa de todos los pasos necesarios para recuperar cientos o miles de equipos virtuales a partir de los pasos de almacenamiento, informática, red y validación de aplicaciones.
- Recuperación de la carga de trabajo con la tecnología FlexClone de ONTAP mediante un método que no cambia el volumen replicado.
  - Evita el riesgo de que se dañen los datos para volúmenes o copias Snapshot.
  - Evita interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
  - Uso potencial de datos de recuperación ante desastres con recursos de cloud computing para flujos de trabajo más allá de la recuperación ante desastres, como DevTest, pruebas de seguridad, pruebas de parches o actualizaciones, y pruebas de corrección.
- Optimización de la CPU y la RAM para ayudar a reducir los costes del cloud al permitir la recuperación en clústeres informáticos más pequeños.

Usar la replicación de Veeam y FSx para ONTAP para la recuperación ante desastres en VMware Cloud on AWS

Autor: Niyaz Mohamed - Ingeniería de Soluciones NetApp

Descripción general

La integración de Amazon FSx para NetApp ONTAP con VMware Cloud en AWS es un almacén de datos NFS externo y gestionado por AWS basado en el sistema de archivos ONTAP de NetApp que se puede conectar a un clúster en SDDC. Proporciona a los clientes una infraestructura de almacenamiento virtualizado flexible y de alto rendimiento que se puede escalar independientemente de los recursos de computación.

Para aquellos clientes que busquen usar VMware Cloud en AWS SDDC como objetivo de recuperación ante desastres, los almacenes de datos FSx para ONTAP se pueden usar para replicar datos desde las instalaciones mediante cualquier solución validada de terceros que proporciona la funcionalidad de replicación de máquinas virtuales. Al añadir el almacén de datos FSx para ONTAP, permitirá una puesta en marcha optimizada en costes que la creación del cloud de VMware en SDDC de AWS con una enorme cantidad de hosts ESXi para acomodar el almacenamiento.

Este enfoque también ayuda a los clientes a utilizar un clúster ligero piloto en VMC junto con almacenes de datos de FSx para ONTAP para alojar las réplicas de máquinas virtuales. También se puede ampliar el mismo proceso como una opción de migración a VMware Cloud en AWS al conmutar al nodo de respaldo sin incidencias del plan de replicación.

Declaración del problema

Este documento describe cómo utilizar el almacén de datos FSx para ONTAP y Veeam Backup y la replicación para configurar la recuperación ante desastres para máquinas virtuales VMware on-premises en VMware Cloud on AWS usando la funcionalidad de replicación de máquinas virtuales.

Veeam Backup & Replication permite la replicación local y remota para la recuperación ante desastres (DR). Cuando se replican máquinas virtuales, Veeam Backup & Replication crea una copia exacta de las máquinas virtuales en el formato nativo de VMware vSphere en el clúster SDDC de VMware Cloud on AWS de destino y mantiene la copia sincronizada con la máquina virtual original.

La replicación proporciona los mejores valores de objetivo de tiempo de recuperación (RTO) ya que hay una copia de un equipo virtual en estado listo para comenzar. Este mecanismo de replicación garantiza que las cargas de trabajo puedan iniciarse rápidamente en VMware Cloud on AWS SDDC en caso de un desastre. El software Veeam Backup & Replication también optimiza la transmisión del tráfico para la replicación a través de WAN y conexiones lentas. Además, también filtra los bloques de datos duplicados, cero bloques de datos, archivos de intercambio y archivos excluidos del sistema operativo invitado del equipo virtual, y comprime el tráfico de la réplica.

Para evitar que los trabajos de replicación consuman todo el ancho de banda de la red, se pueden poner en marcha aceleradores WAN y reglas de limitación de red. El proceso de replicación en Veeam Backup & Replication está controlado por tareas, lo que significa que la replicación se realiza mediante la configuración de trabajos de replicación. En caso de desastre, se puede activar la conmutación al respaldo para recuperar las máquinas virtuales conmutando por error a su copia de réplica.

Cuando se realiza una conmutación por error, una máquina virtual replicada asume el rol de la máquina virtual original. La conmutación por error se puede realizar en el estado más reciente de una réplica o en cualquiera de sus puntos de restauración conocidos. Esto permite la recuperación frente al ransomware o las pruebas aisladas según sea necesario. En Veeam Backup & Replication, la conmutación por error y la conmutación

tras recuperación son pasos intermedios temporales que deberían completarse aún más. Veeam Backup & Replication ofrece múltiples opciones para gestionar diferentes escenarios de recuperación ante desastres.

[Diagrama del escenario de recuperación ante desastres con replicación de Veeam y FSx ONTAP para VMC]

Puesta en marcha de la solución

Escalones de alto nivel

1. El software Veeam Backup and Replication se ejecuta en un entorno en las instalaciones con la conectividad de red adecuada.
2. Configure VMware Cloud en AWS, consulte el artículo VMware Cloud Tech Zone "Guía de puesta en marcha de la integración de VMware Cloud on AWS con Amazon FSx para NetApp ONTAP" Para ponerla en marcha, configura VMware Cloud en AWS SDDC y FSx para ONTAP como almacén de datos NFS. (Un entorno piloto configurado con una configuración mínima se puede usar con fines de recuperación ante desastres. Los equipos virtuales se conmutarán por error a este clúster en caso de que se produzca un incidente y se podrán agregar nodos adicionales).
3. Configure trabajos de replicación para crear réplicas de máquinas virtuales con Veeam Backup and Replication.
4. Crear un plan de recuperación tras fallos y realizar una recuperación tras fallos.
5. Vuelva a los equipos virtuales de producción una vez que el evento de desastre haya finalizado y el sitio principal esté activo.

Requisitos previos de la replicación de Veeam VM en VMC y FSx para almacenes de datos de ONTAP

1. Garantizar que la máquina virtual de backup de Veeam Backup & Replication esté conectada a la instancia de vCenter de origen, así como al cloud de VMware de destino en los clústeres de SDDC de AWS.
2. El servidor de copia de seguridad debe ser capaz de resolver nombres cortos y conectarse a vCenters de origen y destino.
3. El almacén de datos FSx para ONTAP de destino debe tener suficiente espacio libre para almacenar VMDK de máquinas virtuales replicadas

Para obtener información adicional, consulte “Consideraciones y limitaciones” cubiertos "aquí".

Detalles de la implementación

Paso 1: Replicar máquinas virtuales

Veeam Backup & Replication aprovecha las funcionalidades de snapshot de VMware vSphere y, durante la replicación, Veeam Backup & Replication solicita a VMware vSphere para crear una snapshot de máquina virtual. La snapshot de la máquina virtual es la copia de un momento específico de una máquina virtual que incluye discos virtuales, estado del sistema, configuración, etc. Veeam Backup & Replication utiliza la snapshot como fuente de datos para la replicación.

Para replicar equipos virtuales, siga los siguientes pasos:

1. Abra Veeam Backup & Replication Console.
2. En la vista Inicio, seleccione Replication Job > Virtual machine > VMware vSphere.
3. Especifique un nombre de trabajo y seleccione la casilla de control avanzada adecuada. Haga clic en Siguiente.
   - Active la casilla de verificación Replica seeding si la conectividad entre las instalaciones y AWS tiene ancho de banda restringido.
   - Seleccione la casilla de verificación Remapping de red (para sitios VMC de AWS con redes diferentes) si los segmentos de VMware Cloud en AWS SDDC no coinciden con los de las redes del sitio local.
   - Si el esquema de direccionamiento IP en el sitio de producción local difiere del esquema en el sitio VMC de AWS, seleccione la casilla de verificación Réplica por IP (para sitios de DR con esquema de direccionamiento IP diferente).

     [dr veeam fsx image2] | *dr-veeam-fsx-image2.png*
4. Seleccione las máquinas virtuales que se deben replicar en el almacén de datos FSx para ONTAP conectado a VMware Cloud en AWS SDDC en el paso * Máquinas virtuales **. Las máquinas virtuales se pueden colocar en vSAN para llenar la capacidad de almacenes de datos vSAN disponible. En un clúster ligero piloto, la capacidad útil de un clúster de 3 nodos se verá limitada. El resto de datos puede replicarse en los almacenes de datos de FSx for ONTAP. Haga clic en *Agregar**, luego en la ventana **Agregar Objeto** seleccione las VM o contenedores de VM necesarios y haga clic en **Agregar**. Haga clic en **Siguiente**.

   [dr veeam fsx image3] | *dr-veeam-fsx-image3.png*
5. Después de eso, seleccione el destino como clúster/host SDDC de VMware Cloud on AWS y el conjunto de recursos apropiado, la carpeta de VM y el almacén de datos FSx para ONTAP para réplicas de VM. Luego haga clic en **Siguiente**.

   [dr veeam fsx image4] | *dr-veeam-fsx-image4.png*
6. En el siguiente paso, cree la asignación entre la red virtual de origen y de destino según sea necesario.

   [dr veeam fsx image5] | *dr-veeam-fsx-image5.png*
7. En el paso **Configuración del trabajo**, especifique el repositorio de copia de seguridad que almacenará metadatos para réplicas de VM, política de retención, etc.
8. Actualice los servidores proxy **Source** y **Target** en el paso **Data Transfer** y deje la selección **Automatic** (predeterminada) y mantenga seleccionada la opción **Direct** y haga clic en **Next**.
9. En el paso **Guest Processing**, selecciona la opción **Enable application-aware processing** según sea necesario. Haga clic en **Siguiente**.

[dr veeam fsx image6] | *dr-veeam-fsx-image6.png*

10. Seleccione el programa de replicación para ejecutar el trabajo de replicación con regularidad.
11. En el paso **Summary** del asistente, revise los detalles del trabajo de replicación. Para iniciar el trabajo justo después de cerrar el asistente, seleccione la casilla de verificación **Ejecutar el trabajo cuando haga clic en Finalizar**, de lo contrario deje la casilla de verificación sin seleccionar. A continuación, haga clic en **Finalizar** para cerrar el asistente.

    [dr veeam fsx image7] | *dr-veeam-fsx-image7.png*

Una vez que se inicie el trabajo de replicación, las máquinas virtuales con el sufijo especificado se completarán en el clúster/host de VMC SDDC de destino.

[dr veeam fsx image8] | *dr-veeam-fsx-image8.png*

Para obtener información adicional sobre la replicación de Veeam, consulte "Funcionamiento de la replicación".

Paso 2: Crear un plan de failover

Una vez finalizada la replicación inicial o la propagación, cree el plan de conmutación por error. El plan de conmutación por error ayuda a realizar la conmutación por error de los equipos virtuales dependientes uno por uno o como grupo automáticamente. El plan de conmutación por error es el plan del orden en el que se procesan los equipos virtuales, incluidos los retrasos en el inicio. El plan de conmutación por error también ayuda a garantizar que los equipos virtuales cruciales dependientes ya se estén ejecutando.

Para crear el plan, navegue a la nueva subsección denominada Replicates y seleccione Failover Plan. Seleccione los equipos virtuales adecuados. Veeam Backup & Replication buscará los puntos de restauración más cercanos a este punto en el tiempo y los utilizará para iniciar réplicas de máquinas virtuales.

ⓘ El plan de conmutación por error solo se puede agregar una vez que la replicación inicial se haya completado y las réplicas de las máquinas virtuales estén en estado Listo.

ⓘ El número máximo de equipos virtuales que se pueden iniciar simultáneamente cuando se ejecuta un plan de conmutación al nodo de respaldo es de 10.

ⓘ Durante el proceso de conmutación al nodo de respaldo, los equipos virtuales de origen no se apagarán.

Para crear el **Failover Plan**, haga lo siguiente:

1. En la vista Inicio, seleccione **Failover Plan > VMware vSphere**.
2. A continuación, proporcione un nombre y una descripción al plan. El script previo y posterior al failover se puede agregar según sea necesario. Por ejemplo, ejecute un script para cerrar los equipos virtuales antes de iniciar los equipos virtuales replicados.

   [dr veeam fsx image9] | *dr-veeam-fsx-image9.png*

3. Agregue las máquinas virtuales al plan y modifique el orden de arranque de la máquina virtual y los retrasos de arranque para cumplir con las dependencias de la aplicación.

   [dr veeam fsx image10] | *dr-veeam-fsx-image10.png*

Para obtener más información sobre la creación de trabajos de replicación, consulte "Creación de trabajos de replicación".

Paso 3: Ejecute el plan de failover

En caso de fallo, la máquina virtual de origen del sitio de producción cambia a su réplica en el sitio de recuperación de desastres. Como parte del proceso de conmutación por error, Veeam Backup & Replication restaura la réplica de la máquina virtual al punto de restauración deseado y mueve todas las actividades de I/O del equipo virtual de origen a su réplica. Las réplicas pueden usarse no solo en caso de desastre, sino también para simular simulacros de recuperación ante desastres. Durante la simulación de recuperación tras fallos, la máquina virtual de origen sigue ejecutándose. Una vez realizadas todas las pruebas necesarias, puede deshacer la conmutación por error y volver a las operaciones normales.

Asegúrese de que la segmentación de la red está en su lugar para evitar conflictos de IP durante los simulacros de DR.

Para iniciar el plan de conmutación por error, simplemente haga clic en la pestaña **Planes de conmutación por error** y haga clic con el botón derecho en el plan de conmutación por error. Seleccione **Iniciar**. Se conmutará al nodo de respaldo usando los puntos de restauración más recientes de réplicas de equipos virtuales. Para conmutar por error a puntos de restauración específicos de réplicas de VM, seleccione **Iniciar a**.

[dr veeam fsx image11] | *dr-veeam-fsx-image11.png*

[dr veeam fsx image12] | *dr-veeam-fsx-image12.png*

El estado de la réplica de VM cambia de Ready a Failover y VMs comenzará en el clúster/host de destino de VMware Cloud en AWS SDDC.

[dr veeam fsx image13] | *dr-veeam-fsx-image13.png*

Una vez finalizada la conmutación por error, el estado de las máquinas virtuales cambiará a «Failover».

[dr veeam fsx image14] | *dr-veeam-fsx-image14.png*

Veeam Backup & Replication detiene todas las actividades de replicación de la máquina virtual de origen hasta que su réplica vuelve al estado Ready.

Para obtener información detallada sobre los planes de conmutación por error, consulte "Planes de conmutación al respaldo".

Paso 4: Conmutación por recuperación al sitio de producción

Cuando se ejecuta el plan de failover, se considera un paso intermedio y debe finalizarse según el requisito. Las opciones incluyen las siguientes:

- **Failback to production** - cambia de nuevo a la VM original y transfiere todos los cambios que tuvieron lugar mientras la réplica de la VM se estaba ejecutando a la VM original.

> Al realizar la conmutación por recuperación, los cambios solo se transfieren pero no se publican. Seleccione **Commit failback** (una vez que la VM original se confirme para funcionar como se esperaba) o **Deshacer failback** para volver a la réplica de la VM Si la VM original no funciona como se esperaba.

- **Deshacer failover** - cambiar de nuevo a la VM original y descartar todos los cambios realizados en la réplica de la VM mientras se estaba ejecutando.
- **Failover permanente** - Cambie permanentemente de la VM original a una réplica de VM y utilice esta réplica como la VM original.

En esta demostración se eligió la conmutación de retorno tras recuperación en producción. Se ha seleccionado la conmutación por recuperación a la VM original durante el paso de destino del asistente y la casilla de verificación “Power on VM after restoring” estaba activada.

[dr veeam fsx image15] | *dr-veeam-fsx-image15.png*

[dr veeam fsx image16] | *dr-veeam-fsx-image16.png*

La confirmación de conmutación por recuperación es una de las formas de finalizar la operación de conmutación por recuperación. Cuando se confirma la conmutación por recuperación, confirma que los cambios enviados a la máquina virtual que se devuelve una conmutación por error (la máquina virtual de producción) funcionan según lo esperado. Tras la operación de confirmación, Veeam Backup & Replication reanuda las actividades de replicación para la máquina virtual de producción.

Para obtener información detallada sobre el proceso de conmutación por recuperación, consulte la documentación de Veeam para "Conmutación al nodo de respaldo y conmutación de retorno tras recuperación para replicación".

[dr veeam fsx image17] | *dr-veeam-fsx-image17.png*

[dr veeam fsx image18] | *dr-veeam-fsx-image18.png*

Una vez que la conmutación de retorno tras recuperación en producción se realiza correctamente, las máquinas virtuales se restauran de nuevo en el sitio de producción original.

[dr veeam fsx image19] | *dr-veeam-fsx-image19.png*

Conclusión

La funcionalidad de almacén de datos FSx para ONTAP permite que Veeam o cualquier herramienta validada de terceros proporcionen una solución de recuperación ante desastres de bajo coste con un clúster ligero de piloto y sin necesidad de instalar un gran número de hosts en el clúster para acomodar la copia de réplica de la máquina virtual. Esto ofrece una potente solución que gestiona un plan de recuperación ante desastres personalizado y personalizado, y permite también reutilizar productos de backup existentes de forma interna para satisfacer las necesidades de recuperación ante desastres, lo que permite la recuperación ante

desastres basada en el cloud saliendo de los centros de datos de recuperación ante desastres en las instalaciones. La conmutación por error se puede realizar como conmutación al respaldo planificada o conmutación al respaldo con un clic de un botón cuando se produce un desastre y se toma la decisión de activar el sitio de recuperación ante desastres.

Para obtener más información sobre este proceso, puede seguir el vídeo detallado del tutorial.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.