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

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

Tabla de contenidos

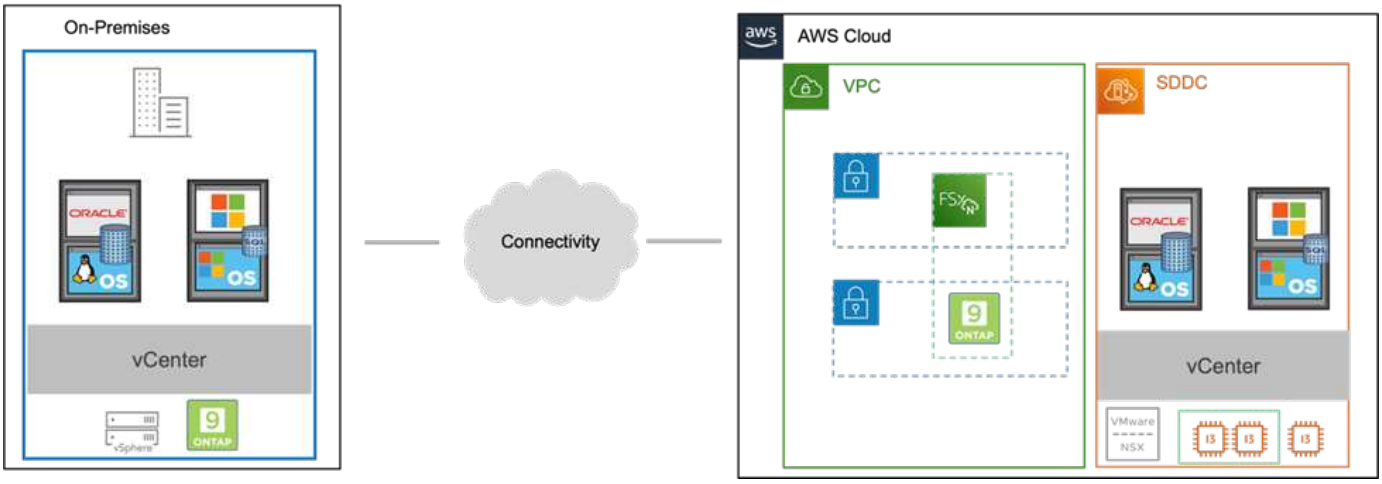
TR-4931: Recuperación ante desastres con VMware Cloud en Amazon Web Services y Guest Connect

Un entorno y un plan de recuperación ante desastres (DR) comprobados son fundamentales para que las organizaciones garanticen que las aplicaciones críticas para el negocio puedan restaurarse rápidamente en caso de una interrupción importante. Esta solución se centra en demostrar casos de uso de DR con un enfoque en tecnologías VMware y NetApp , tanto locales como con VMware Cloud en AWS.

Descripción general

NetApp tiene una larga trayectoria de integración con VMware como lo demuestran las decenas de miles de clientes que han elegido a NetApp como su socio de almacenamiento para su entorno virtualizado. Esta integración continúa con opciones conectadas por invitados en la nube y también con integraciones recientes con almacenes de datos NFS. Esta solución se centra en el caso de uso comúnmente conocido como almacenamiento conectado por invitado.

En el almacenamiento conectado a invitados, el VMDK invitado se implementa en un almacén de datos aprovisionado por VMware y los datos de la aplicación se alojan en iSCSI o NFS y se asignan directamente a la VM. Se utilizan aplicaciones Oracle y MS SQL para demostrar un escenario de DR, como se muestra en la siguiente figura.



Supuestos, prerrequisitos y descripción general de los componentes

Antes de implementar esta solución, revise la descripción general de los componentes, los requisitos previos necesarios para implementar la solución y las suposiciones realizadas al documentar esta solución.

"Requisitos, prerrequisitos y planificación de la solución DR"

Realizar recuperación ante desastres con SnapCenter

En esta solución, SnapCenter proporciona instantáneas consistentes 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 clúster local AFF y FSx ONTAP . Además, Veeam Backup & Replication proporciona capacidades de respaldo y restauración para nuestras máquinas virtuales.

En esta sección, cubrimos la configuración de SnapCenter, SnapMirror y Veeam tanto para la copia de seguridad como para la restauración.

Las siguientes secciones cubren 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 dentro del sistema de almacenamiento principal (principal > espejo) y en sistemas de almacenamiento secundario (principal > bóveda) con el propósito de archivado y retención 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 destino deben estar en redes interconectadas mediante el emparejamiento de Amazon VPC, una puerta de enlace de tránsito, AWS Direct Connect o una VPN de AWS.

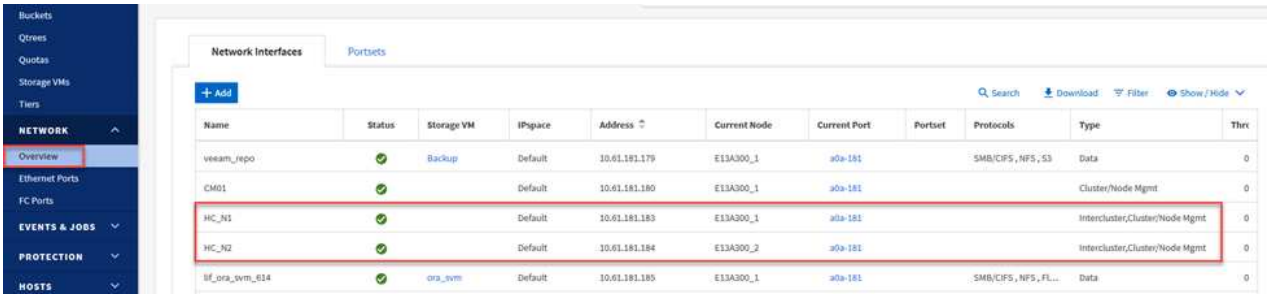
Los siguientes pasos son necesarios para configurar las relaciones de SnapMirror entre un sistema ONTAP local y FSx ONTAP:

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

Registrar las interfaces lógicas entre clústeres de origen y destino

Para el sistema ONTAP de origen que reside localmente, puede recuperar la información LIF entre clústeres desde el Administrador del sistema o desde la CLI.

1. En ONTAP System Manager, navegue a la página Descripción general de la red y recupere las direcciones IP del tipo: entre clústeres que están configuradas para comunicarse con la VPC de AWS donde está instalado FSx.



2. Para recuperar las direcciones IP entre 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.
```

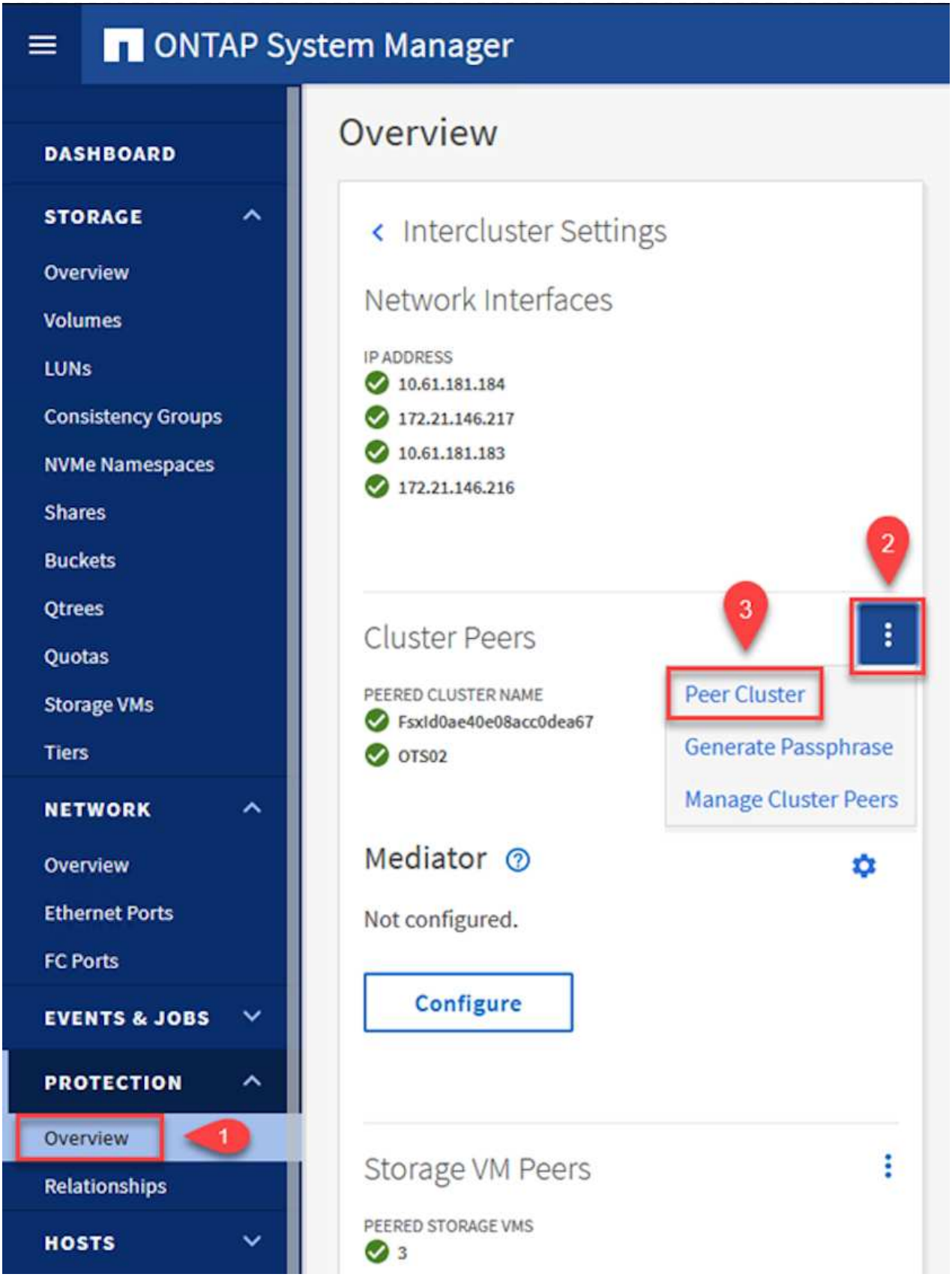
Establecer peering de clúster entre ONTAP y FSx

Para establecer intercambio de clústeres entre clústeres ONTAP , se debe confirmar en el otro clúster par una frase de contraseña única ingresada en el clúster ONTAP iniciador.

1. Configure el peering en el clúster FSx de destino mediante el `cluster peer create` dominio. Cuando se le solicite, ingrese una frase de contraseña única que se utilizará 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 pares del clúster mediante ONTAP System Manager o la CLI. Desde el Administrador del sistema ONTAP , navegue a Protección > Descripción general y seleccione Clúster de pares.

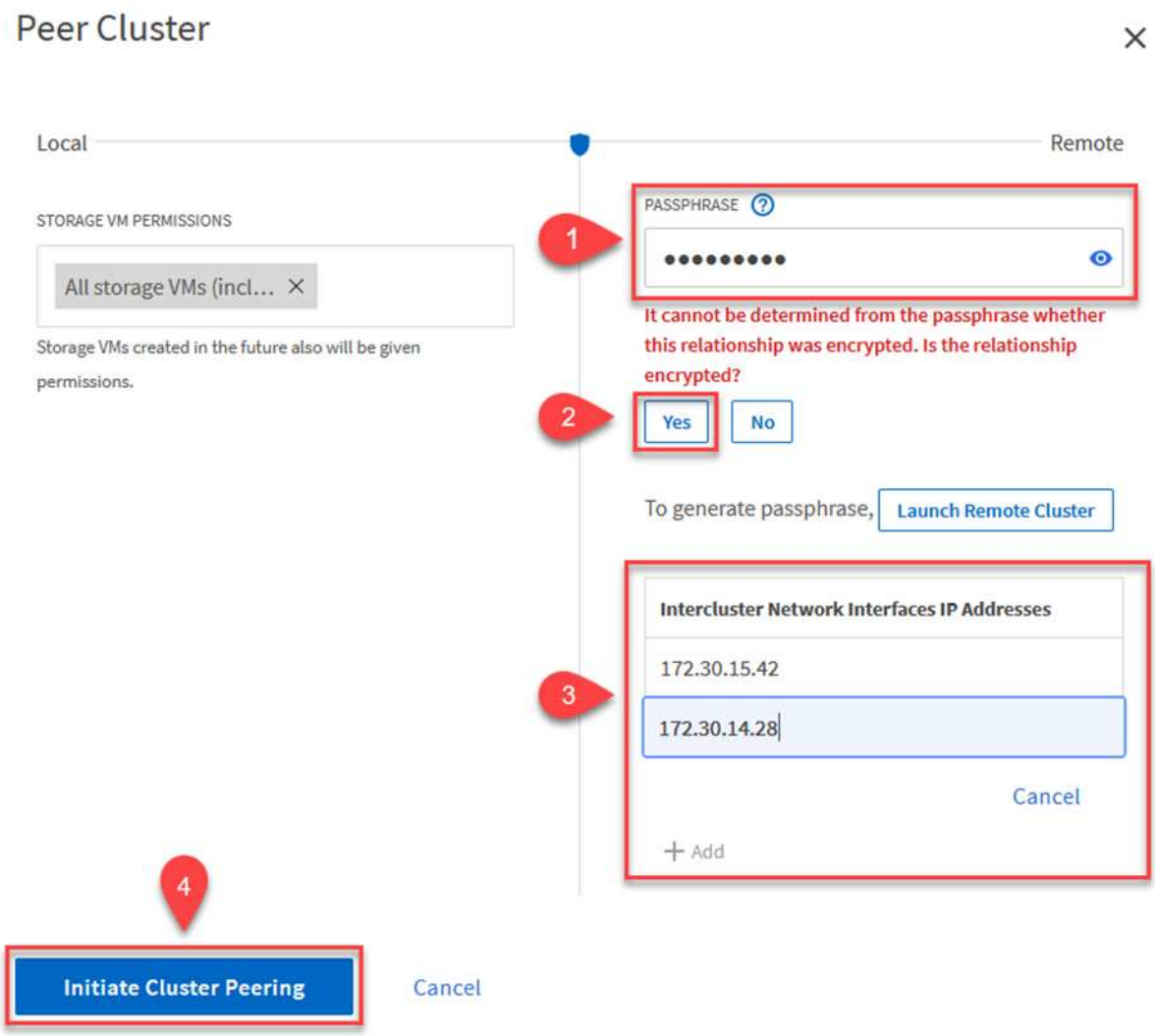


3. En el cuadro de diálogo Clúster de pares, complete la información requerida:
   a. Ingrese la frase de contraseña que se utilizó para establecer la relación de clúster de pares en el clúster FSx de destino.

b. Seleccionar `Yes` para establecer una relación encriptada.

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

d. Haga clic en Iniciar peering de clúster para finalizar el proceso.



4. Verifique el estado de la relación de pares 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
```

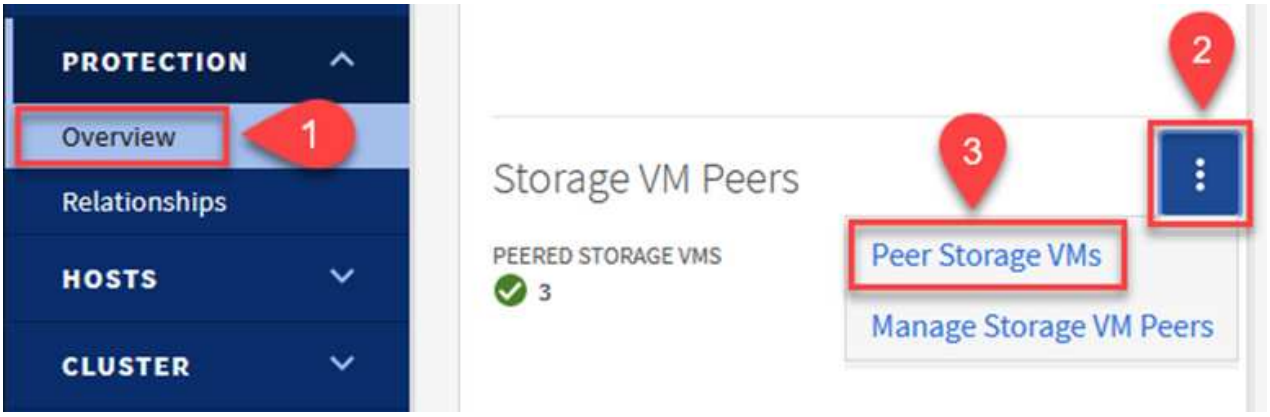
Establecer una relación de peering de SVM

El siguiente paso es configurar una relación SVM entre las máquinas virtuales de almacenamiento de origen y destino que contienen los volúmenes que estarán en las relaciones de SnapMirror .

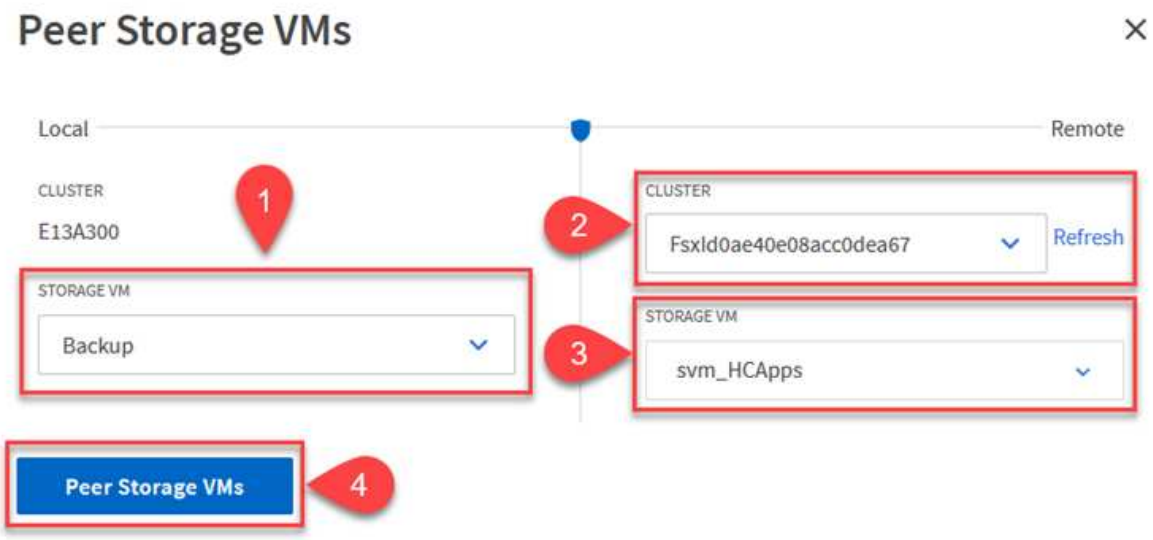
1. Desde el clúster FSx de origen, utilice el siguiente comando desde la CLI para crear la relación de pares SVM:

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

2. Desde el clúster ONTAP de origen, acepte la relación de emparejamiento con ONTAP System Manager o la CLI.
3. Desde el Administrador del sistema ONTAP , vaya a Protección > Descripción general y seleccione Máquinas virtuales de almacenamiento de pares en Pares de máquinas virtuales de almacenamiento.



4. En el cuadro de diálogo de la máquina virtual de almacenamiento de pares, complete los campos obligatorios:
   - 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 peering SVM.

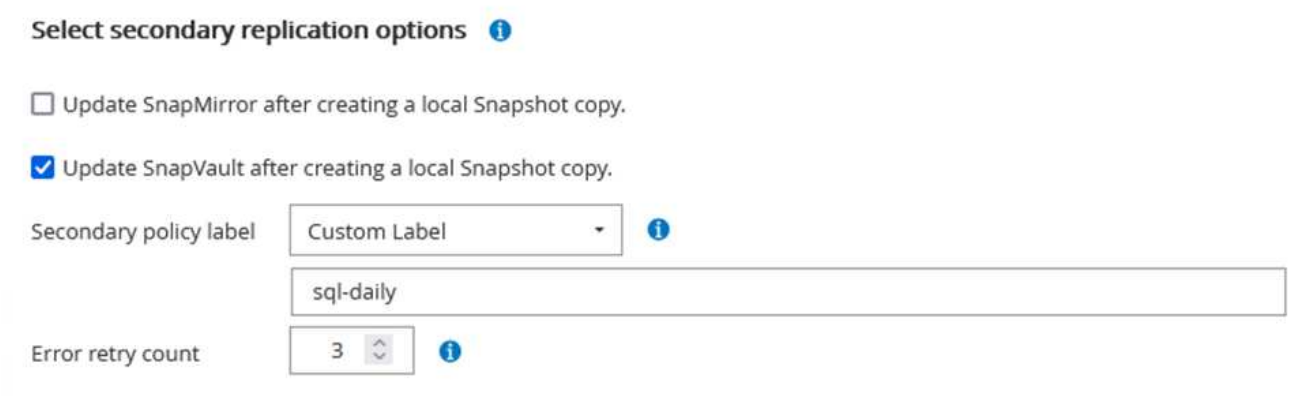
Crear una política de retención de instantáneas

SnapCenter administra los programas de retención de las copias de seguridad que existen como copias instantáneas en el sistema de almacenamiento principal. Esto se establece al crear una política en SnapCenter. SnapCenter no administra políticas de retención para copias de seguridad que se conservan en sistemas de almacenamiento secundario. Estas políticas se administran por separado a través de una política SnapMirror creada en el clúster FSx secundario y asociada con los volúmenes de destino que están en una relación SnapMirror con el volumen de origen.

Al crear una política de SnapCenter , tiene la opción de especificar una etiqueta de política secundaria que se agrega a la etiqueta SnapMirror de cada instantánea generada cuando se realiza una copia de seguridad de SnapCenter .

> En el almacenamiento secundario, estas etiquetas coinciden con las reglas de políticas asociadas con el volumen de destino con el fin de garantizar la retención de instantáneas.

El siguiente ejemplo muestra una etiqueta SnapMirror que está presente en todas las instantáneas generadas como parte de una política utilizada para las copias de seguridad diarias de nuestra base de datos de SQL Server y los volúmenes de registro.



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

Primero debe crear una política SnapMirror con reglas que dicten la cantidad de copias de instantáneas que se deben conservar.

1. Cree la política SnapMirror en el clúster FSx.

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

2. Agregue 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 proporciona un ejemplo de una regla que podría agregarse a una política:

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

Cree reglas adicionales para cada etiqueta de SnapMirror y la cantidad de instantáneas que se conservarán (período de retención).

Crear volúmenes de destino

Para crear un volumen de destino en FSx que será el destinatario de copias instantáneas 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
```

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

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

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

Inicializar las relaciones de SnapMirror

Inicializar la relación SnapMirror . Este proceso inicia una nueva instantánea generada desde el volumen de origen y la copia al volumen de destino.

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

Implementar y configurar el servidor Windows SnapCenter en las instalaciones.

Implementar Windows SnapCenter Server en las instalaciones

Esta solución utiliza NetApp SnapCenter para realizar copias de seguridad consistentes con las aplicaciones de bases de datos de SQL Server y Oracle. Junto con Veeam Backup & Replication para realizar copias de seguridad de los VMDK de máquinas virtuales, esto proporciona una solución integral de recuperación ante desastres para centros de datos locales y basados en la nube.

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

El SnapCenter software se puede obtener en "este enlace" .

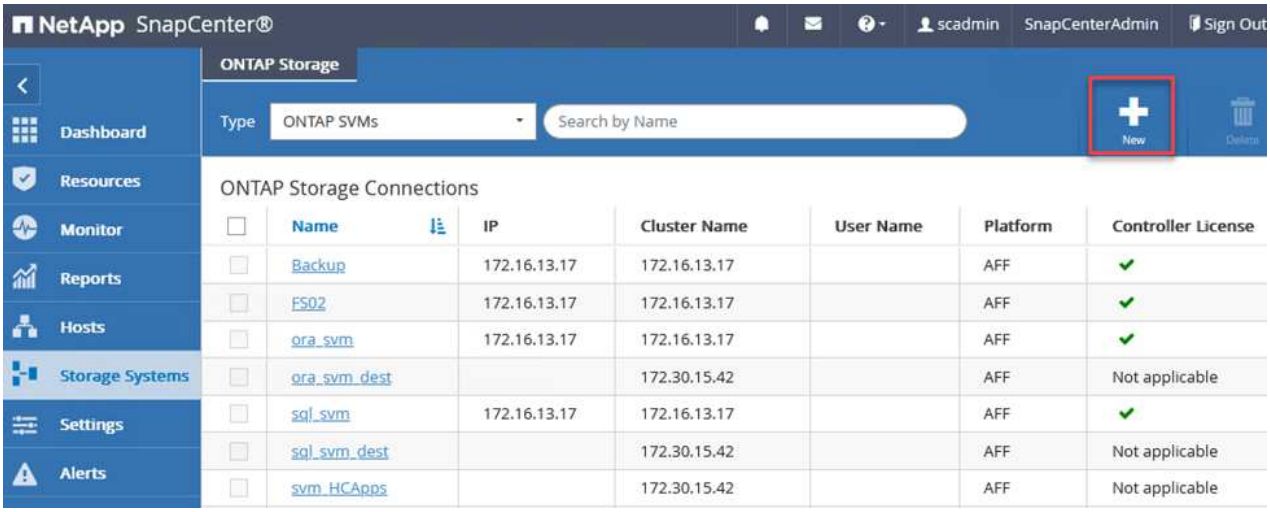
Una vez instalado, puede acceder a la consola de SnapCenter desde un navegador web usando *https://Virtual_Cluster_IP_or_FQDN:8146*.

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

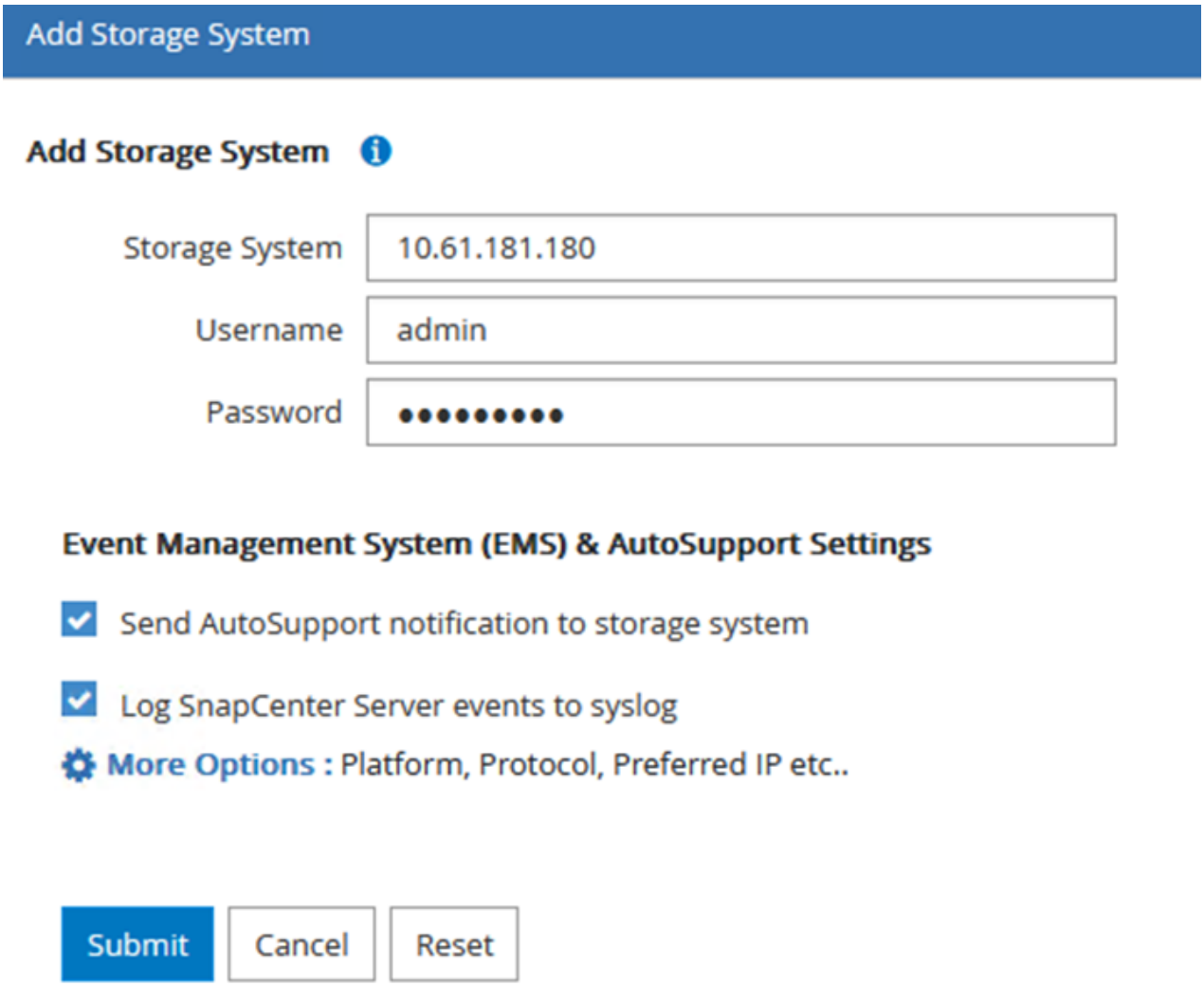
Agregar controladores de almacenamiento a SnapCenter

Para agregar controladores de almacenamiento a SnapCenter, complete los siguientes pasos:

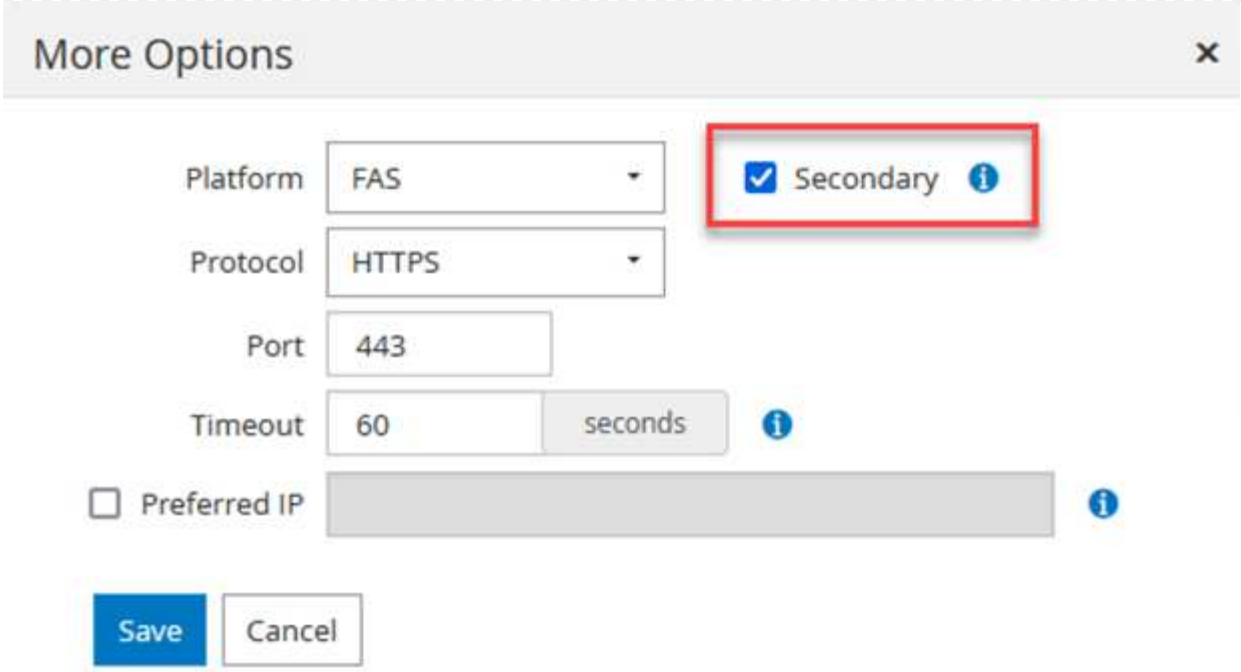
1. En el menú de la izquierda, seleccione Sistemas de almacenamiento y luego haga clic en Nuevo para comenzar el proceso de agregar sus controladores de almacenamiento a SnapCenter.



2. En el cuadro de diálogo Agregar sistema de almacenamiento, agregue la dirección IP de administración para el clúster ONTAP local y el nombre de usuario y la contraseña. Luego haga clic en Enviar para comenzar 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 Agregar sistema de almacenamiento y haga clic en la casilla de verificación Secundario para designar el sistema FSx como el sistema de almacenamiento secundario actualizado con copias de SnapMirror o nuestras instantáneas de respaldo principales.

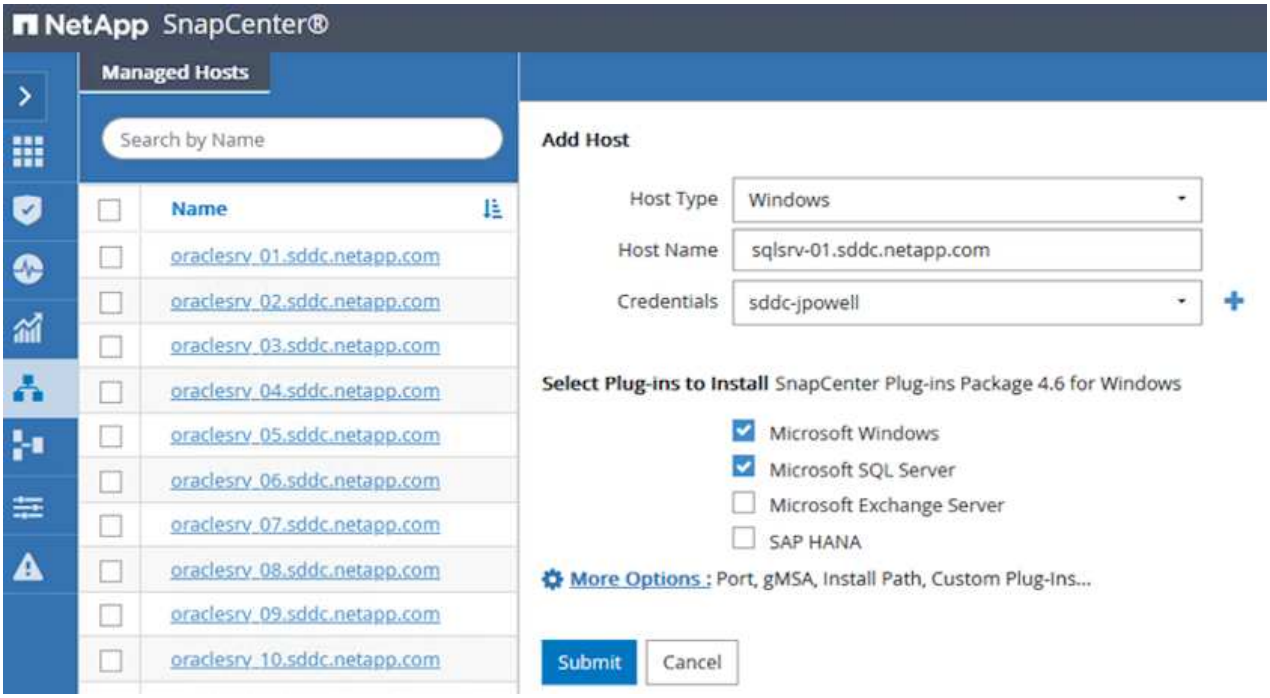


Para obtener más información relacionada con la adición de sistemas de almacenamiento a SnapCenter, consulte la documentación en "este enlace" .

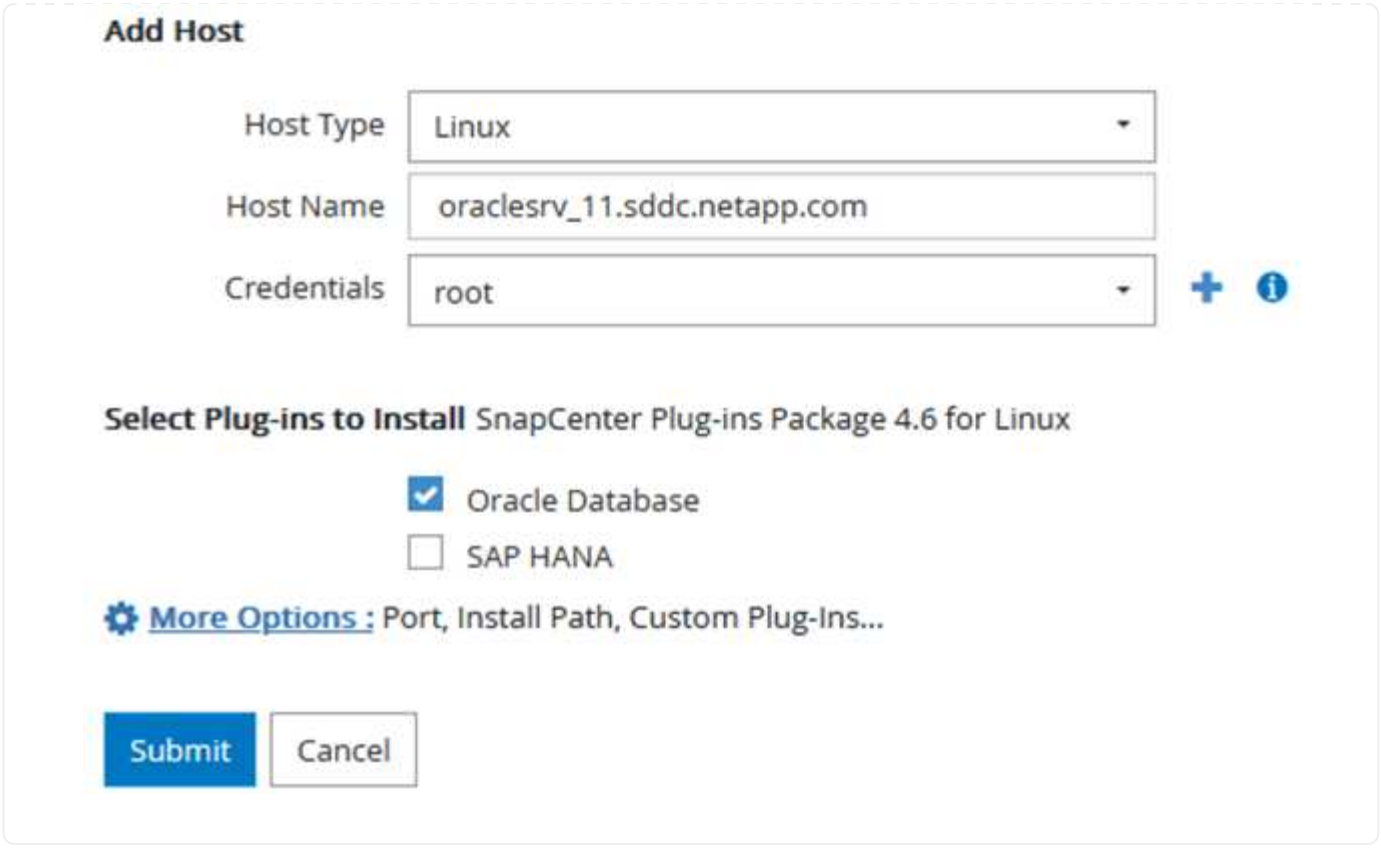
Agregar hosts a SnapCenter

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 luego haga clic en Agregar para comenzar el proceso de agregar controladores de almacenamiento a SnapCenter.
2. En la ventana Agregar hosts, agregue el tipo de host, el nombre de host y las credenciales del sistema host. Seleccione el tipo de complemento. Para SQL Server, seleccione el complemento Microsoft Windows y Microsoft SQL Server.



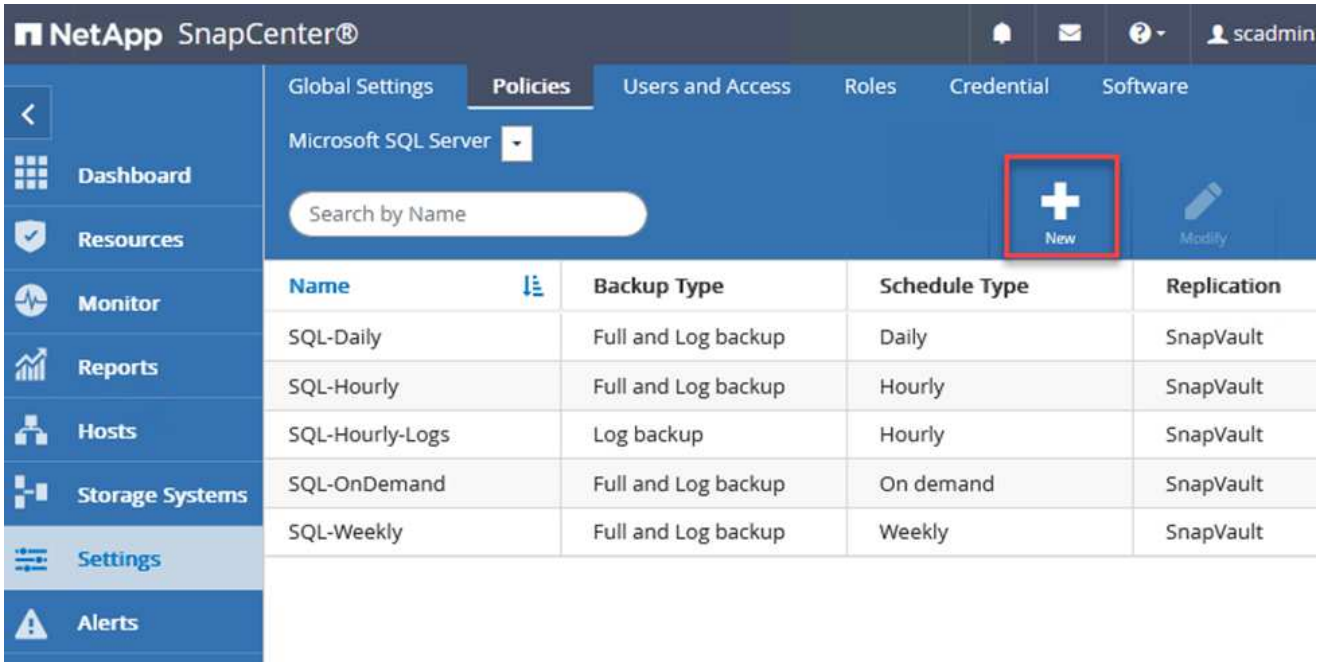
3. Para Oracle, complete los campos obligatorios en el cuadro de diálogo Agregar host y marque la casilla del complemento de Oracle Database. A continuación, haga clic en Enviar para iniciar el proceso de descubrimiento y agregar el host a SnapCenter.


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 un trabajo de respaldo. Incluyen, entre otros, la programación de copias de seguridad, el tipo de replicación y cómo SnapCenter maneja la realización de copias de seguridad y el truncamiento de los registros de transacciones.

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



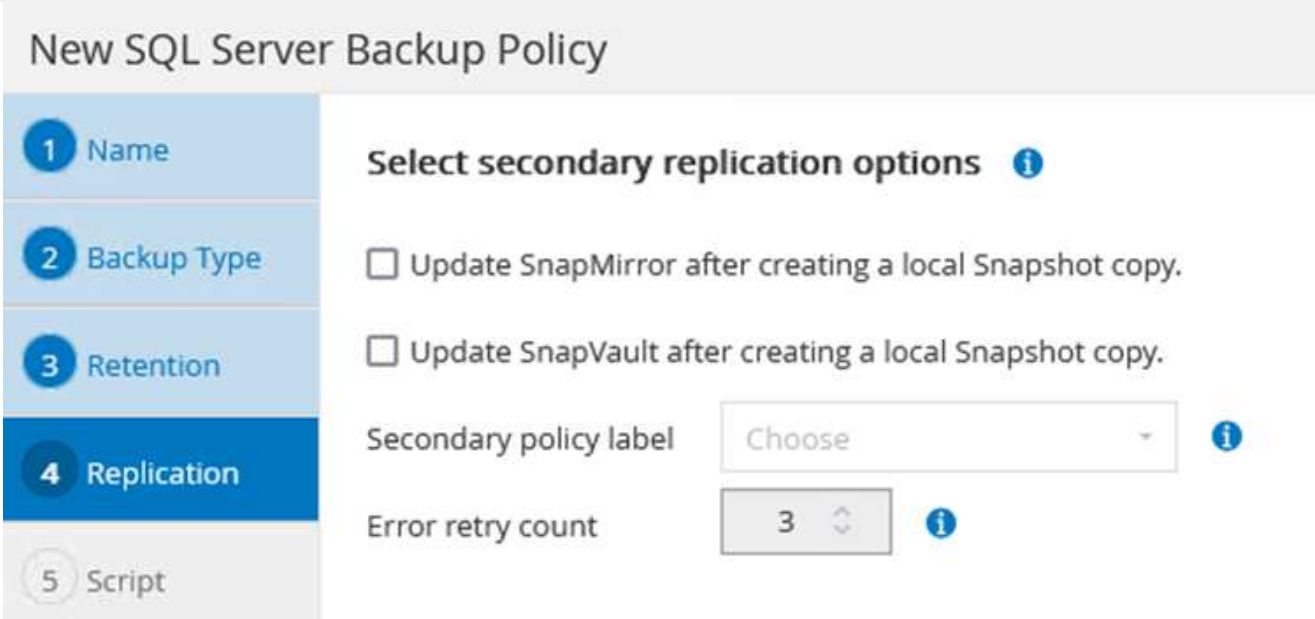
Para obtener información completa sobre la creación de políticas para copias de seguridad de SQL Server, consulte la "Documentación de SnapCenter" .

Para obtener información completa sobre la creación de políticas para copias de seguridad de Oracle, consulte la "Documentación de SnapCenter" .

Notas:

- A medida que avanza en el asistente de creación de políticas, preste especial atención a la sección Replicación. En esta sección usted estipula los tipos de copias secundarias de SnapMirror que desea que se tomen durante el proceso de copias de seguridad.
- La configuración "Actualizar SnapMirror después de crear una copia de instantánea local" se refiere 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 configuración "Actualizar SnapVault después de crear una copia SnapShot local" se utiliza para actualizar una relación SnapMirror que existe entre dos clústeres separados y entre un sistema ONTAP local y Cloud Volumes ONTAP o FSx ONTAP.

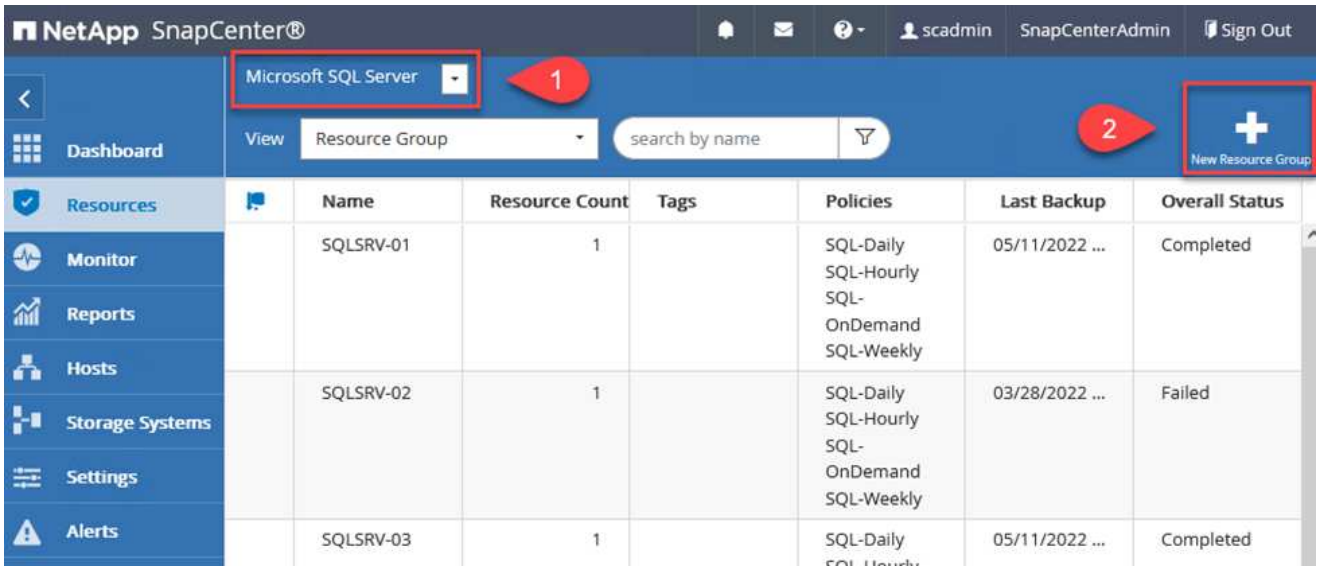
La siguiente imagen muestra las opciones anteriores y cómo se ven en el asistente de política de respaldo.



Crear grupos de recursos de SnapCenter

Los grupos de recursos le permiten seleccionar los recursos de base de datos que desea incluir en sus copias de seguridad y las políticas seguidas para esos recursos.

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



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

Para realizar una copia de seguridad de los recursos de SQL, siga "este enlace" .

Para realizar copias de seguridad de los recursos de Oracle, siga "este enlace" .

Implementar y configurar Veeam Backup Server

El software Veeam Backup & Replication se utiliza en la solución para realizar copias de seguridad de nuestras máquinas virtuales de aplicaciones y archivar una copia de las copias de seguridad en un depósito de Amazon S3 mediante un repositorio de copias de seguridad escalable de Veeam (SOBR). Veeam se implementa en un servidor Windows en esta solución. Para obtener orientación específica sobre la implementación de Veeam, consulte la "Centro de ayuda de Veeam Documentación técnica" .

Configurar el repositorio de copias de seguridad escalables de Veeam

Después de implementar y licenciar el software, puede crear un repositorio de respaldo escalable (SOBR) como almacenamiento de destino para trabajos de respaldo. También debe incluir un bucket S3 como respaldo de los datos de la máquina virtual fuera del sitio para la recuperación ante desastres.

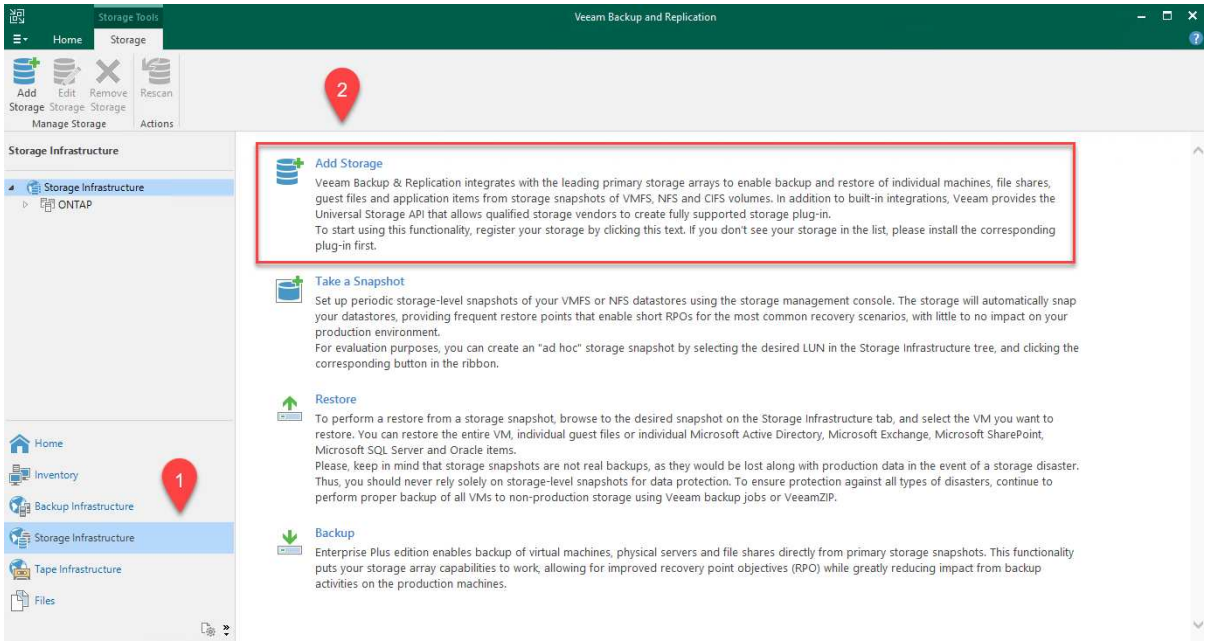
Consulte los siguientes requisitos previos antes de comenzar.

1. Cree un recurso compartido de archivos SMB en su sistema ONTAP local como almacenamiento de destino para las copias de seguridad.
2. Cree un bucket de Amazon S3 para incluirlo en SOBR. Este es un repositorio para las copias de seguridad externas.

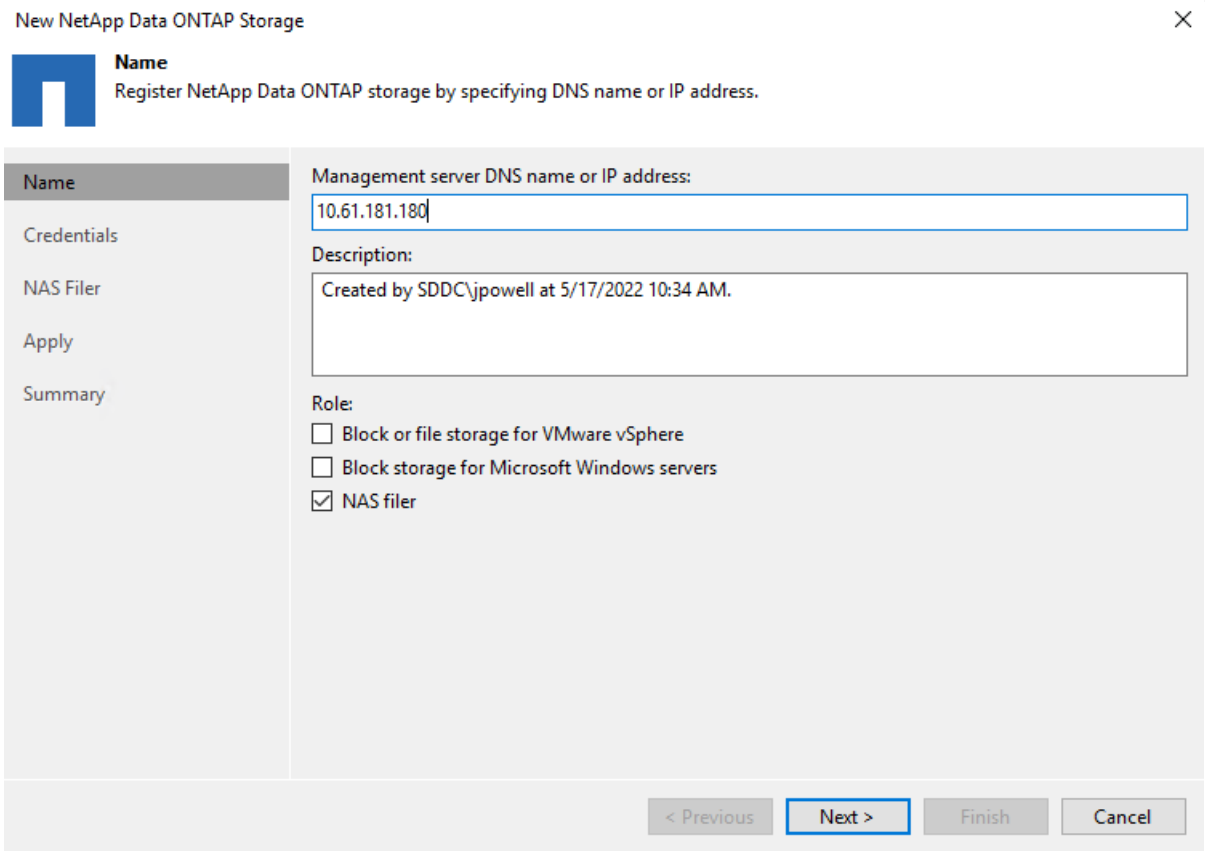
Agregue almacenamiento ONTAP a Veeam

Primero, agregue el clúster de almacenamiento ONTAP y el sistema de archivos SMB/NFS asociado como infraestructura de almacenamiento en Veeam.

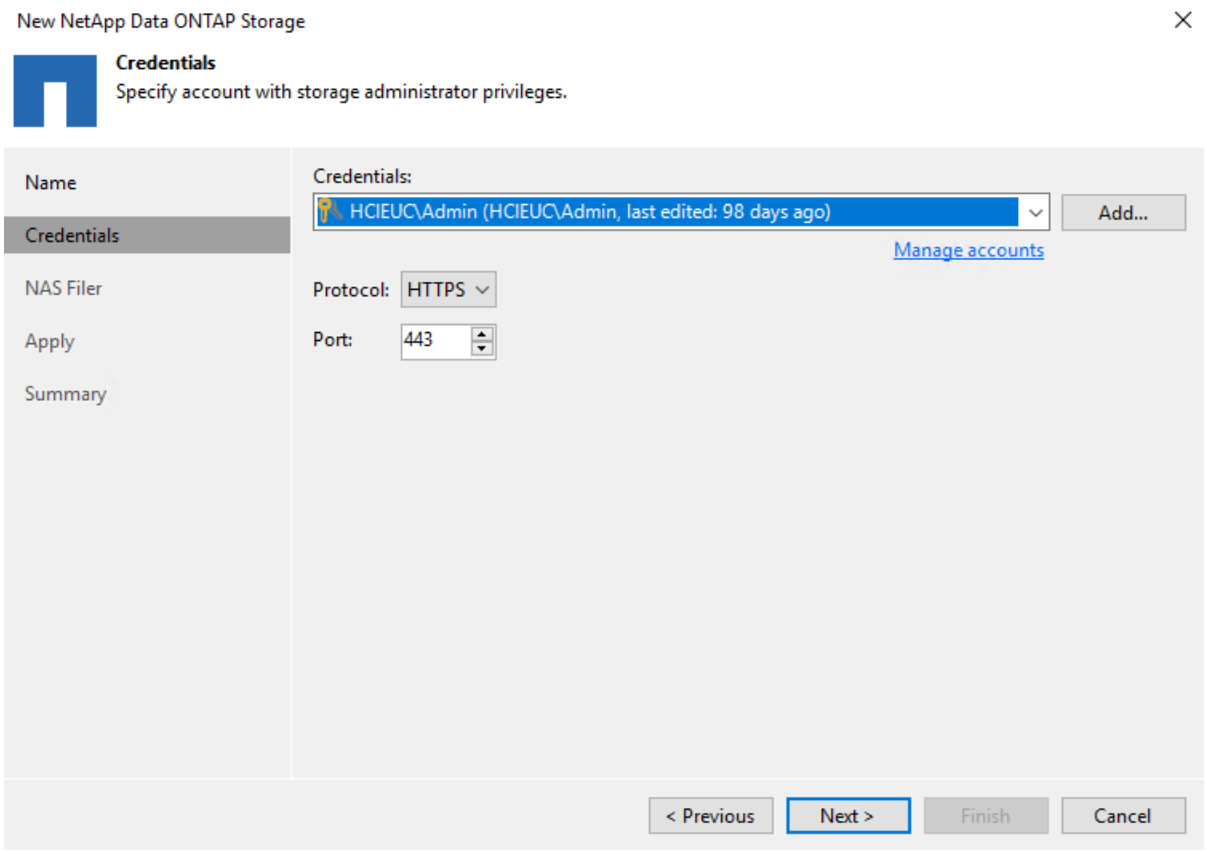
1. Abra la consola de Veeam e inicie sesión. Navegue hasta Infraestructura de almacenamiento y luego seleccione Agregar almacenamiento.



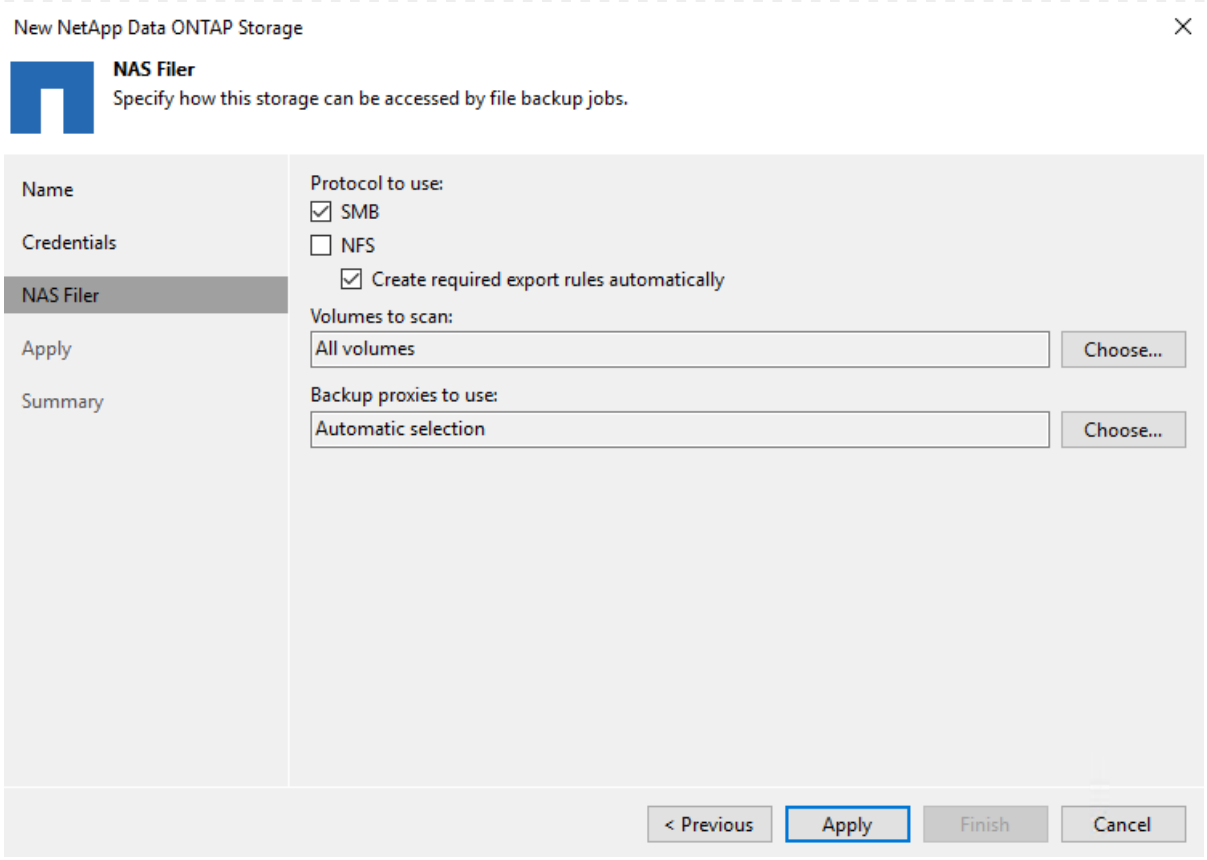
2. En el asistente Agregar almacenamiento, seleccione NetApp como proveedor de almacenamiento y luego seleccione Data ONTAP.
3. Introduzca la dirección IP de administración y marque la casilla NAS Filer. Haga clic en Siguiente.



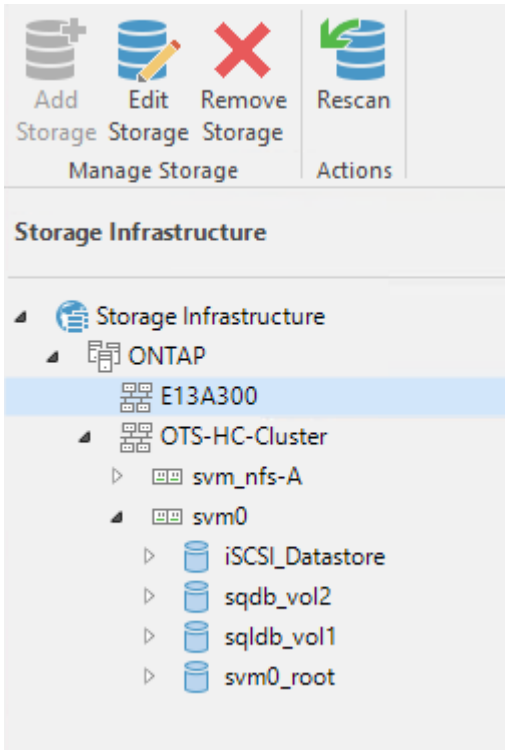
4. Agregue sus credenciales para acceder al clúster ONTAP .



5. En la página NAS Filer, seleccione los protocolos que desea escanear y seleccione Siguiente.

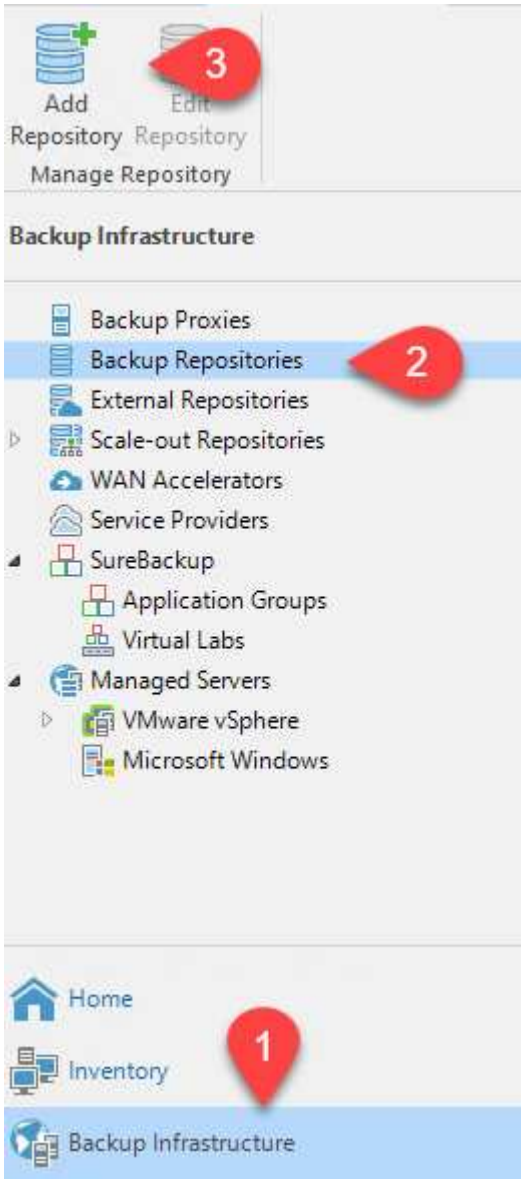


6. Complete las páginas Aplicar y Resumen del asistente y haga clic en Finalizar para comenzar el proceso de descubrimiento de almacenamiento. Una vez finalizado el escaneo, se agrega el clúster ONTAP junto con los archivadores NAS como recursos disponibles.

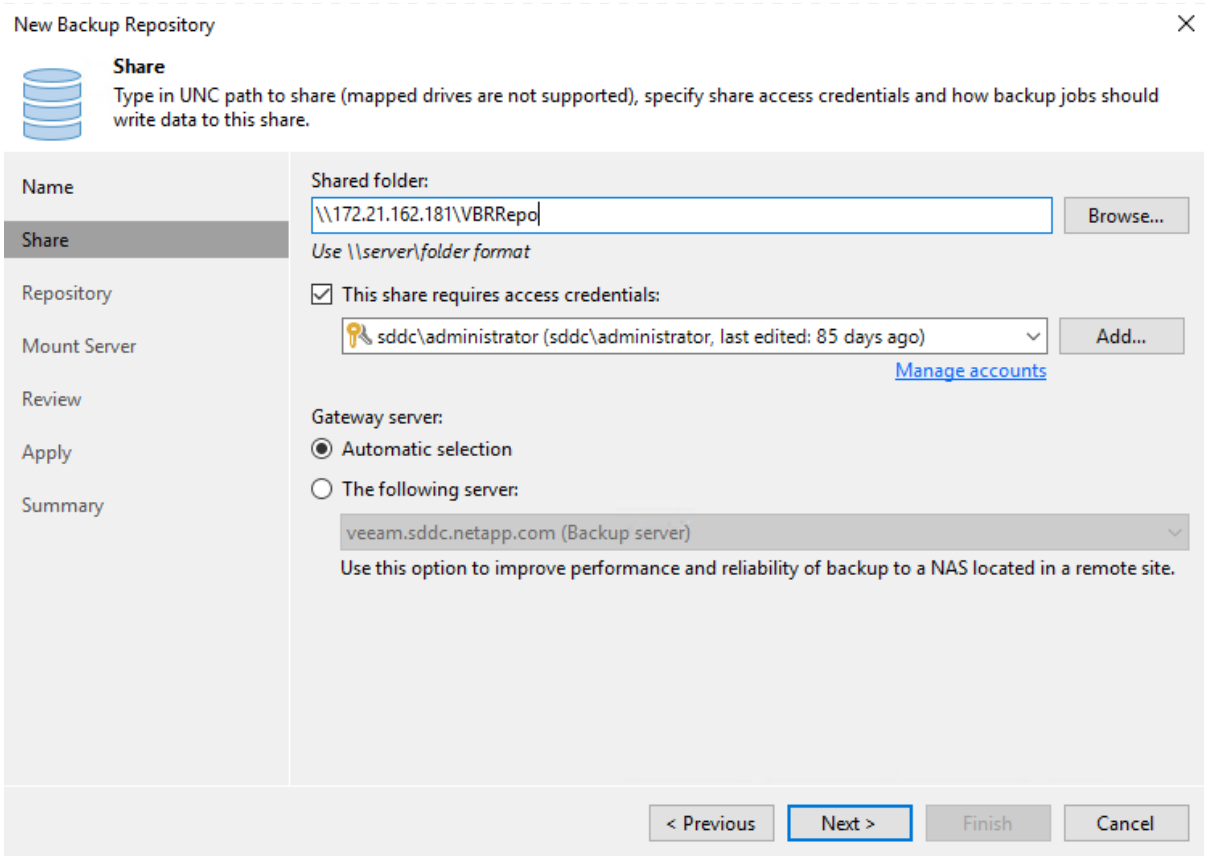


7. Cree un repositorio de respaldo utilizando los recursos compartidos NAS recién descubiertos. Desde Infraestructura de respaldo, seleccione Repositorios de respaldo y haga clic en el

elemento de menú Agregar repositorio.



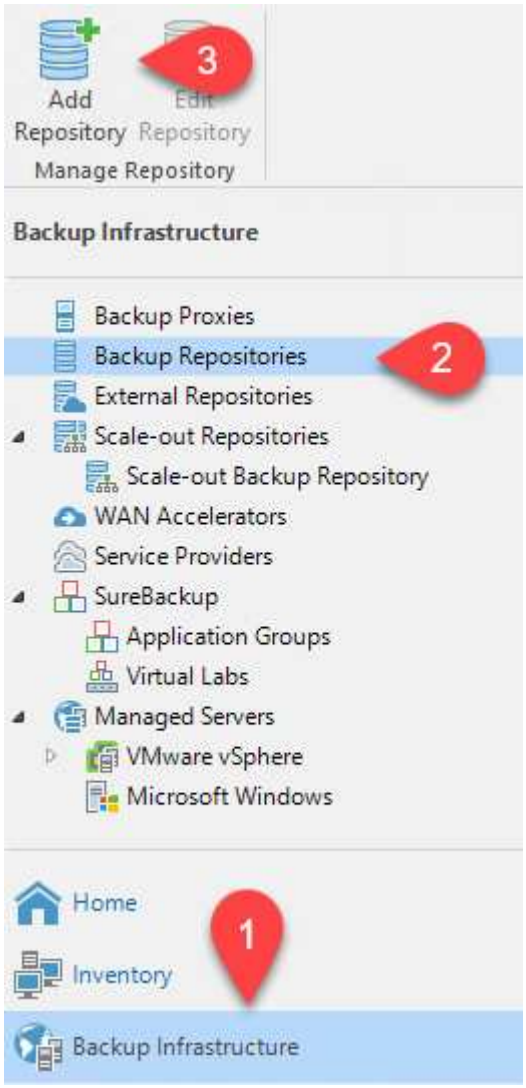
8. Siga todos los pasos del Asistente para nuevo repositorio de copia de seguridad para crear el repositorio. Para obtener información detallada sobre la creación de repositorios de Veeam Backup, consulte la "Documentación de Veeam" .


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

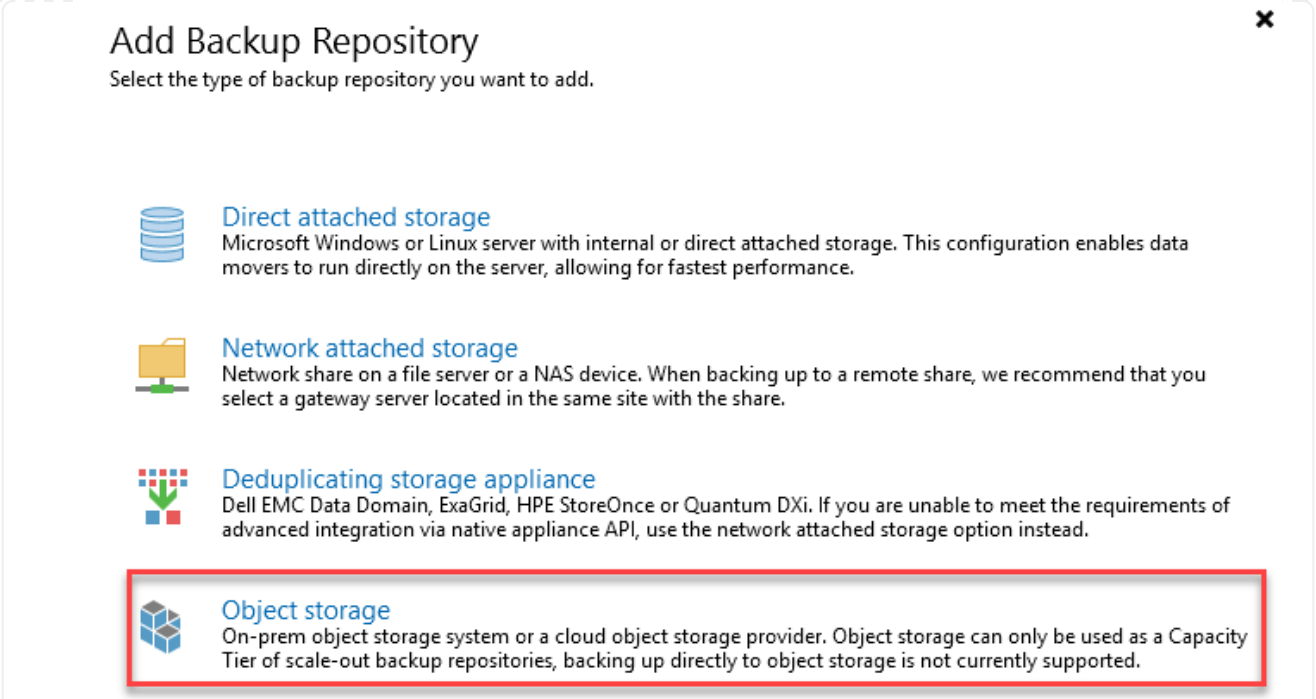
Agregue el bucket de Amazon S3 como repositorio de respaldo

El siguiente paso es agregar el almacenamiento de Amazon S3 como repositorio de respaldo.

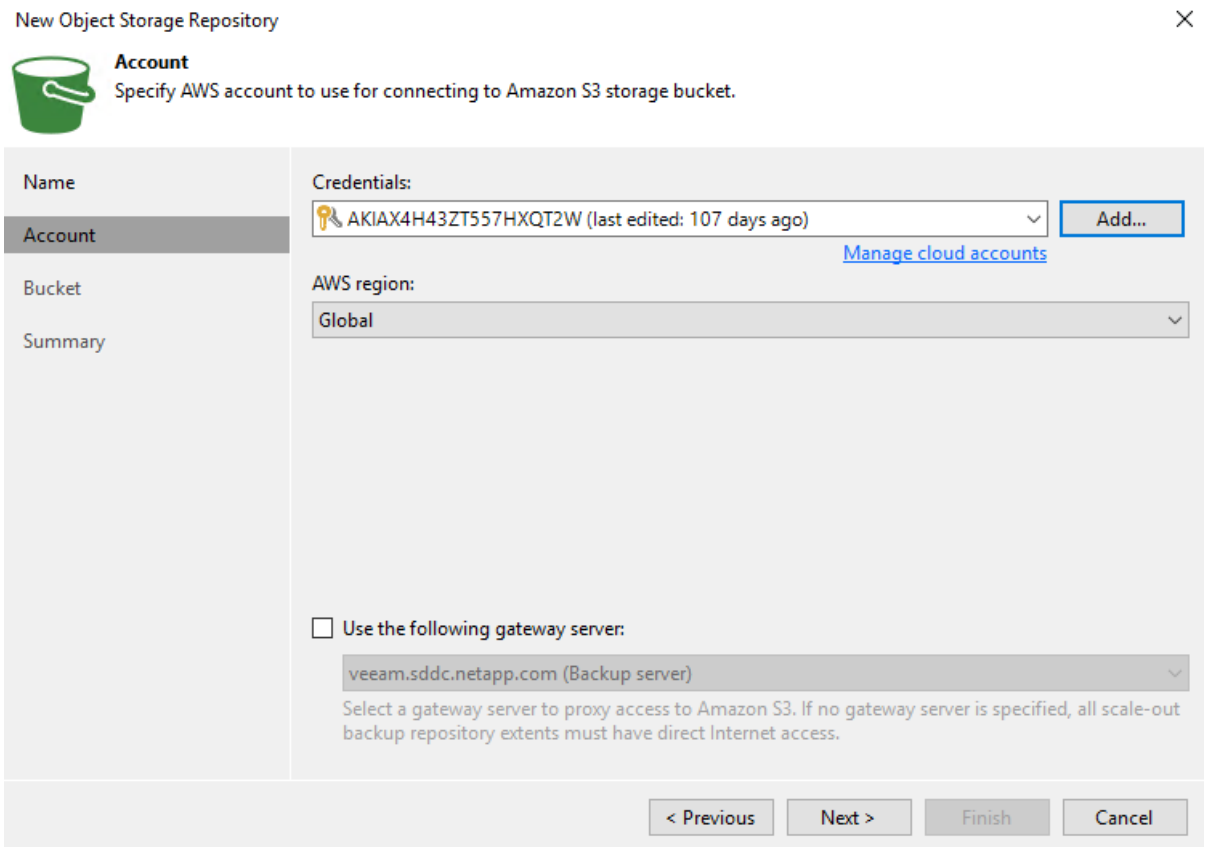
1. Vaya a Infraestructura de respaldo > Repositorios de respaldo. Haga clic en Agregar repositorio.



2. En el asistente Agregar repositorio de respaldo, seleccione Almacenamiento de objetos y luego Amazon S3. Esto inicia el asistente para crear nuevo repositorio de almacenamiento de objetos.



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

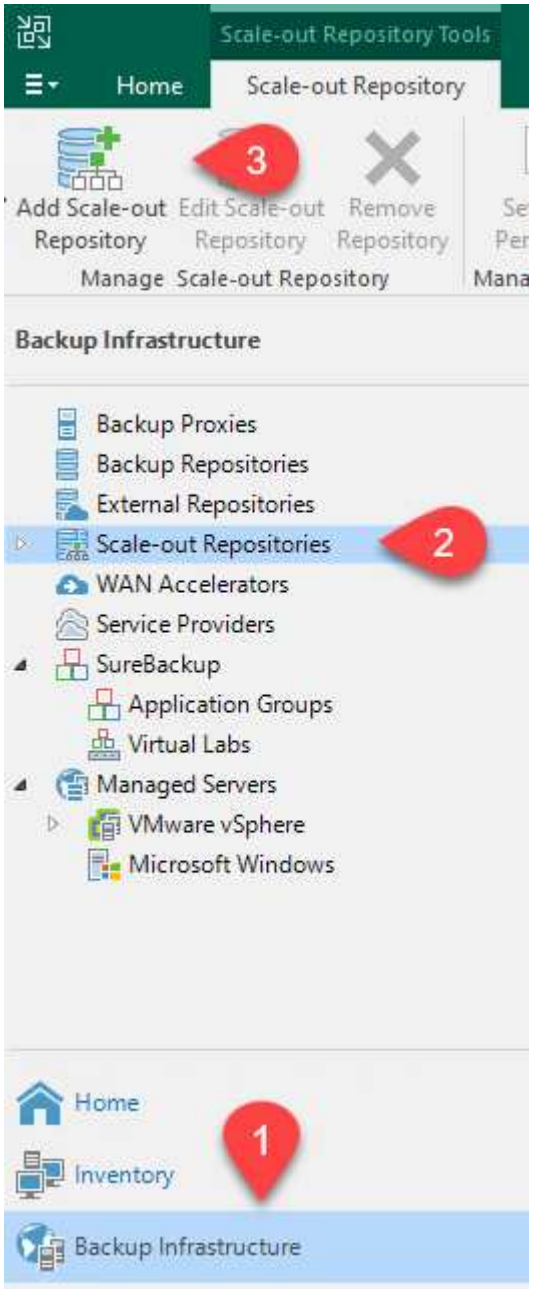


5. Después de que se cargue la configuración de Amazon, elija su centro de datos, depósito y carpeta y haga clic en Aplicar. Por último, haga clic en Finalizar para cerrar el asistente.

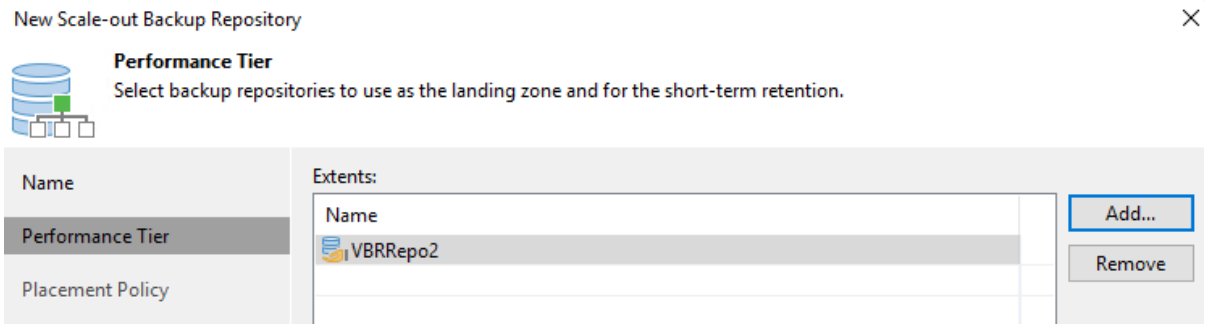
Crear un repositorio de respaldo escalable

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

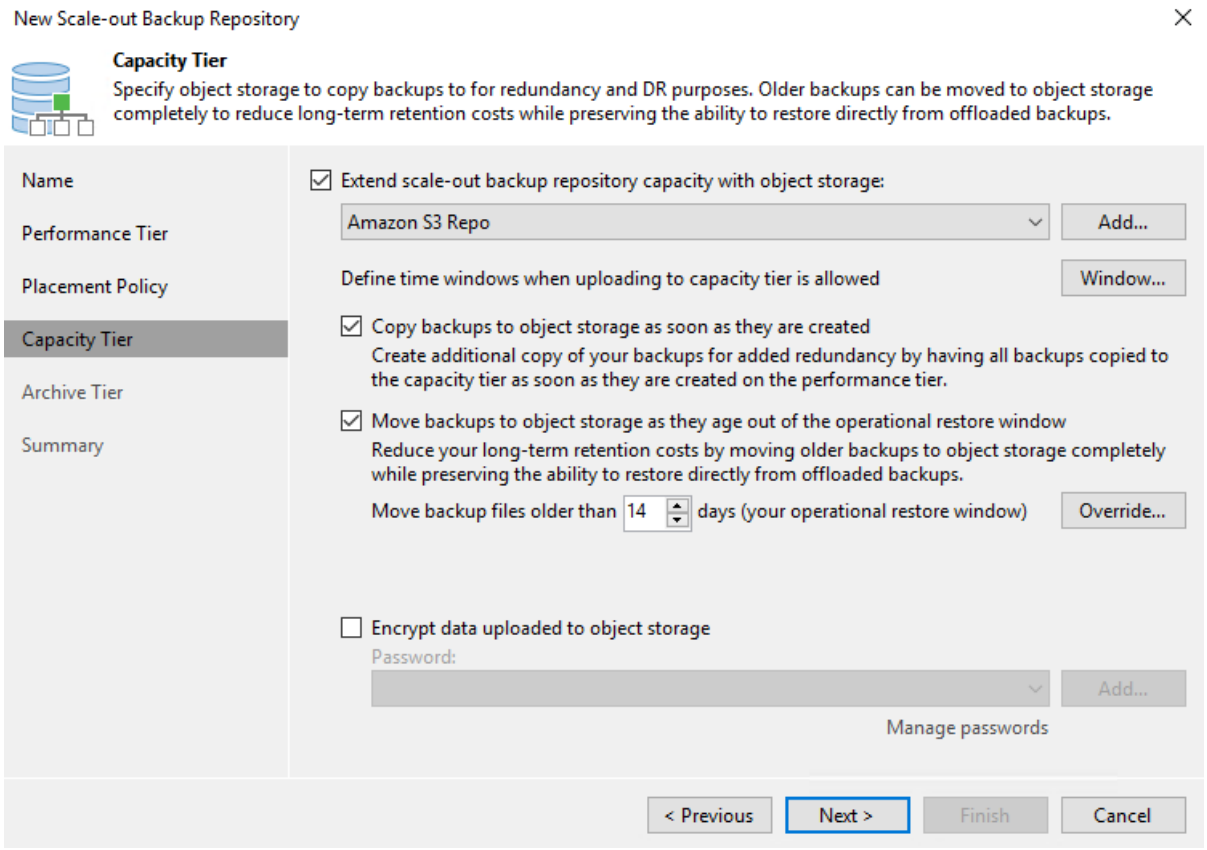
1. En Infraestructura de respaldo, seleccione Repositorios de escalamiento horizontal y luego haga clic en el elemento de menú Agregar repositorio de escalamiento horizontal.



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



4. Para la Política de ubicación, elija Localidad de datos o Rendimiento según sus requisitos. Seleccione siguiente.
5. Para Capacity Tier ampliamos SOBR con almacenamiento de objetos de Amazon S3. Para fines de recuperación ante desastres, seleccione Copiar copias de seguridad al almacenamiento de objetos tan pronto como se creen para garantizar la entrega oportuna de nuestras copias de seguridad secundarias.



6. Por último, seleccione Aplicar y Finalizar para finalizar la creación del SOBR.

Crear los trabajos del repositorio de respaldo de escalamiento horizontal

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

Herramientas y configuración de BlueXP backup and recovery

Para realizar una conmutación por error de las máquinas virtuales de la aplicación y los volúmenes de bases de datos a los servicios de VMware Cloud Volume que se ejecutan en AWS, debe instalar y configurar una instancia en ejecución de SnapCenter Server y Veeam Backup and Replication Server. Una vez completada la conmutación por error, también debe configurar estas herramientas para reanudar las operaciones de respaldo normales hasta que se planifique y ejecute una conmutación por error al centro de datos local.

Implementar un servidor secundario de Windows SnapCenter

SnapCenter Server se implementa en VMware Cloud SDDC o se instala en una instancia EC2 que reside en una VPC con conectividad de red al entorno de VMware Cloud.

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

Puede encontrar el SnapCenter software en "este enlace" .

Configurar el servidor secundario de Windows SnapCenter

Para realizar una restauración de los datos de la 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 las máquinas virtuales y las copias de seguridad de las aplicaciones pueden reanudarse utilizando FSx ONTAP como almacenamiento principal.

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

1. Configure el nombre de la computadora para que sea idéntico al servidor SnapCenter local original.
2. Configurar la red para comunicarse con VMware Cloud y la instancia de FSx ONTAP .
3. Complete el procedimiento para restaurar la base de datos de SnapCenter .
4. Confirme que SnapCenter esté en modo de recuperación ante desastres para asegurarse de que FSx sea ahora el almacenamiento principal para las copias de seguridad.
5. Confirme que se restablezca la comunicación con las máquinas virtuales restauradas.

Implementar un servidor secundario de Veeam Backup & Replication

Puede instalar el servidor Veeam Backup & Replication en un servidor Windows en VMware Cloud on AWS o en una instancia EC2. Para obtener una guía de implementación detallada, consulte la "Documentación técnica del Centro de ayuda de Veeam" .

Configurar el servidor secundario de Veeam Backup & Replication

Para realizar una restauración de máquinas virtuales que se han respaldado en el almacenamiento de Amazon S3, debe instalar Veeam Server en un servidor Windows y configurarlo para que se comunique con VMware Cloud, FSx ONTAP y el depósito S3 que contiene el repositorio de respaldo original. También debe tener un nuevo repositorio de respaldo configurado en FSx ONTAP para realizar nuevas copias de seguridad de las máquinas virtuales después de que se restauren.

Para realizar este proceso se deben completar los siguientes elementos:

1. Configure la red para comunicarse con VMware Cloud, FSx ONTAP y el depósito S3 que contiene el repositorio de respaldo original.
2. Configure un recurso compartido SMB en FSx ONTAP para que sea un nuevo repositorio de respaldo.
3. Monte el depósito S3 original que se utilizó como parte del repositorio de respaldo de escalamiento horizontal en las instalaciones.
4. Después de restaurar la máquina virtual, establezca nuevos trabajos de respaldo para proteger las máquinas virtuales SQL y Oracle.

Para obtener más información sobre cómo restaurar máquinas virtuales con Veeam, consulte la sección"Restaurar máquinas virtuales de aplicaciones con Veeam Full Restore" .

Copia de seguridad de la base de datos de SnapCenter para recuperación ante desastres

SnapCenter permite la copia de seguridad y la recuperación de su base de datos MySQL subyacente y de sus datos de configuración 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 AWS EC2 que reside en nuestra VPC. Para obtener más información sobre la recuperación ante desastres de SnapCenter, consulte "este enlace" .

Requisitos previos para la copia de seguridad de SnapCenter

Se requieren los siguientes requisitos previos para realizar la copia de seguridad de SnapCenter :

- Un volumen y un recurso compartido SMB creados en el sistema ONTAP local para ubicar la base de datos respaldada y los archivos de configuración.
- Una relación SnapMirror entre el sistema ONTAP local y FSx o CVO en la cuenta de AWS. Esta relación se utiliza para transportar la instantánea que contiene la base de datos de SnapCenter respaldada y los archivos de configuración.
- Windows Server instalado en la cuenta en la nube, ya sea en una instancia EC2 o en una VM en VMware Cloud SDDC.
- SnapCenter instalado en la instancia EC2 de Windows o en la máquina virtual en VMware Cloud.

Resumen del proceso de copia de seguridad y restauración de SnapCenter

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

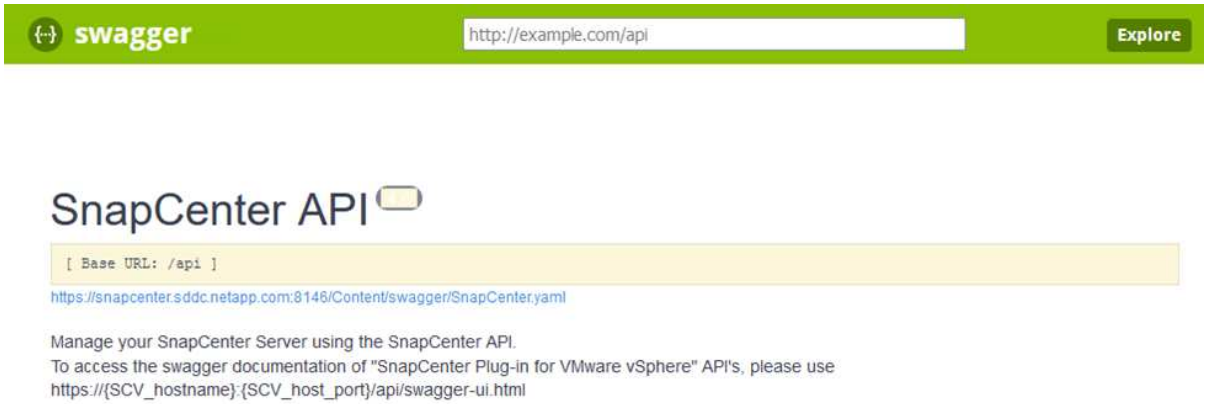
Realice una copia de seguridad de la base de datos y la configuración de SnapCenter

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

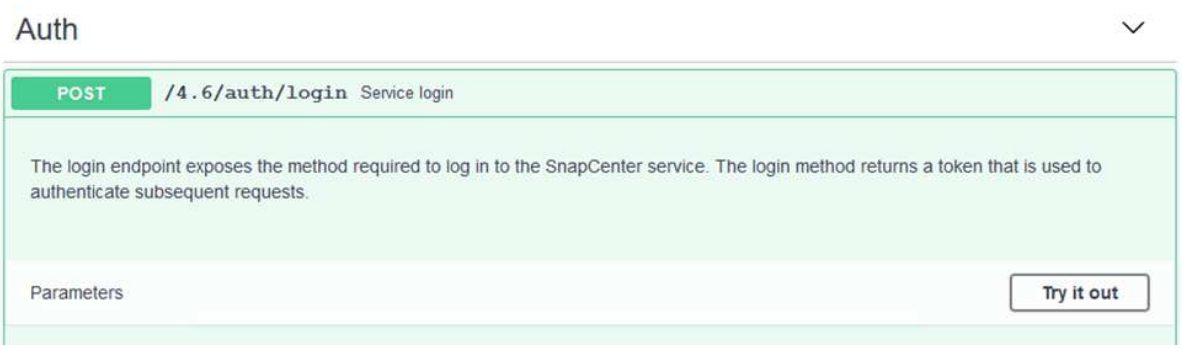
Inicie sesión en Swagger y obtenga el token de autorización

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

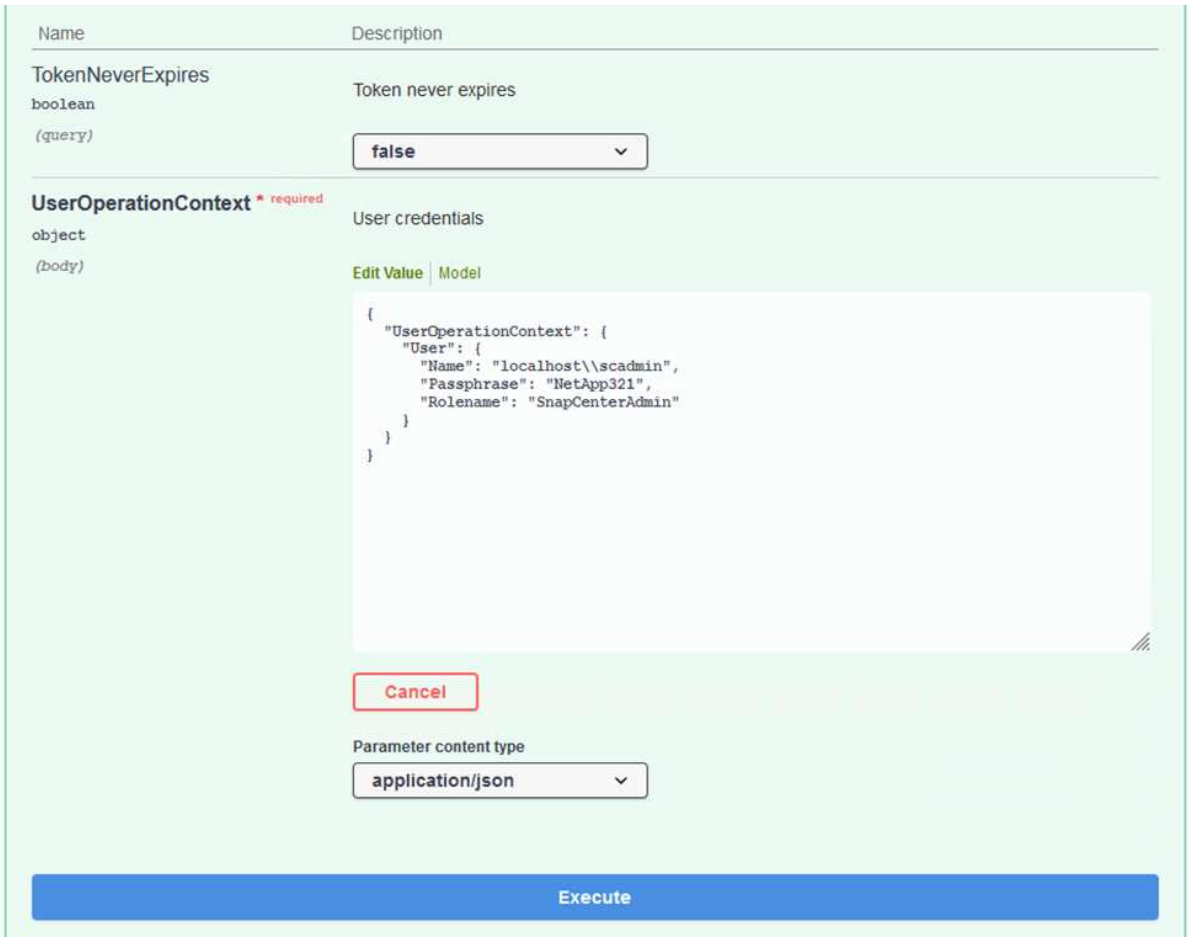
1. Acceda a la página web de la API Swagger de SnapCenter en *https://< IP del servidor SnapCenter >:8146/swagger/*.



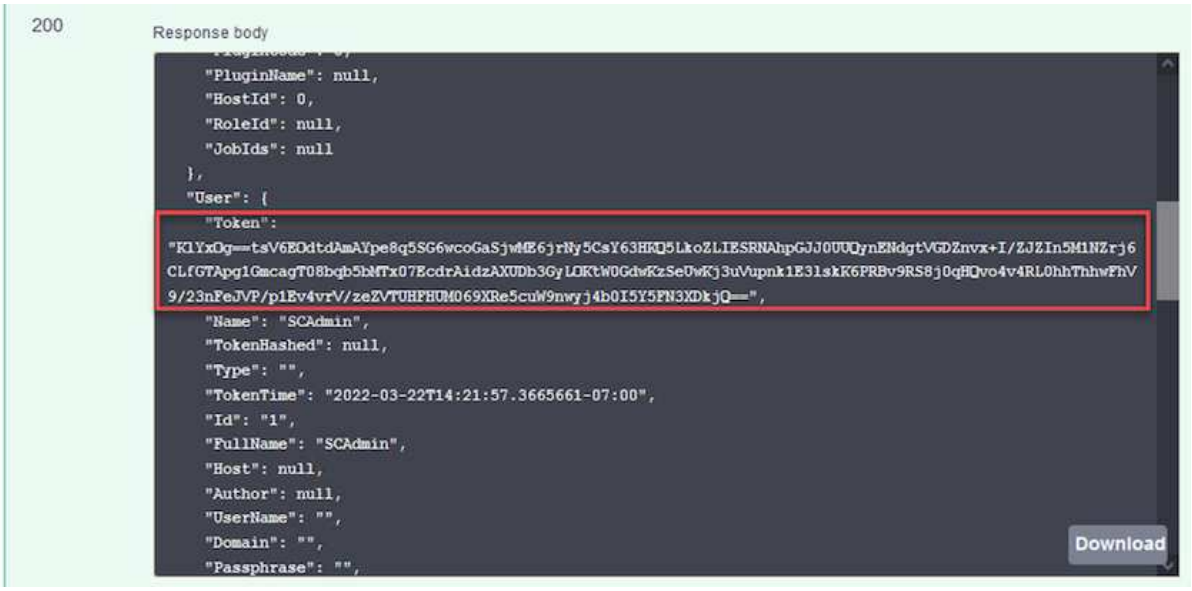
2. Expande la sección Autenticación y haz clic en Probarlo.



3. En el área UserOperationContext, complete las credenciales y el rol de SnapCenter y haga clic en Ejecutar.



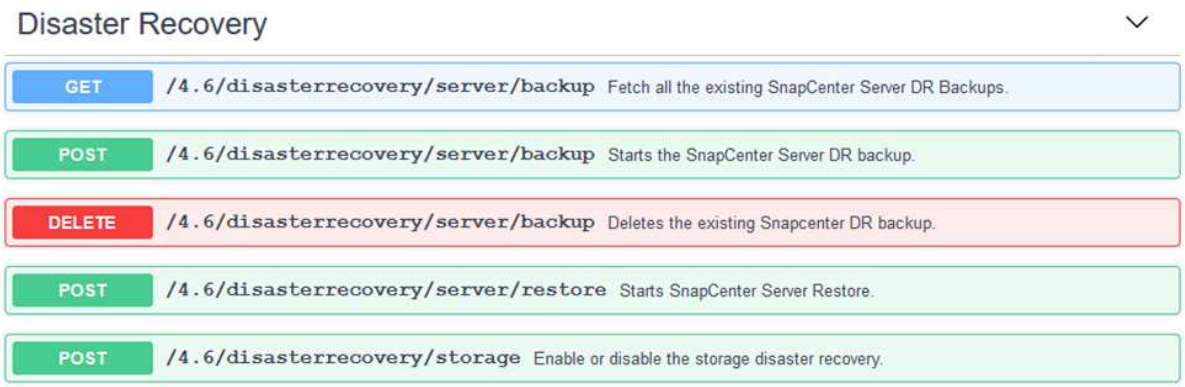
4. En el cuerpo de respuesta a continuación, puedes ver el token. Copie el texto del token para la autenticación al ejecutar el proceso de copia de seguridad.



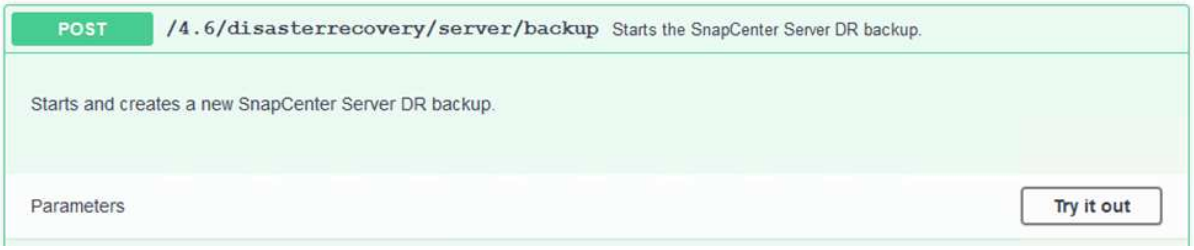
Realizar una copia de seguridad de la base de datos de SnapCenter

A continuación, vaya al área Recuperación ante desastres en la página Swagger para comenzar el proceso de copia de seguridad de SnapCenter .

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

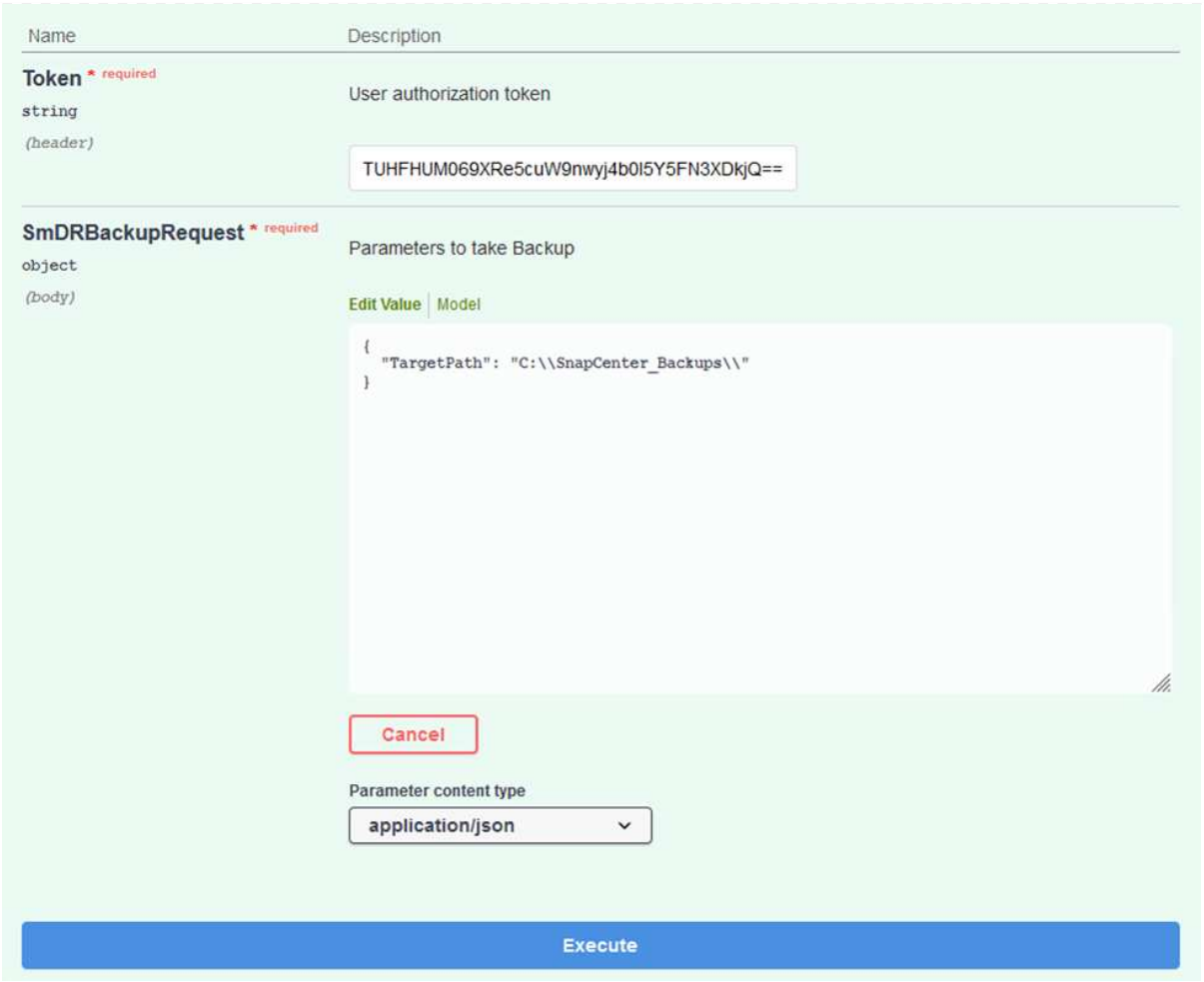


2. Ampliar el `/4.6/disasterrecovery/server/backup` sección y haga clic en Probarlo.



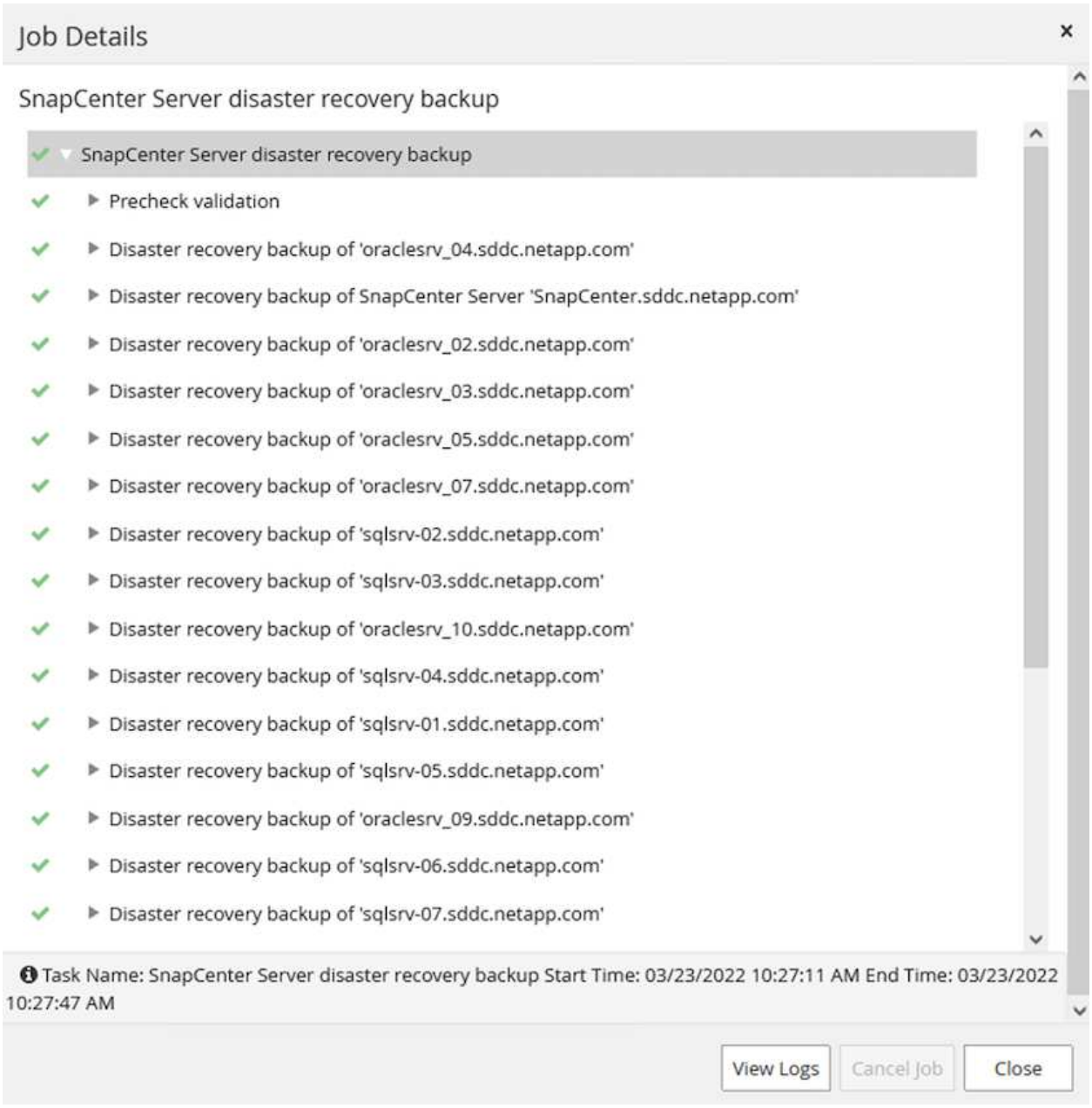
3. En la sección SmDRBackupRequest, agregue la ruta de destino local correcta y seleccione Ejecutar para iniciar la copia de seguridad de la base de datos y la configuración de SnapCenter .

> El proceso de copia de seguridad no permite realizar copias de seguridad 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

Supervisar el trabajo de respaldo 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 Monitor, puede ver los detalles de la copia de seguridad de recuperación ante desastres del servidor SnapCenter .



Utilice la utilidad XCOPY para copiar el archivo de respaldo de la base de datos al recurso compartido SMB

A continuación, debe mover la copia de seguridad de la unidad local en el servidor SnapCenter al recurso compartido CIFS que se utiliza para copiar SnapMirror los datos a la ubicación secundaria ubicada en la instancia 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, ingrese 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 por error

El desastre ocurre en el sitio principal

En caso de un desastre que ocurre en el centro de datos local principal, nuestro escenario incluye conmutación por error a un sitio secundario que reside en la infraestructura de Amazon Web Services mediante VMware Cloud on AWS. Suponemos que las máquinas virtuales y nuestro clúster ONTAP local ya no son accesibles. Además, las máquinas virtuales SnapCenter y Veeam ya no son accesibles y deben reconstruirse en nuestro sitio secundario.

En esta sección abordamos la conmutación por error de nuestra infraestructura a la nube y cubrimos los siguientes temas:

- Restauración de la base de datos de SnapCenter . Después de establecer un nuevo servidor SnapCenter , restaure la base de datos MySQL y los archivos de configuración y cambie la base de datos al modo de recuperación ante desastres para permitir que el almacenamiento secundario FSx se convierta en el dispositivo de almacenamiento principal.
- Restaure las máquinas virtuales de la aplicación mediante Veeam Backup & Replication. Conecte el almacenamiento S3 que contiene las copias de seguridad de la máquina virtual, importe las copias de seguridad y restáurelas en VMware Cloud en AWS.
- Restaure los datos de la aplicación SQL Server mediante SnapCenter.
- Restaure los datos de la aplicación Oracle mediante SnapCenter.

Proceso de restauración de la base de datos de SnapCenter

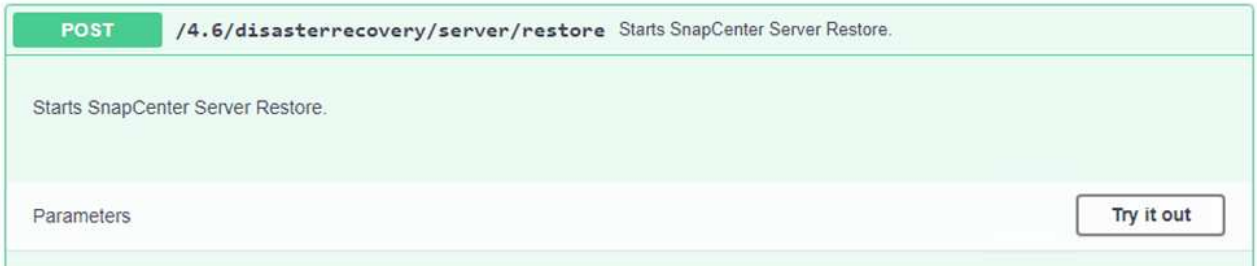
SnapCenter admite escenarios de recuperación ante desastres al permitir la copia de seguridad y la restauración de su base de datos MySQL y sus archivos de configuración. Esto permite que un administrador mantenga copias de seguridad periódicas de la base de datos de SnapCenter en el centro de datos local y luego restaure esa base de datos en una base de datos secundaria de SnapCenter .

Para acceder a los archivos de respaldo de SnapCenter en el servidor remoto de SnapCenter , complete los siguientes pasos:

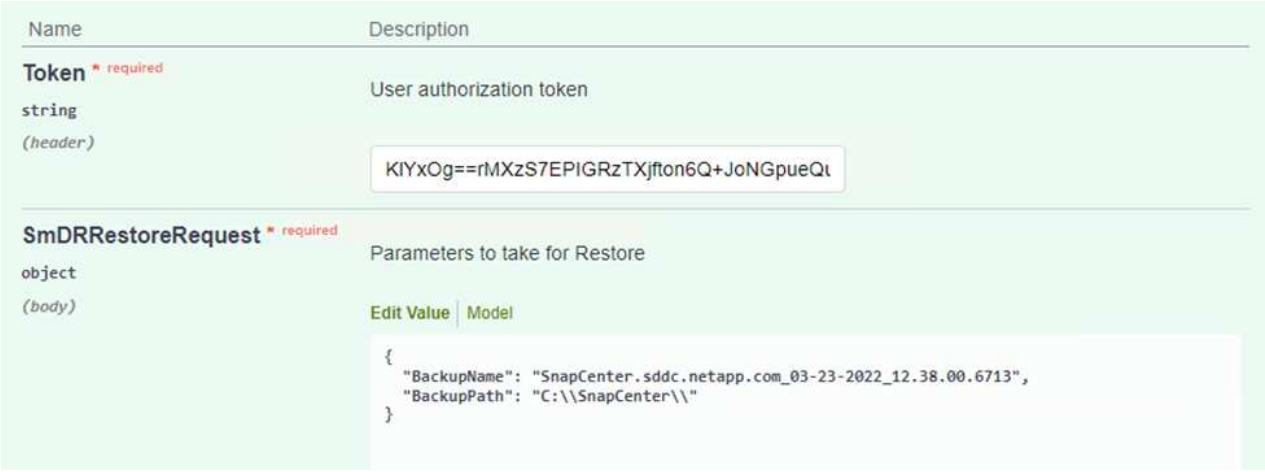
1. Romper la relación SnapMirror del clúster FSx, lo que hace que el volumen sea de lectura y escritura.
2. Cree un servidor CIFS (si es necesario) y cree un recurso compartido CIFS que apunte a la ruta de unión del volumen clonado.
3. Utilice xcopy para copiar los archivos de respaldo a un directorio local en el sistema SnapCenter secundario.
4. Instalar SnapCenter v4.6.
5. Asegúrese de que el servidor SnapCenter tenga el mismo FQDN que el servidor original. Esto es necesario para que la restauración de la base de datos sea exitosa.

Para iniciar el proceso de restauración, complete los siguientes pasos:

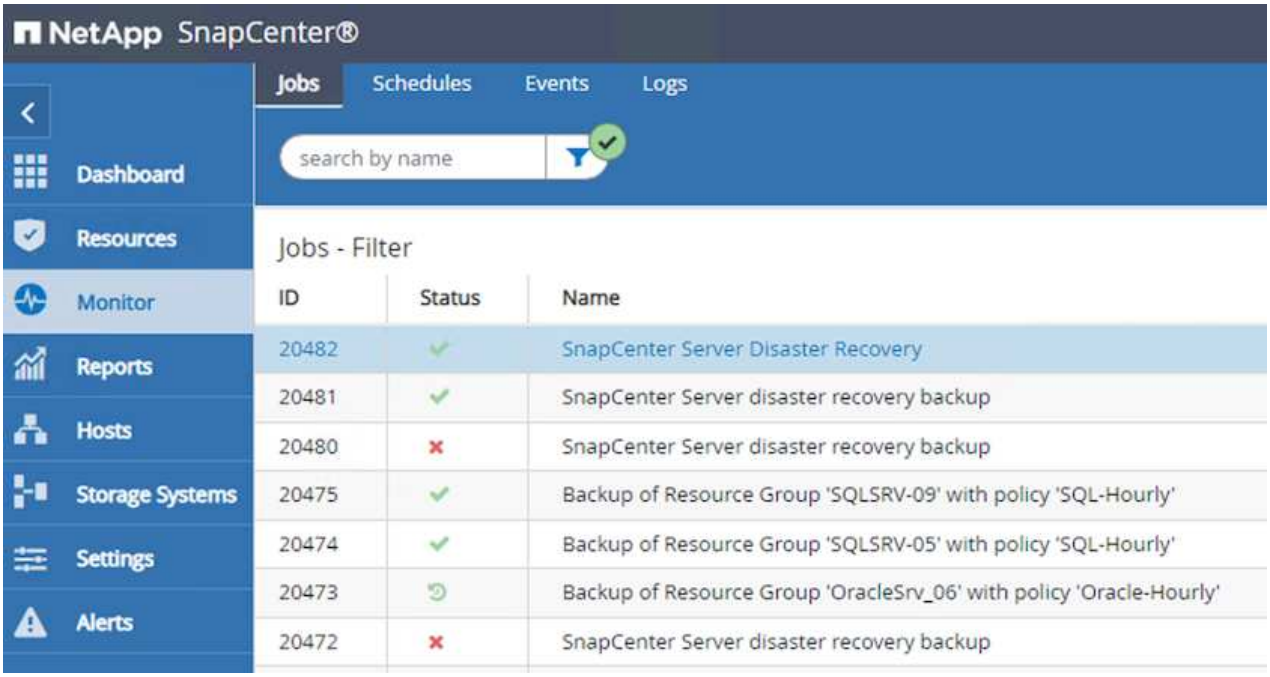
1. Navegue a la página web de la API de Swagger para el servidor secundario SnapCenter y siga las instrucciones anteriores para obtener un token de autorización.
2. Vaya a la sección Recuperación ante desastres de la página Swagger, seleccione `/4.6/disasterrecovery/server/restore` y haga clic en Probarlo.

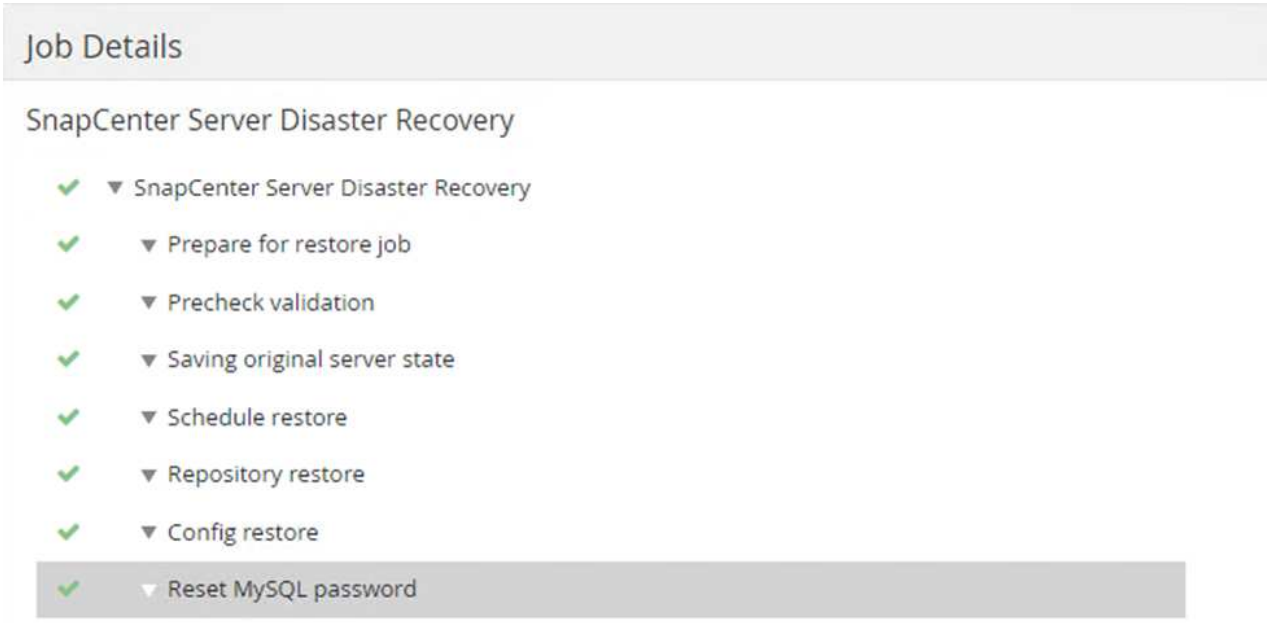


3. Pegue su token de autorización y, en la sección SmDRResterRequest, pegue el nombre de la copia de seguridad y el directorio local en el servidor secundario de SnapCenter .



4. Seleccione el botón Ejecutar para iniciar el proceso de restauración.
5. Desde SnapCenter, navegue a la sección Monitor para ver el progreso del trabajo de restauración.





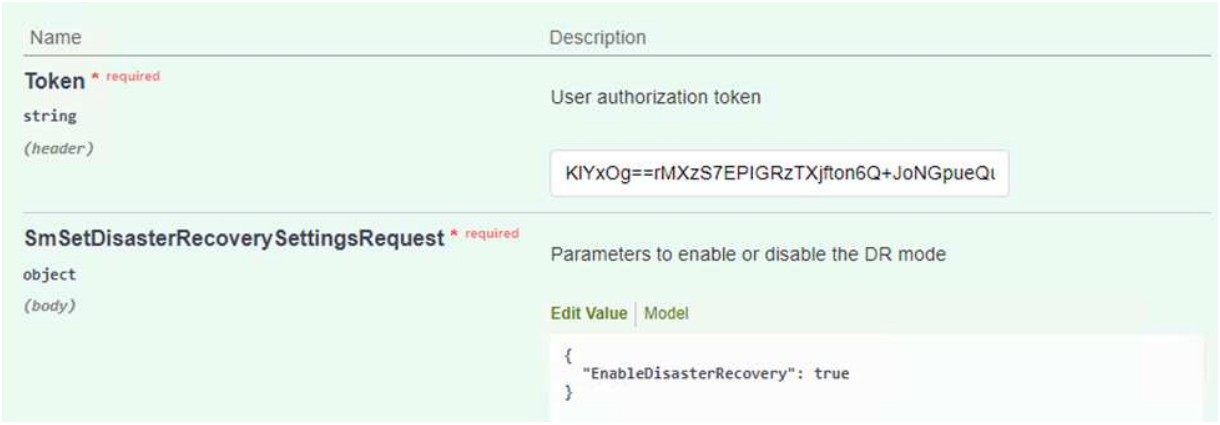
6. Para habilitar las restauraciones de SQL Server desde el almacenamiento secundario, debe alternar la base de datos de SnapCenter al modo de recuperación ante desastres. Esto se realiza como una operación separada y se inicia en la página web de la API de Swagger.

   a. Vaya a la sección Recuperación ante desastres y haga clic en `/4.6/disasterrecovery/storage`.

   b. Pegue el token de autorización del usuario.

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

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



Consulte los comentarios sobre procedimientos adicionales.

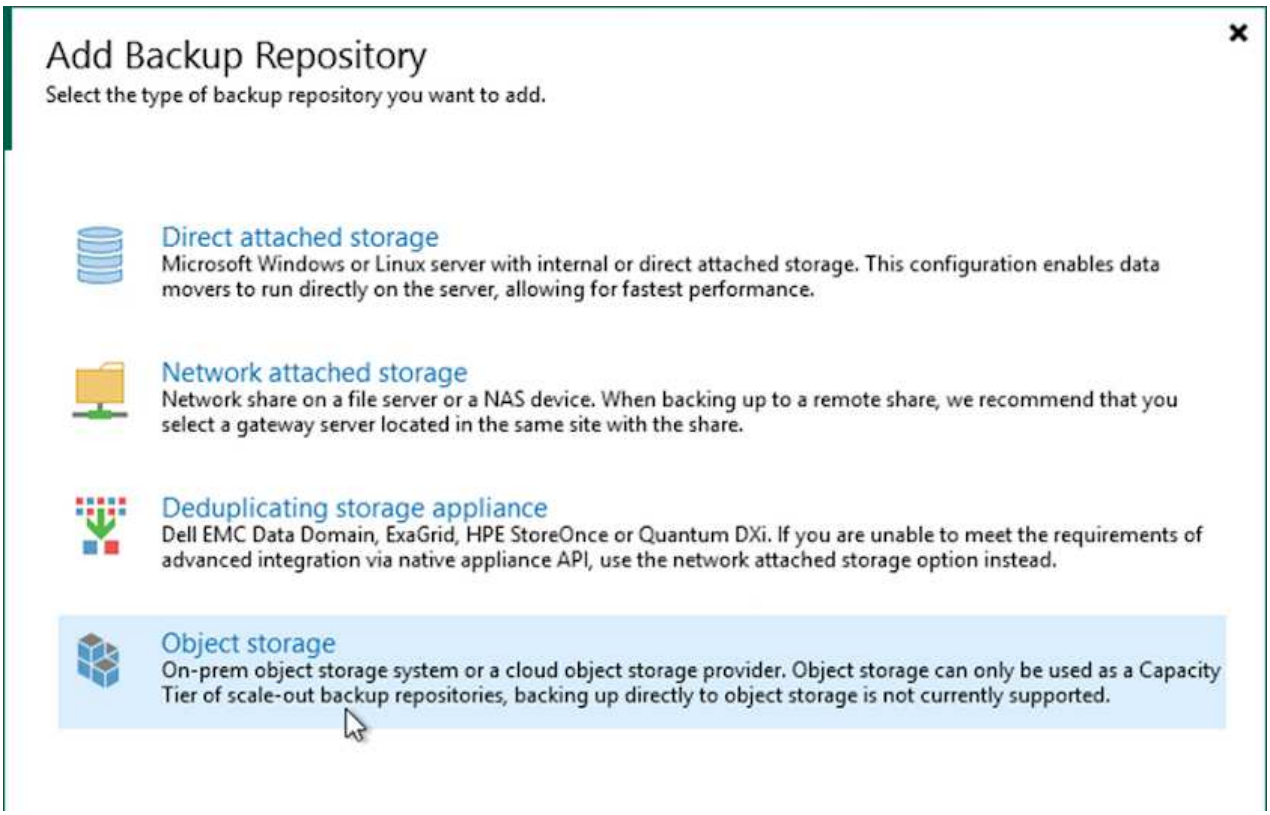
Restaurar máquinas virtuales de aplicaciones con la restauración completa de Veeam

Cree un repositorio de copias de seguridad e importe copias de seguridad desde S3

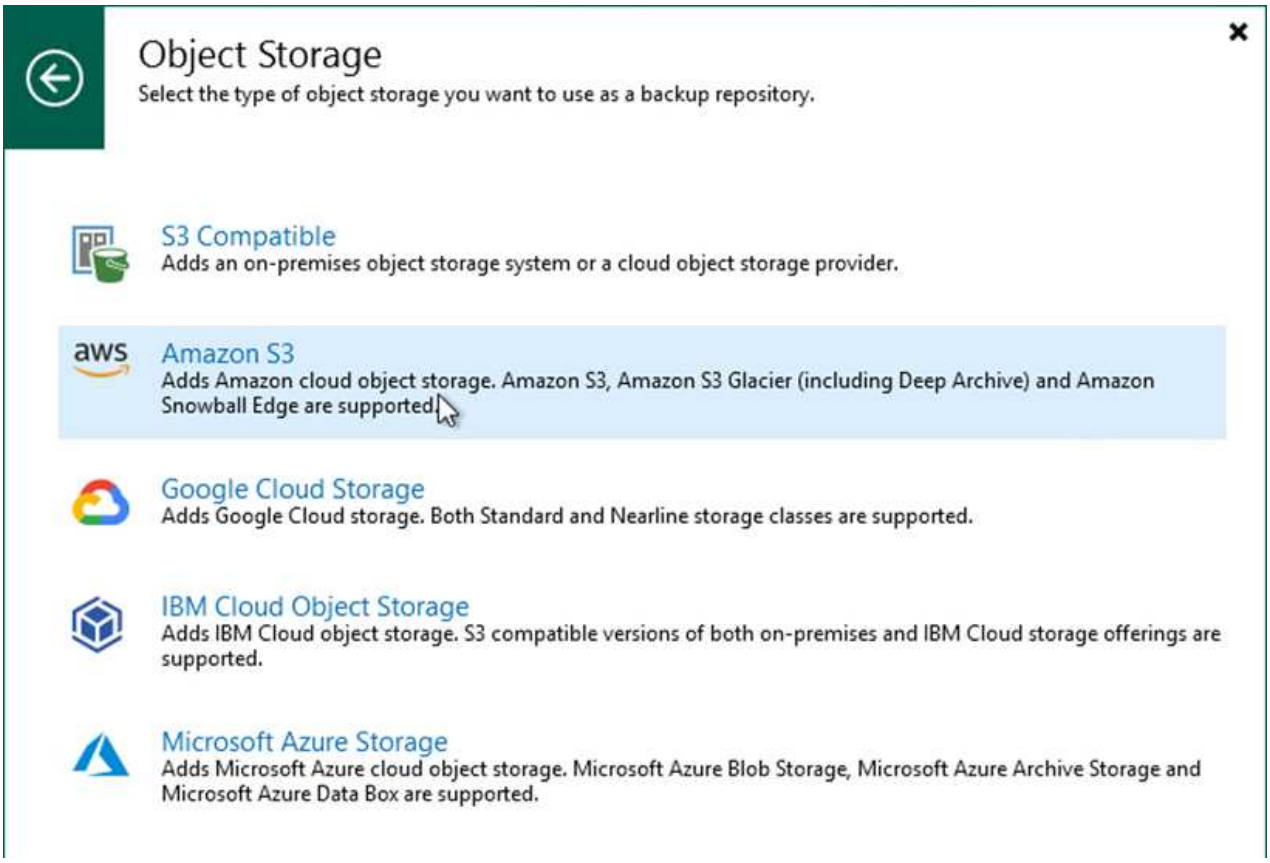
Desde el servidor secundario de Veeam, importe las copias de seguridad del almacenamiento S3 y restaure las máquinas virtuales de SQL Server y Oracle en su clúster de VMware Cloud.

Para importar las copias de seguridad del objeto S3 que formaba parte del repositorio de copias de seguridad de escalamiento horizontal local, complete los siguientes pasos:

1. Vaya a Repositorios de respaldo y haga clic en Agregar repositorio en el menú superior para iniciar el asistente Agregar repositorio de respaldo. En la primera página del asistente, seleccione Almacenamiento de objetos como tipo de repositorio de respaldo.

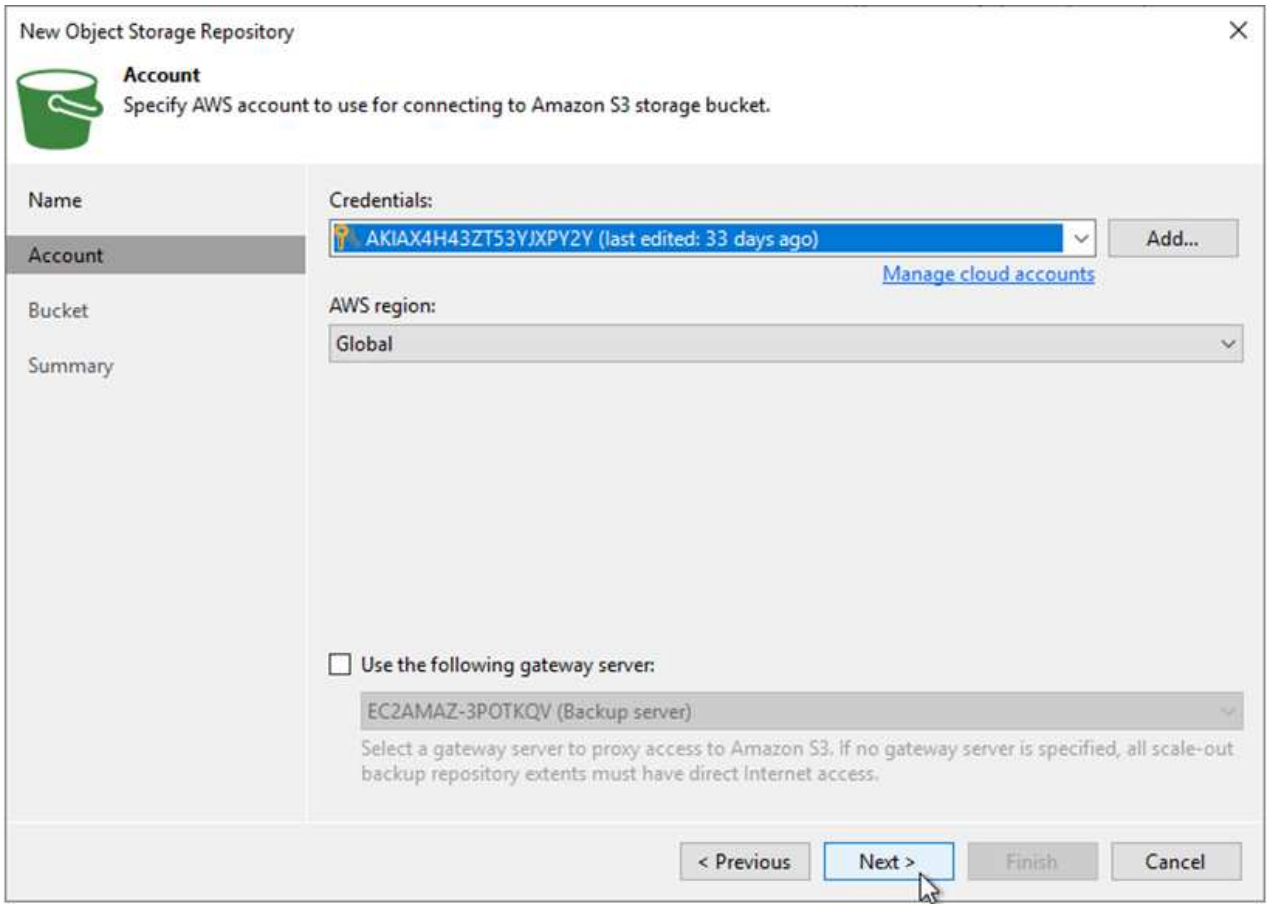


2. Seleccione Amazon S3 como tipo de almacenamiento de objetos.

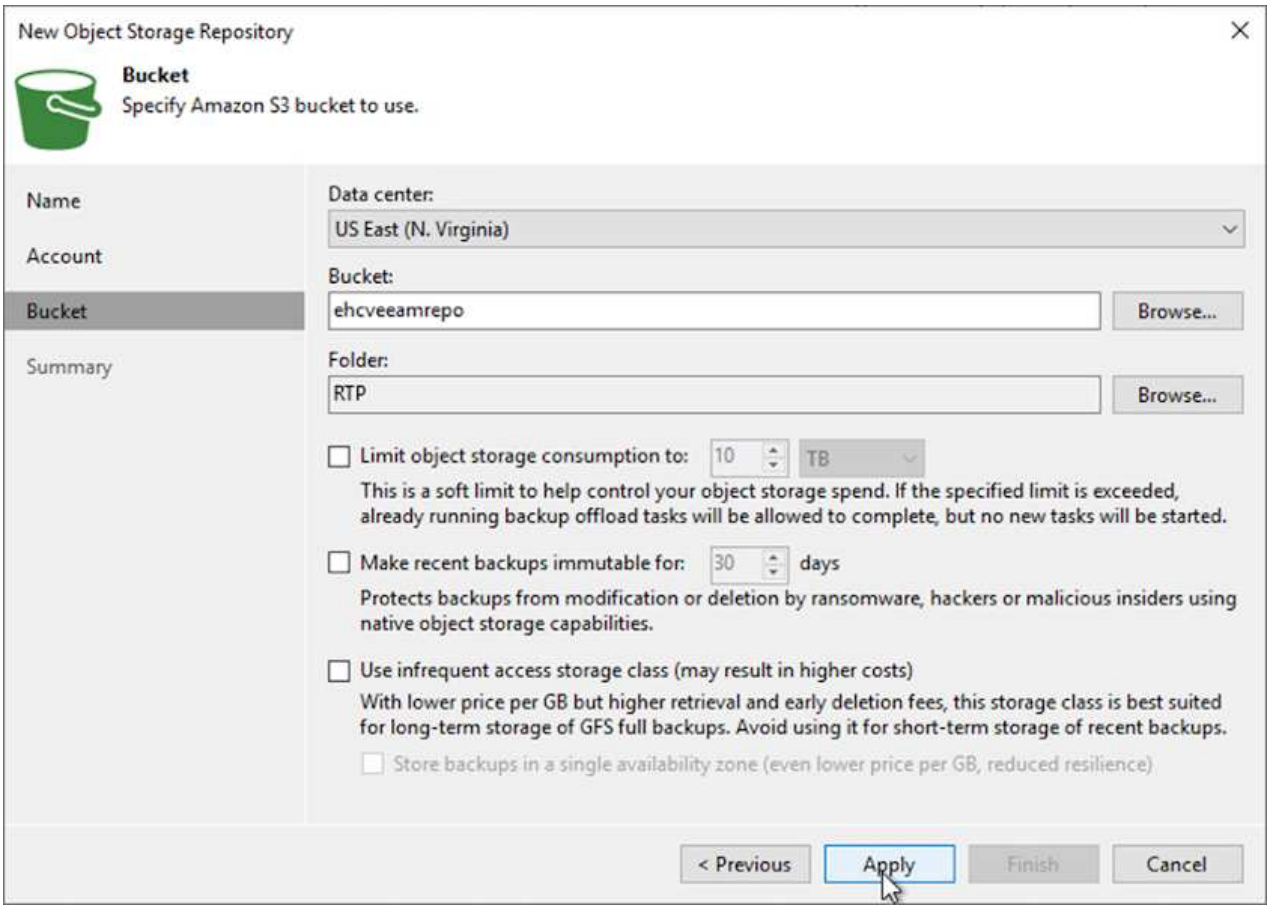


3. De la lista de servicios de almacenamiento en la nube de Amazon, seleccione Amazon S3.

4. Seleccione sus credenciales ingresadas previamente de la lista desplegable o agregue una nueva credencial para acceder al recurso de almacenamiento en la nube. Haga clic en Siguiente para continuar.



5. En la página Cubo, ingrese el centro de datos, el cubo, la carpeta y cualquier opción deseada. Haga clic en Aplicar.

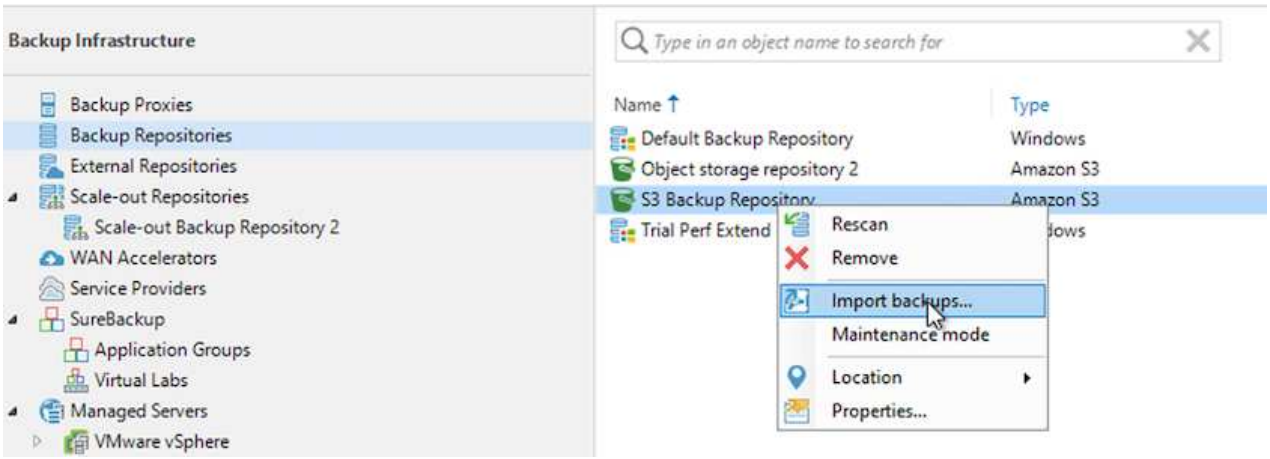


6. Por último, seleccione Finalizar para completar el proceso y agregar el repositorio.

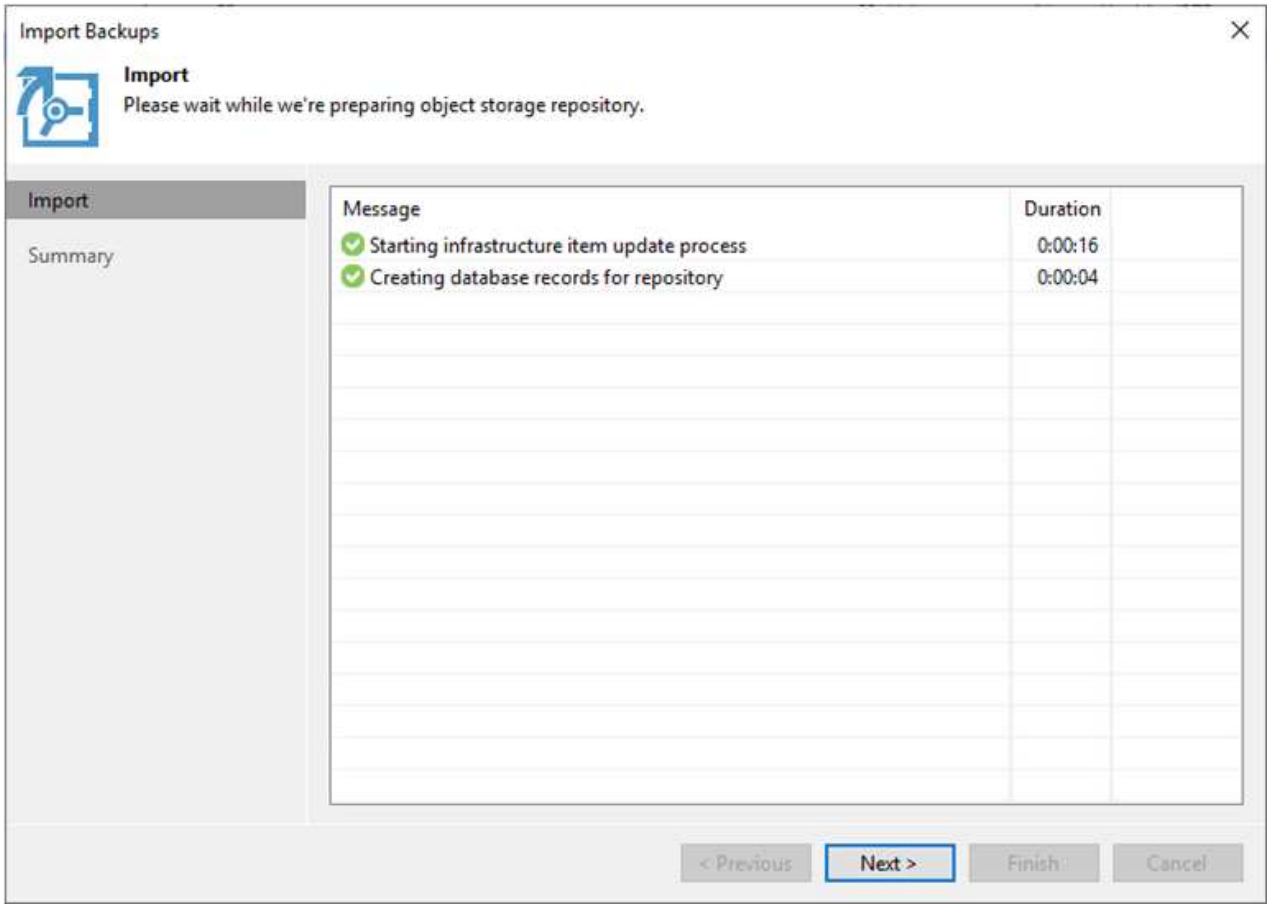
Importar copias de seguridad desde el almacenamiento de objetos S3

Para importar las copias de seguridad del repositorio S3 que se agregó en la sección anterior, complete los siguientes pasos.

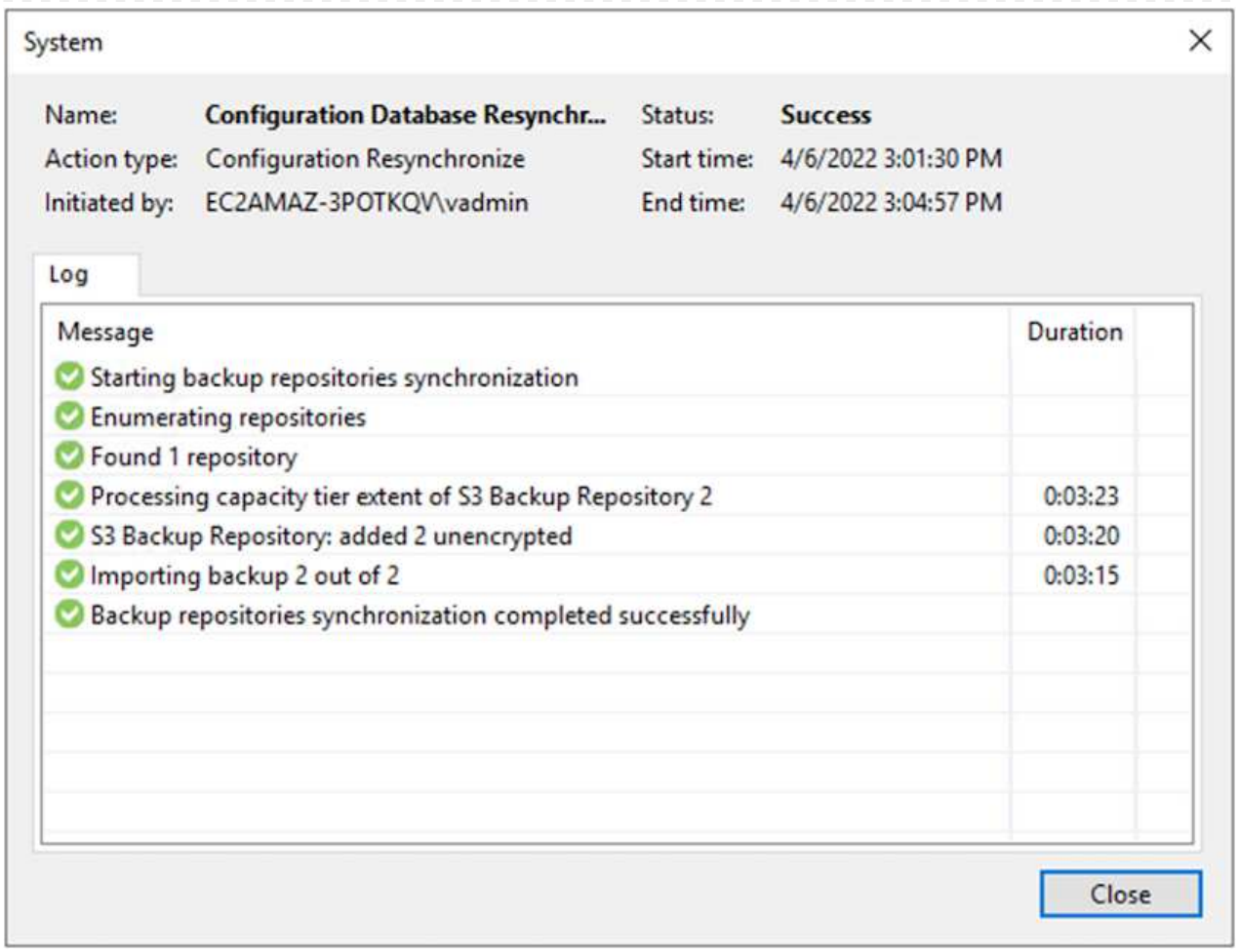
1. Desde el repositorio de copias de seguridad de S3, seleccione Importar copias de seguridad para iniciar el asistente de importación de copias de seguridad.



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



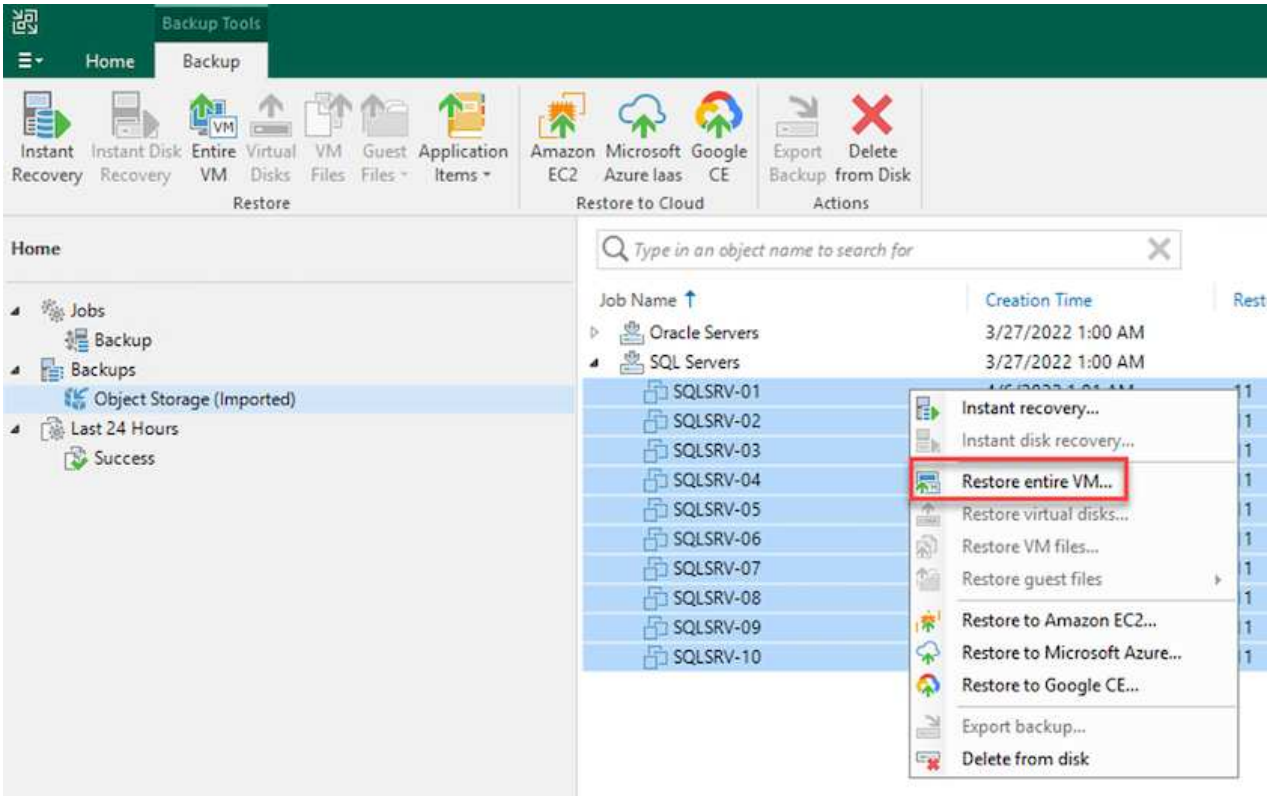
3. Una vez completada la importación, puede restaurar las máquinas virtuales en el clúster de VMware Cloud.


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

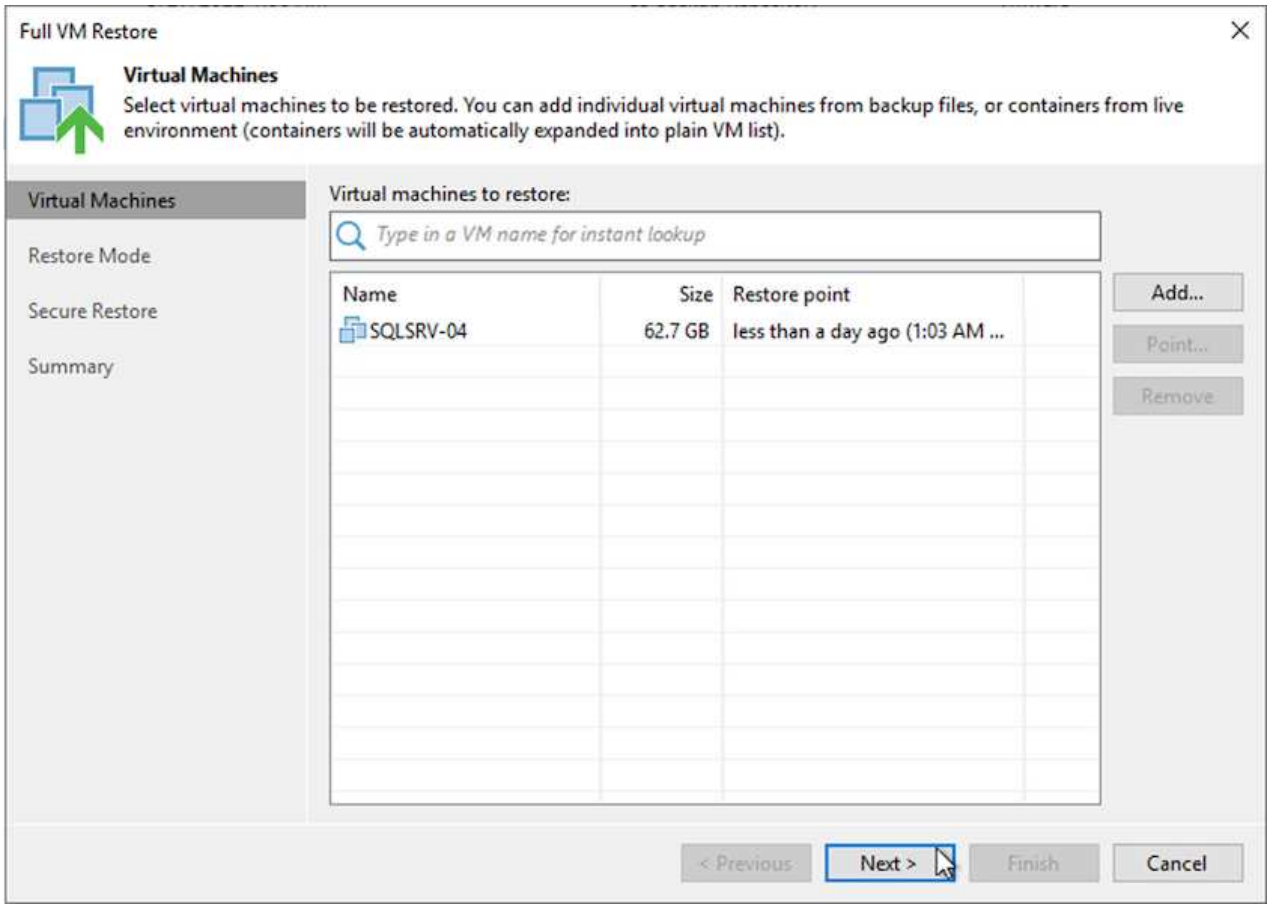
Restaurar máquinas virtuales de aplicaciones con la restauración completa de Veeam en VMware Cloud

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

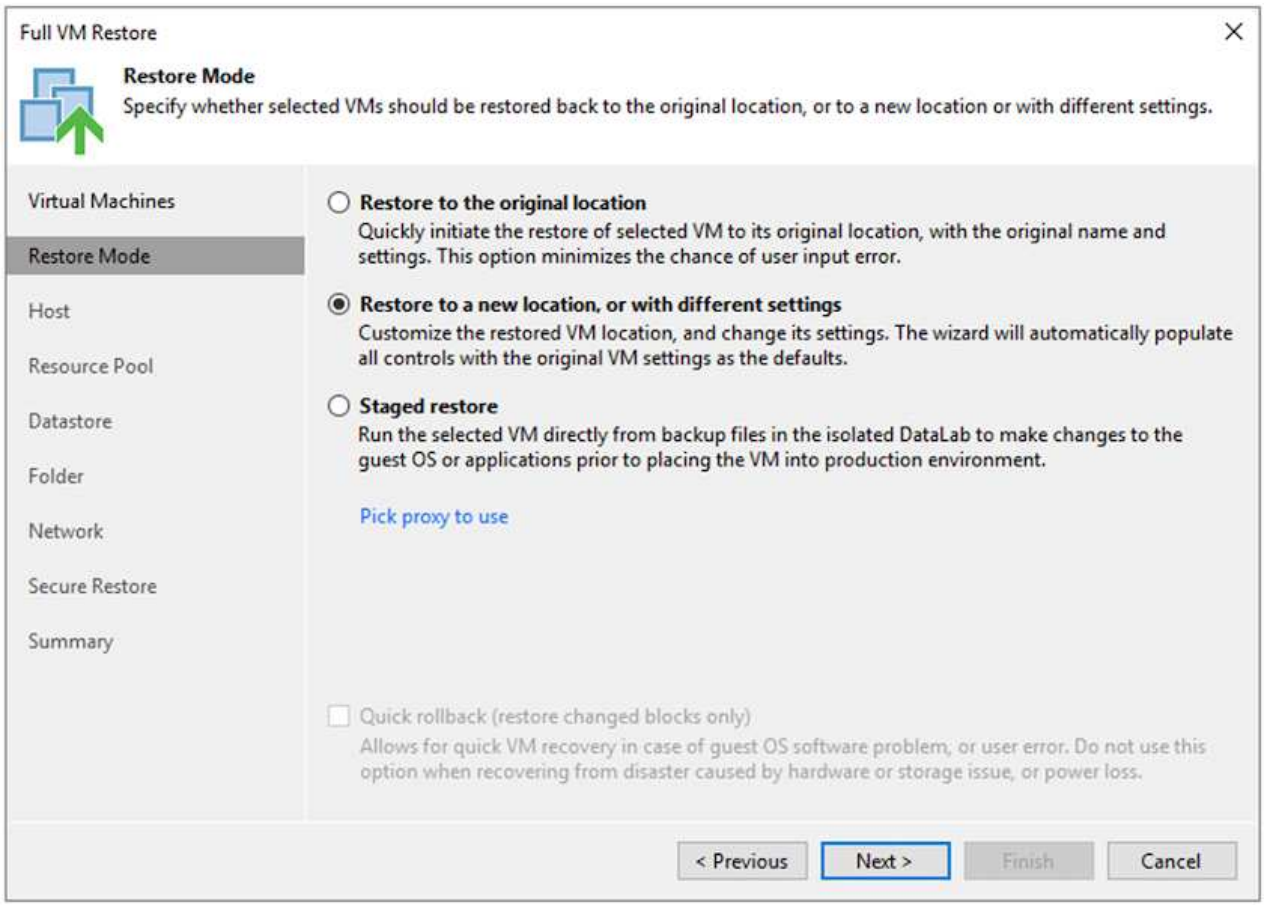
1. Desde la página de inicio de Veeam, seleccione el almacenamiento de objetos que contiene las copias de seguridad importadas, seleccione las máquinas virtuales que desea restaurar y, a continuación, haga clic con el botón derecho y seleccione Restaurar máquina virtual completa.



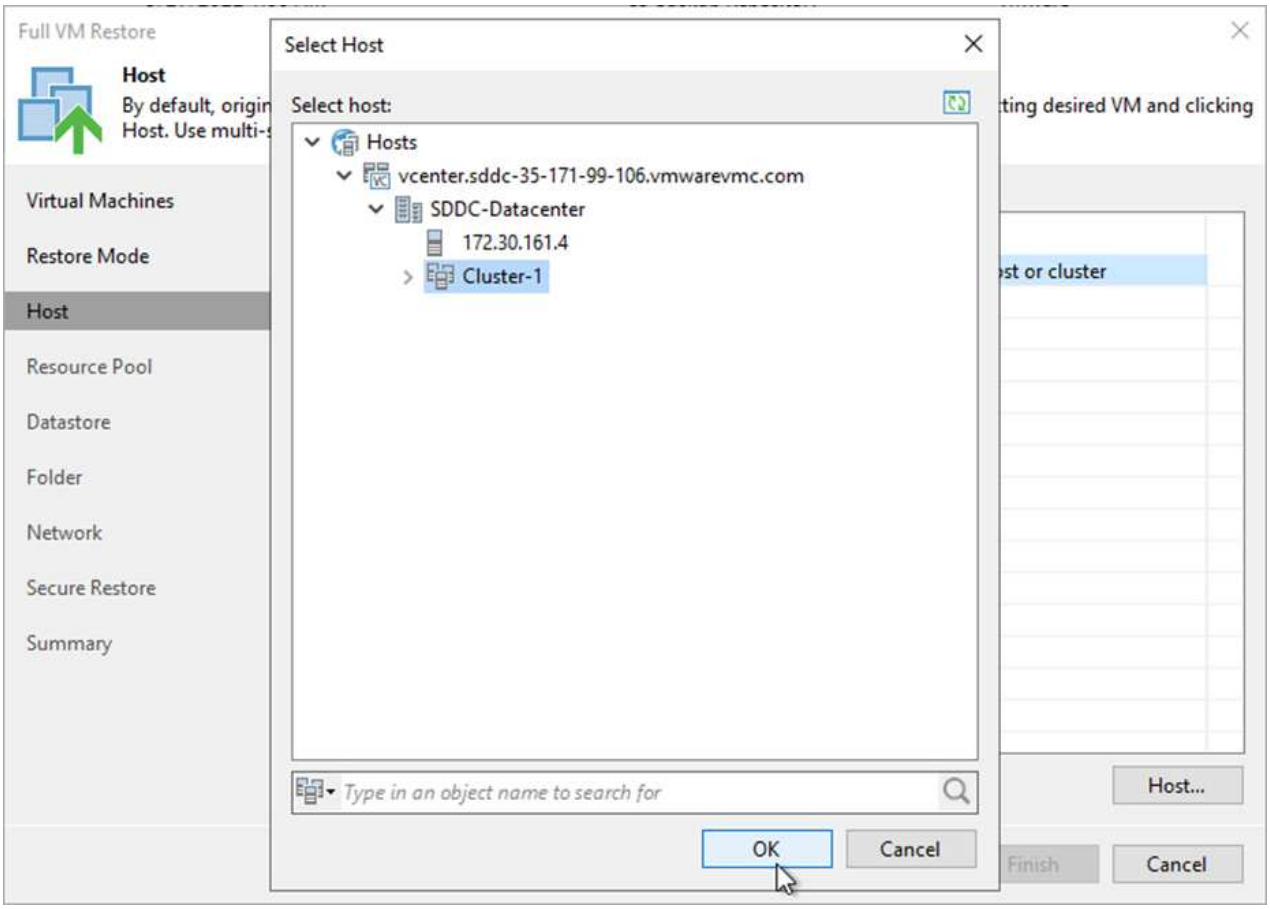
2. En la primera página del asistente de restauración completa de máquinas virtuales, modifique las máquinas virtuales de las que desea realizar una copia de seguridad y seleccione Siguiente.



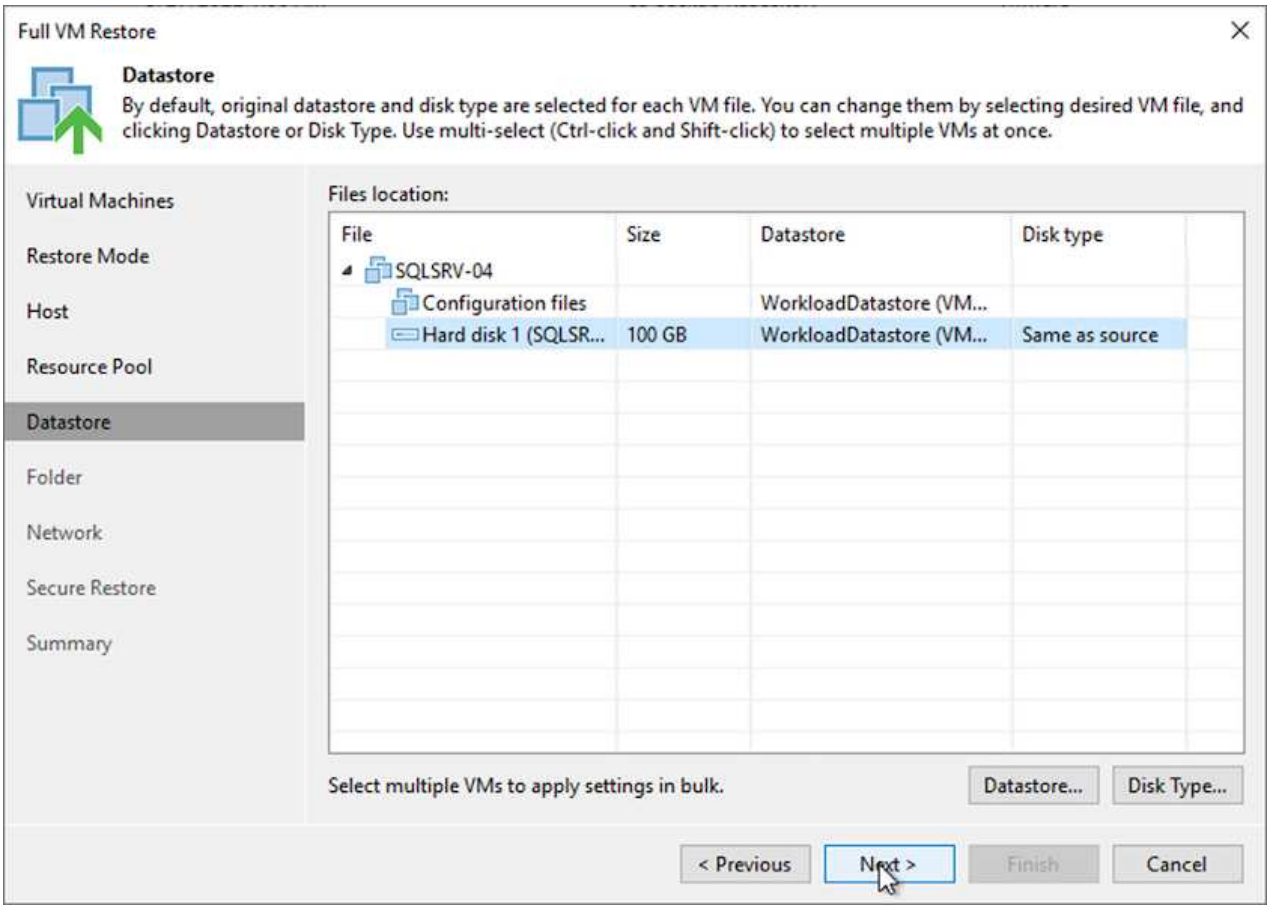
3. En la página Modo de restauración, seleccione Restaurar en una nueva ubicación o con configuraciones diferentes.



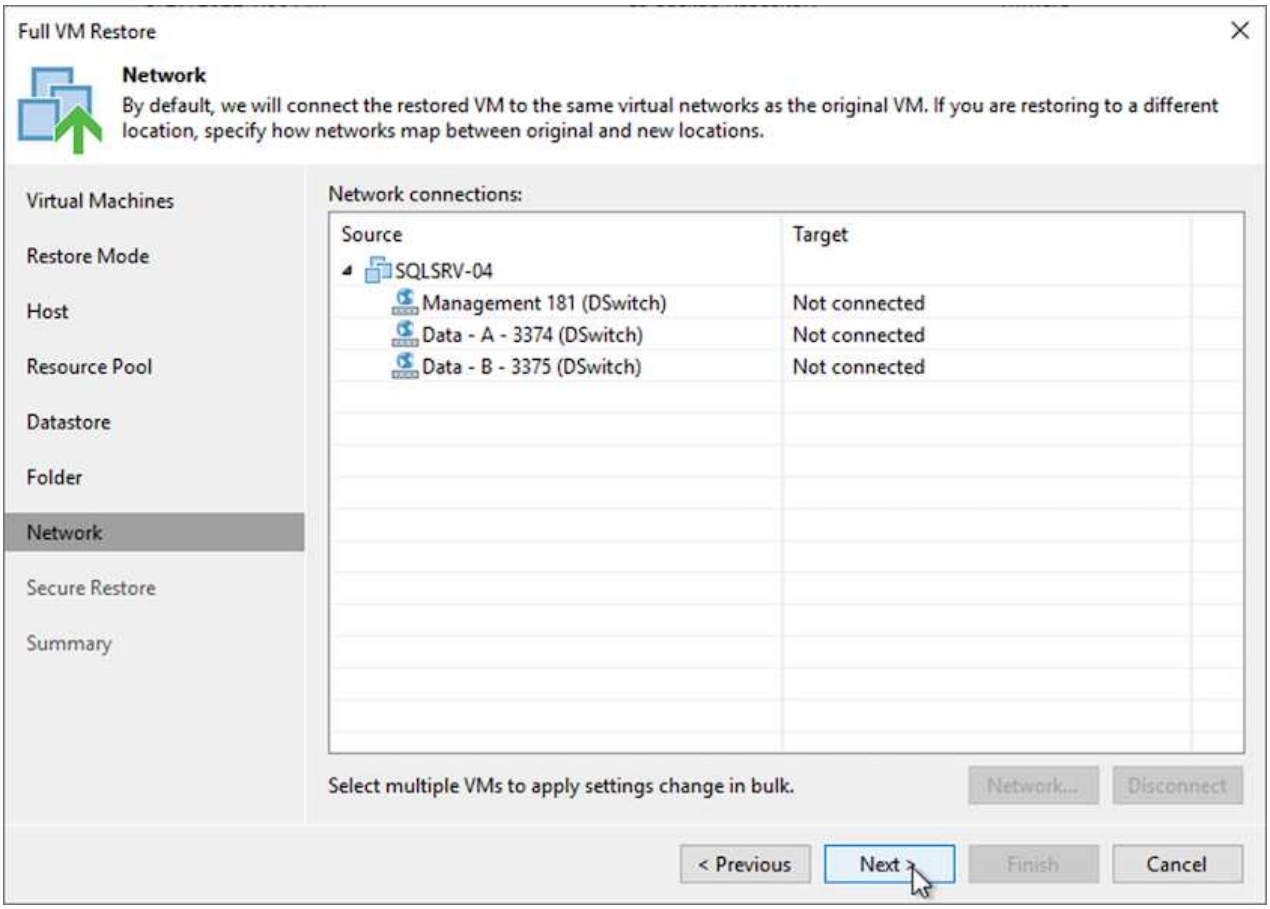
4. En la página del host, seleccione el host o clúster ESXi de destino donde restaurar la máquina virtual.

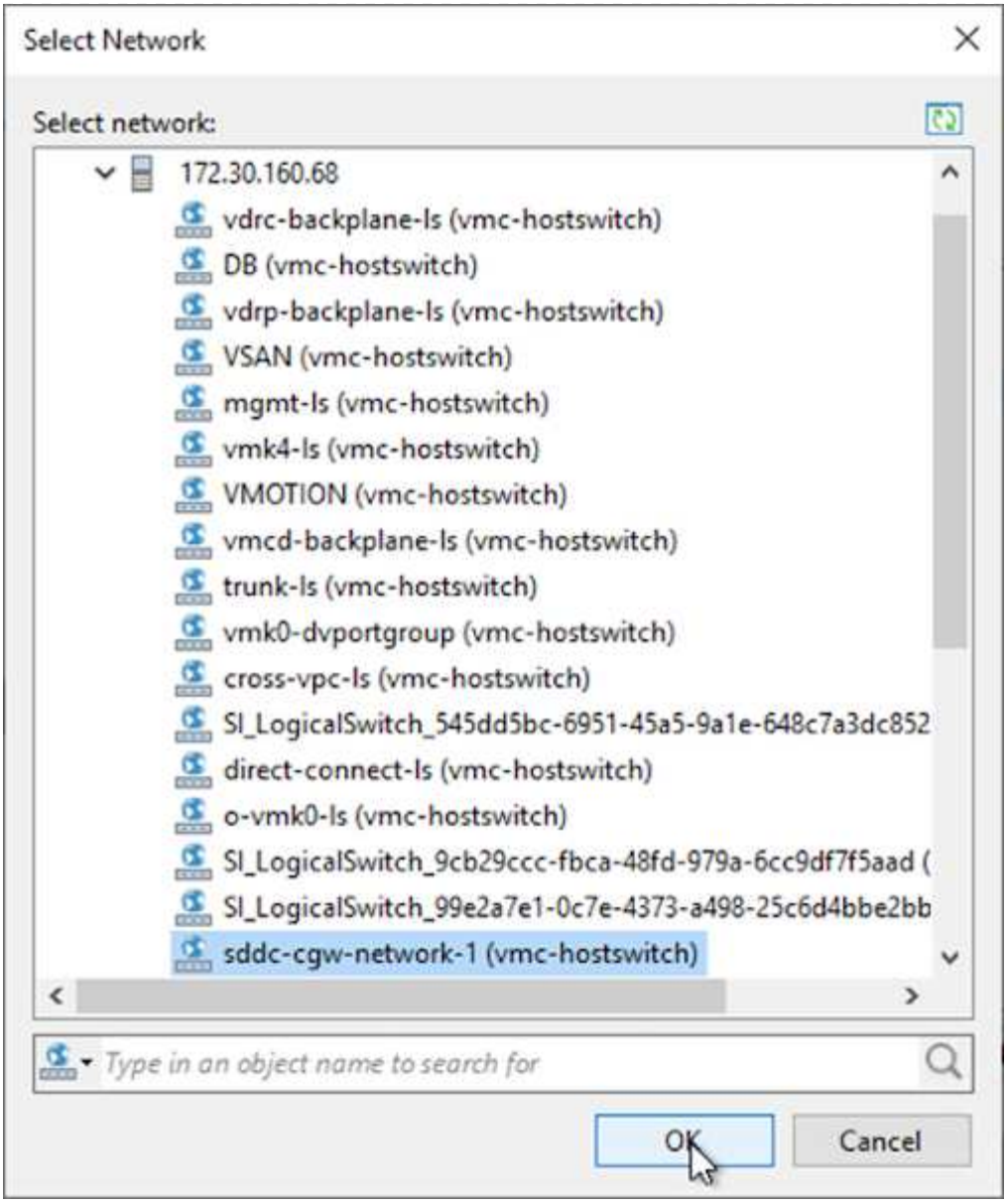


5. En la página Almacenes de datos, seleccione la ubicación del almacén de datos de destino para los archivos de configuración y el disco duro.



6. En la página Red, asigne las redes originales de la máquina 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 escanear la máquina virtual restaurada en busca de malware, revise la página de resumen y haga clic en Finalizar para iniciar la restauración.

Restaurar datos de la aplicación SQL Server

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

Se supone que se cumplen los siguientes requisitos previos para poder continuar con los pasos de recuperación:

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

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

Una vez completada la restauración de la máquina virtual, debe configurar la red y otros elementos como preparación para redescubrir la máquina virtual host dentro de SnapCenter.

1. Asignar nuevas direcciones IP para administración y iSCSI o NFS.
2. Unir el host al dominio de Windows.
3. Agregue los nombres de host al DNS o al archivo de hosts en el servidor SnapCenter .

> Si el complemento de SnapCenter se implementó con credenciales de dominio diferentes a las del dominio actual, debe cambiar la cuenta de inicio de sesión del complemento para el servicio de Windows en la máquina virtual de SQL Server. Después de cambiar la cuenta de inicio de sesión, reinicie los servicios SnapCenter SMCore, Plug-in para Windows y Plug-in para SQL Server.

> Para redescubrir automáticamente las máquinas virtuales restauradas en SnapCenter, el FQDN debe ser idéntico a la máquina virtual que se agregó originalmente a SnapCenter en las instalaciones.

Configurar el almacenamiento FSx para la restauración de SQL Server

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

1. Para romper la relación SnapMirror existente para 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. Otorgue acceso al LUN mediante la creación de un grupo de iniciadores que contenga el IQN iSCSI de la máquina virtual Windows de SQL Server:

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

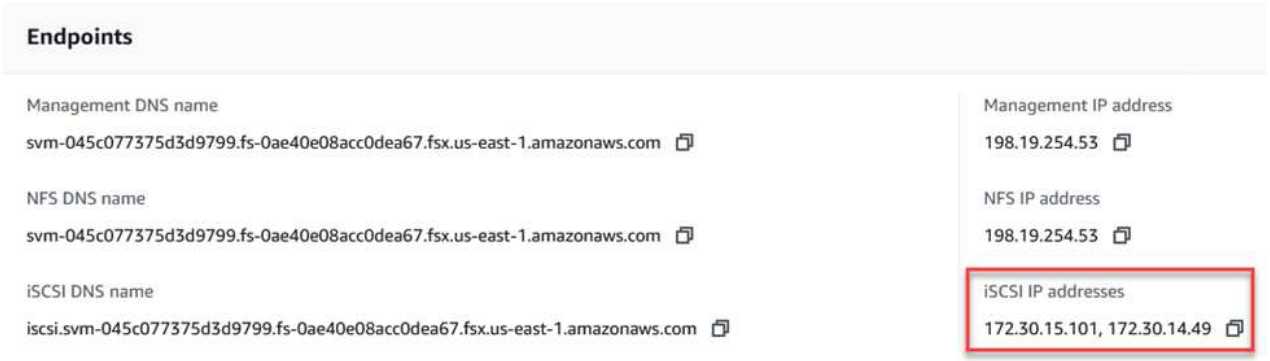
3. Por último, asigne los LUN al grupo de iniciadores que acaba de crear:

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

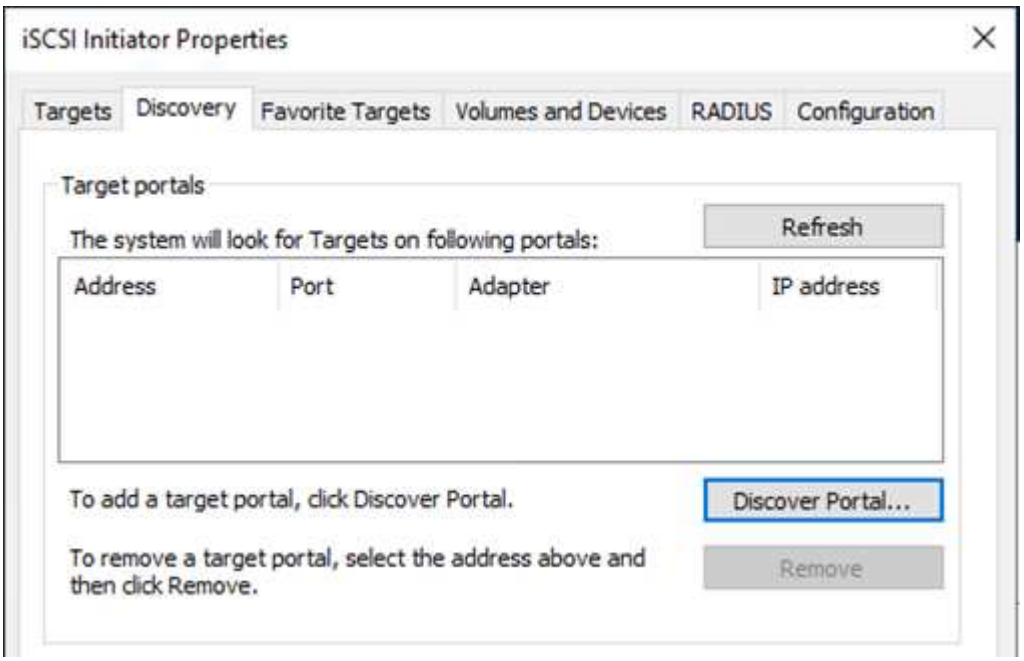
4. Para encontrar el nombre de la ruta, ejecute el `lun show` dominio.

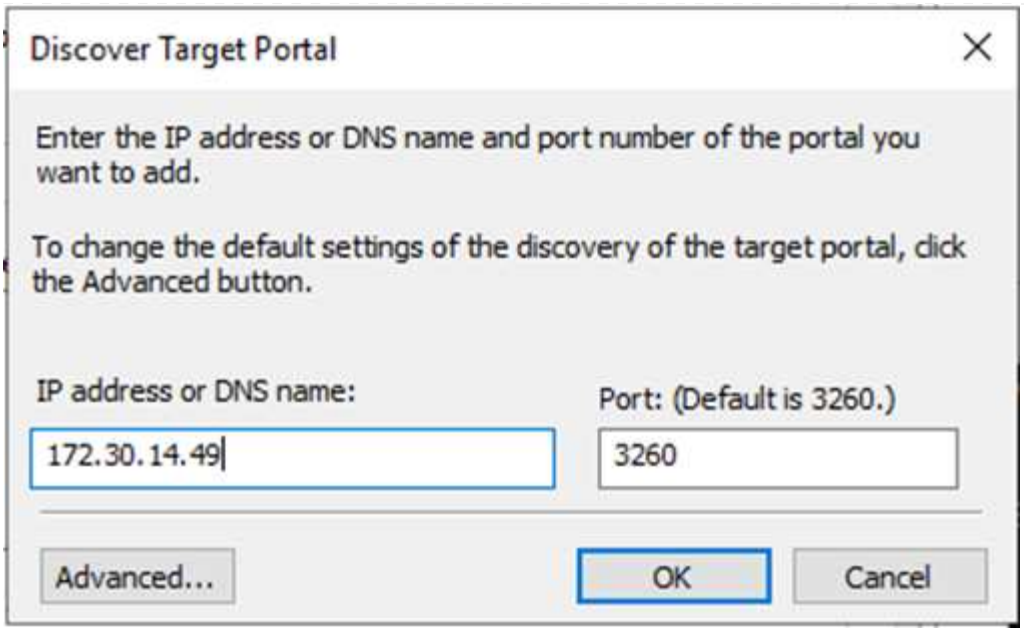
Configurar la máquina virtual de Windows para el acceso iSCSI y descubrir los sistemas de archivos

1. Desde la máquina virtual de SQL Server, configure su adaptador de red iSCSI para comunicarse en el grupo de puertos VMware que se ha establecido con conectividad a las interfaces de destino iSCSI en su instancia FSx.
2. Abra la utilidad Propiedades del iniciador iSCSI y borre las configuraciones de conectividad anteriores en las pestañas Descubrimiento, Destinos favoritos y Destinos.
3. Localice las direcciones IP para acceder a la interfaz lógica iSCSI en la instancia/clúster FSx. Esto se puede encontrar en la consola de AWS en Amazon FSx > ONTAP > Máquinas virtuales de almacenamiento.

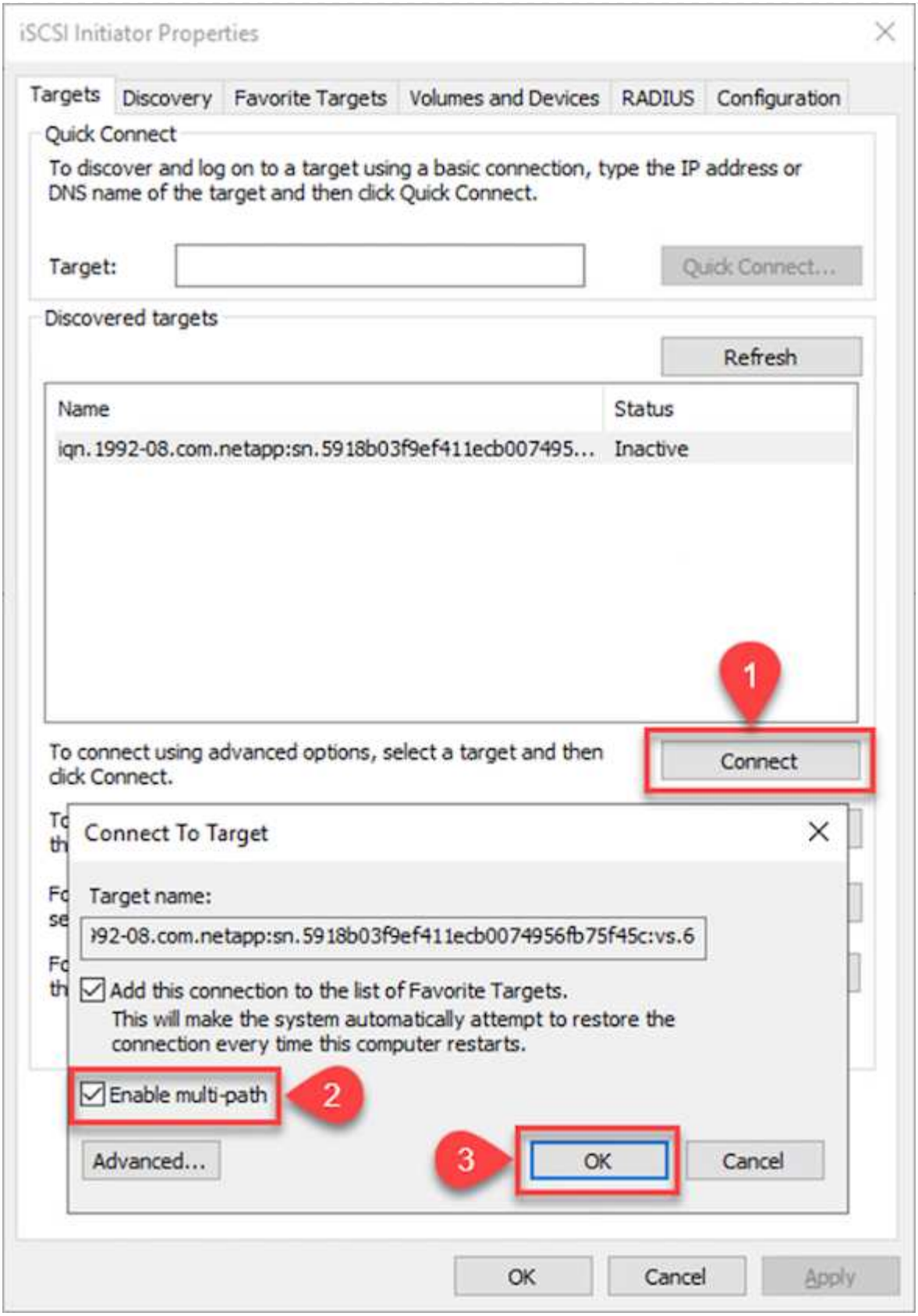


4. Desde la pestaña Descubrimiento, haga clic en Portal de descubrimiento e ingrese las direcciones IP para sus objetivos iSCSI de FSx.

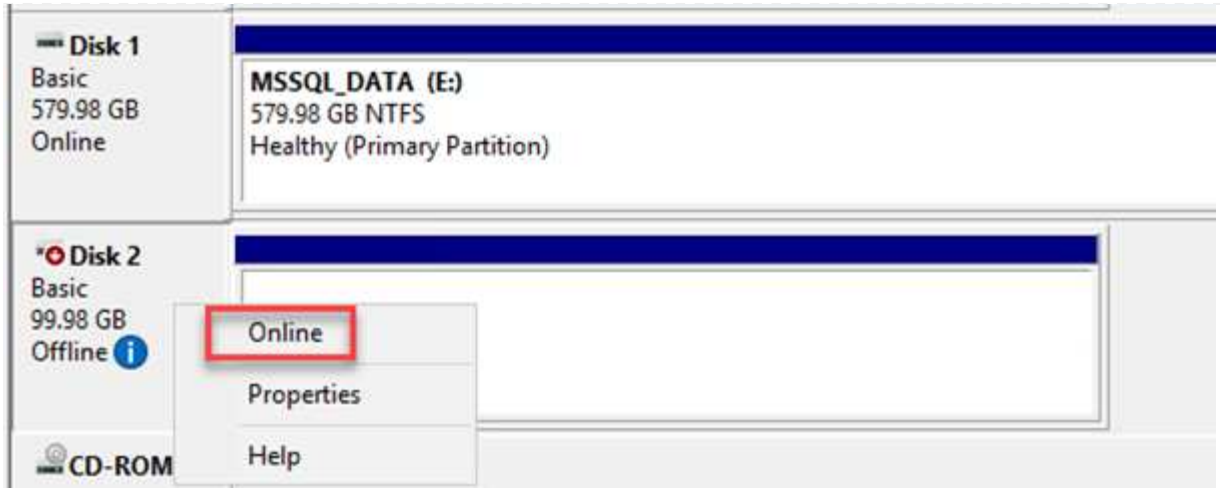




5. En la pestaña Destino, haga clic en Conectar, seleccione Habilitar múltiples rutas si corresponde a su configuración y luego haga clic en Aceptar para conectarse al destino.

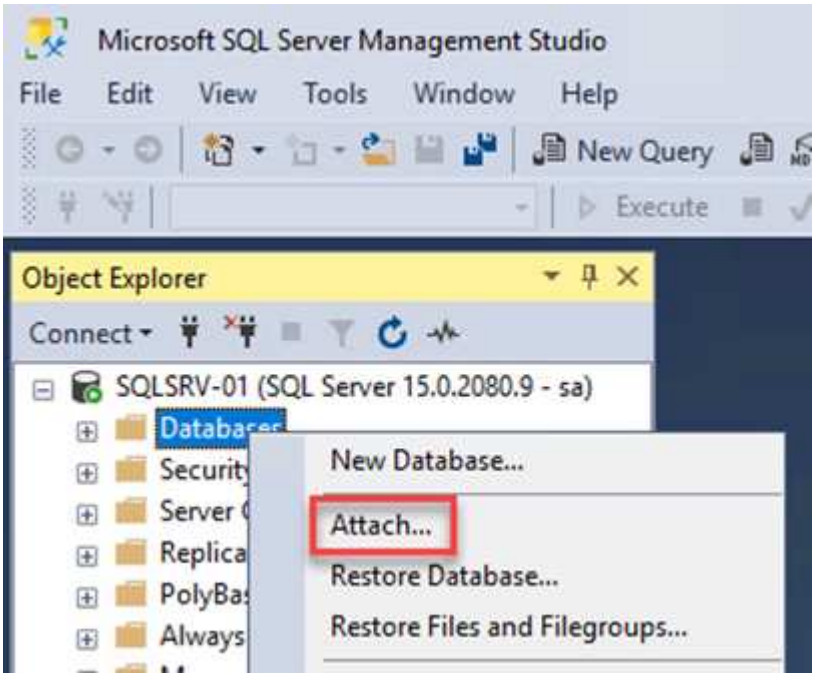


6. Abra la utilidad de Administración de equipos y ponga los discos en línea. Verifique que conserven las mismas letras de unidad que tenían anteriormente.

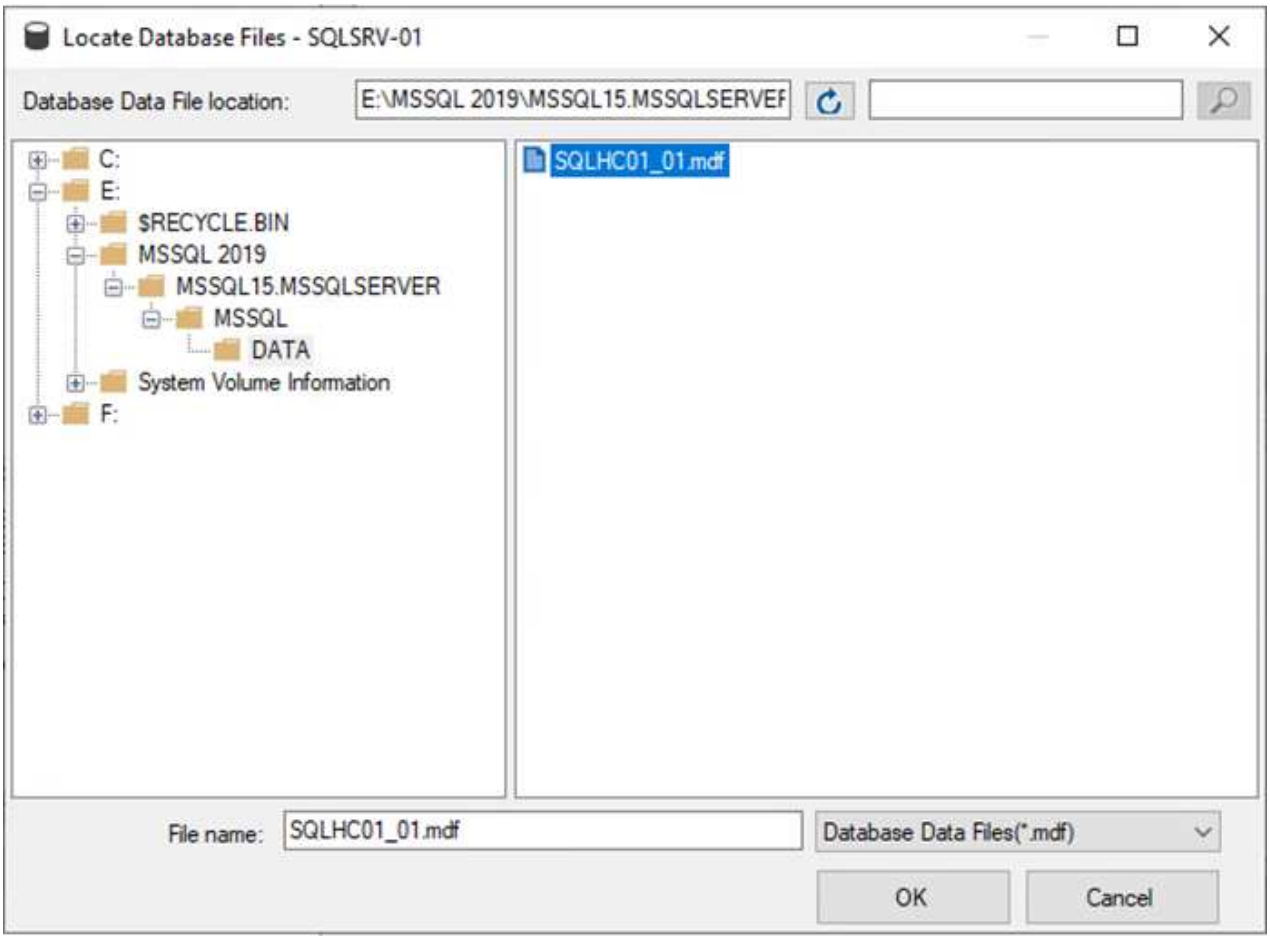

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

Adjuntar las bases de datos de SQL Server

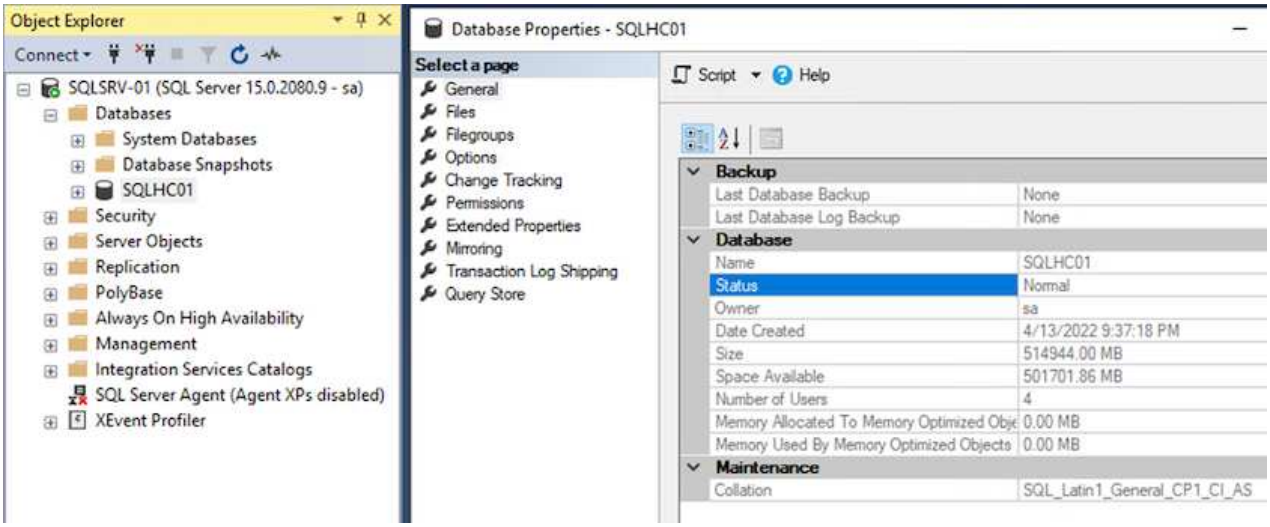
1. Desde la máquina virtual de SQL Server, abra Microsoft SQL Server Management Studio y seleccione Conectar para iniciar el proceso de conexión a la base de datos.



2. Haga clic en Agregar y navegue hasta 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 están en una unidad separada, elija la carpeta que contiene el registro de transacciones.
4. Cuando termine, haga clic en Aceptar para adjuntar la base de datos.

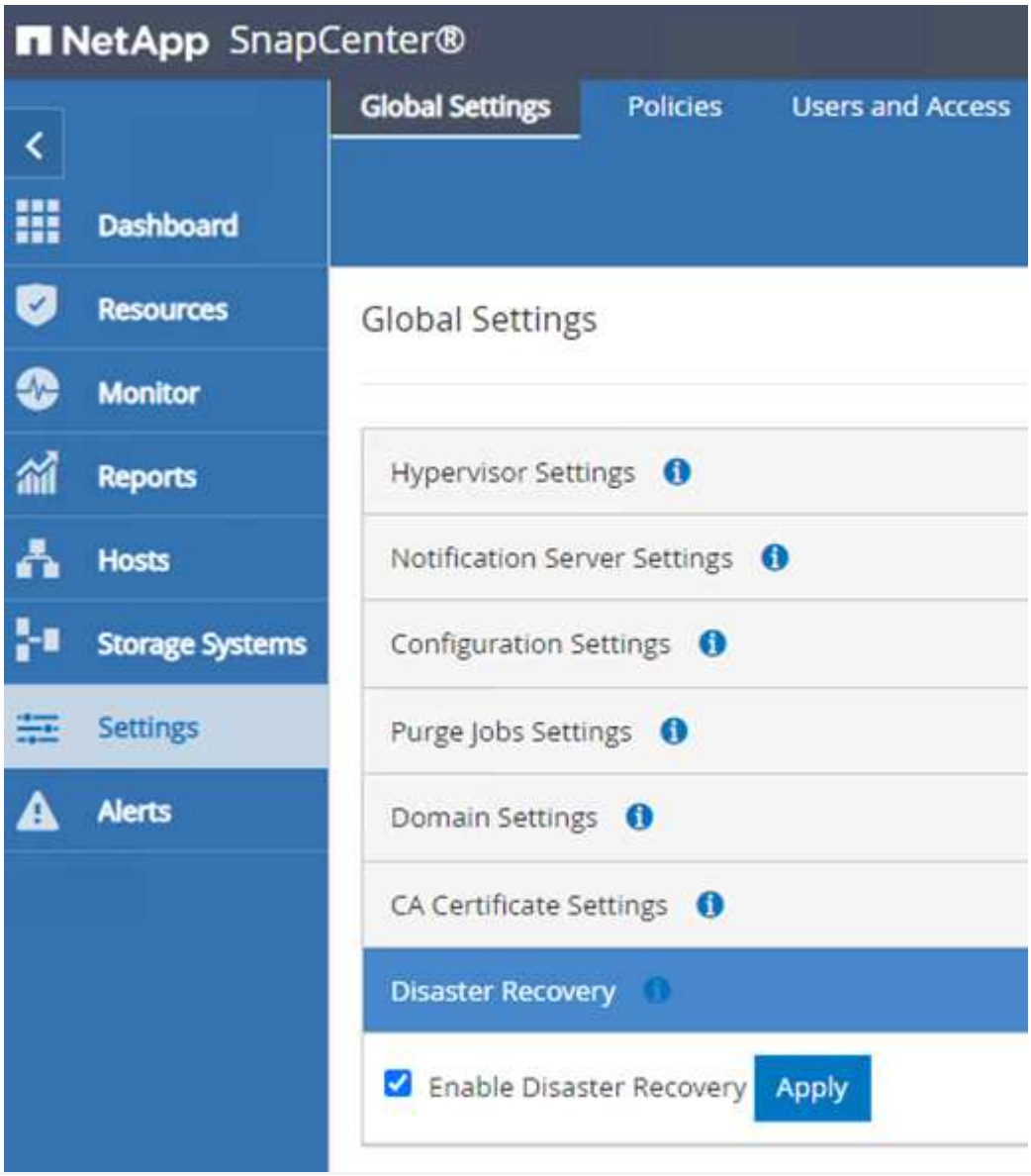


Confirmar la comunicación de SnapCenter con el complemento de SQL Server

Una vez restaurada la base de datos de SnapCenter a su estado anterior, se redescubren automáticamente los hosts de SQL Server. Para que esto funcione correctamente, tenga en cuenta los siguientes requisitos previos:

- SnapCenter debe colocarse en modo de recuperación ante desastres. Esto se puede lograr a través de la API Swagger o en Configuración global en Recuperación ante desastres.
- El FQDN del servidor SQL debe ser idéntico a la instancia que se estaba ejecutando en el centro de datos local.
- La relación original de SnapMirror debe romperse.
- Los LUN que contienen la base de datos deben montarse en la instancia de SQL Server y la base de datos debe estar conectada.

Para confirmar que SnapCenter está en modo de recuperación ante desastres, navegue a Configuración desde el cliente web de SnapCenter . Vaya a la pestaña Configuración global y luego haga clic en Recuperación ante desastres. Asegúrese de que la casilla de verificación Habilitar recuperación ante desastres esté habilitada.



Restaurar datos de la aplicación Oracle

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

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

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

Configurar FSx para la restauración de Oracle: romper la relación de SnapMirror

Para que los volúmenes de almacenamiento secundario alojados en la instancia de FSx ONTAP sean accesibles para los servidores Oracle, primero debe romper la relación 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::>
```

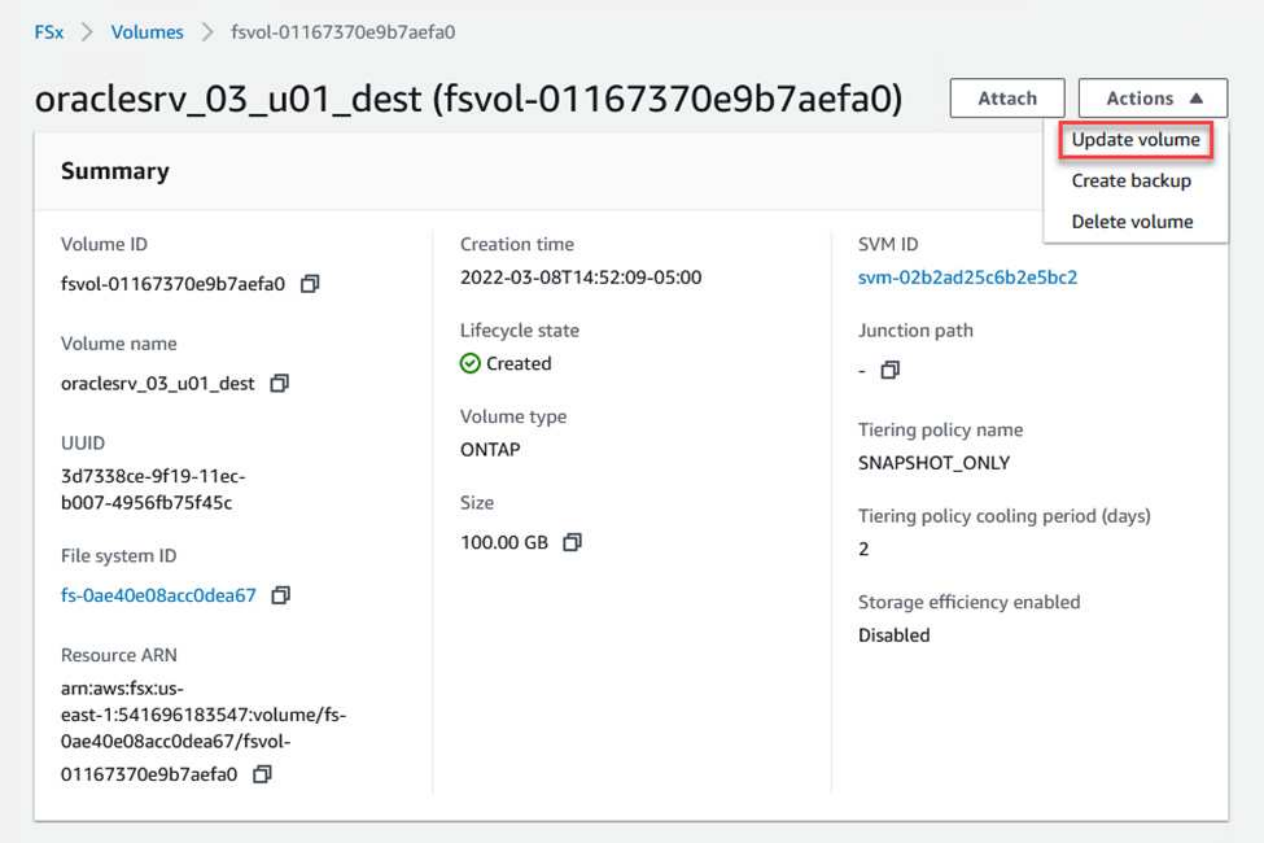
2. Ejecute el siguiente comando para romper las relaciones SnapMirror existentes.

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

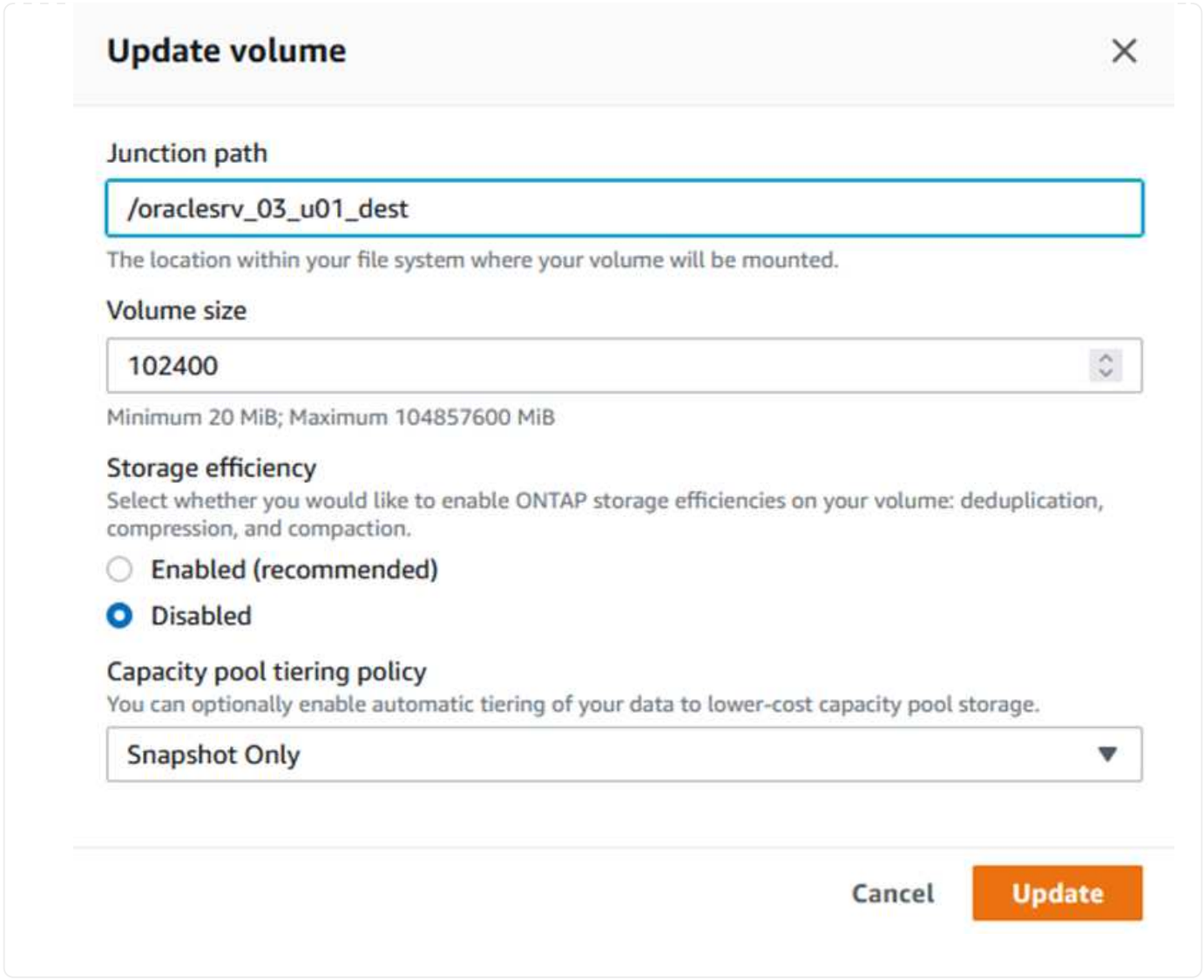
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

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 :



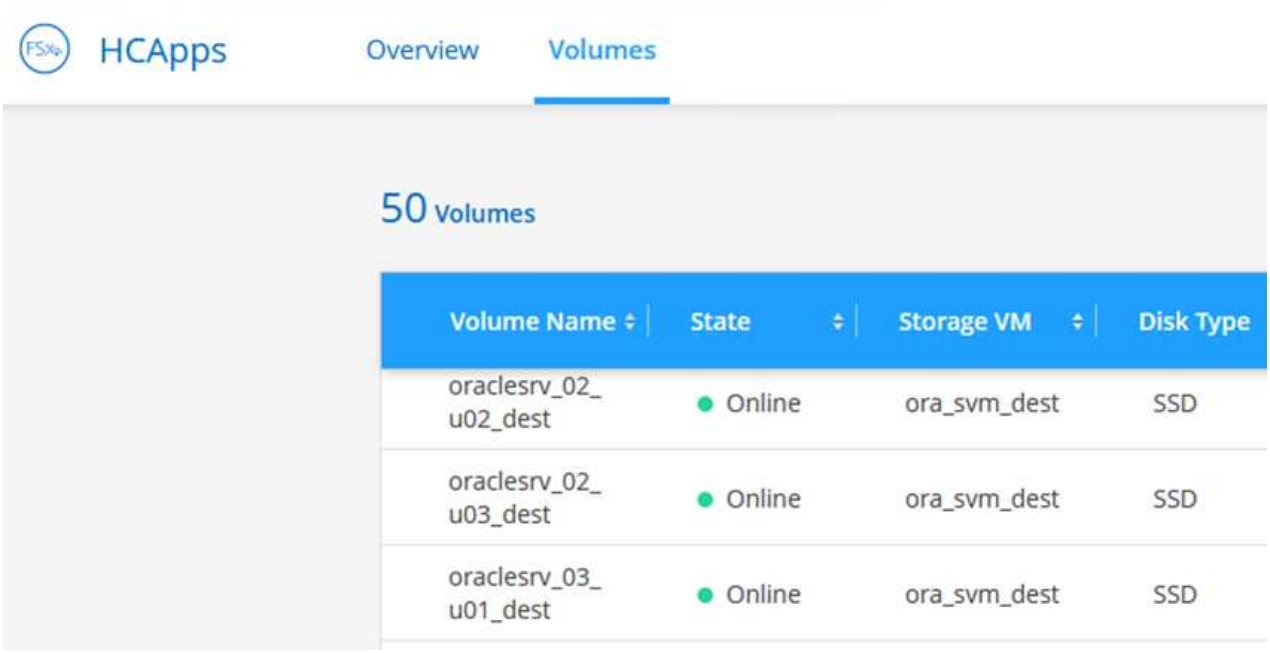
4. Agregue el nombre de la ruta de unión y haga clic en Actualizar. Especifique esta ruta de unión al montar el volumen NFS desde el servidor Oracle.


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

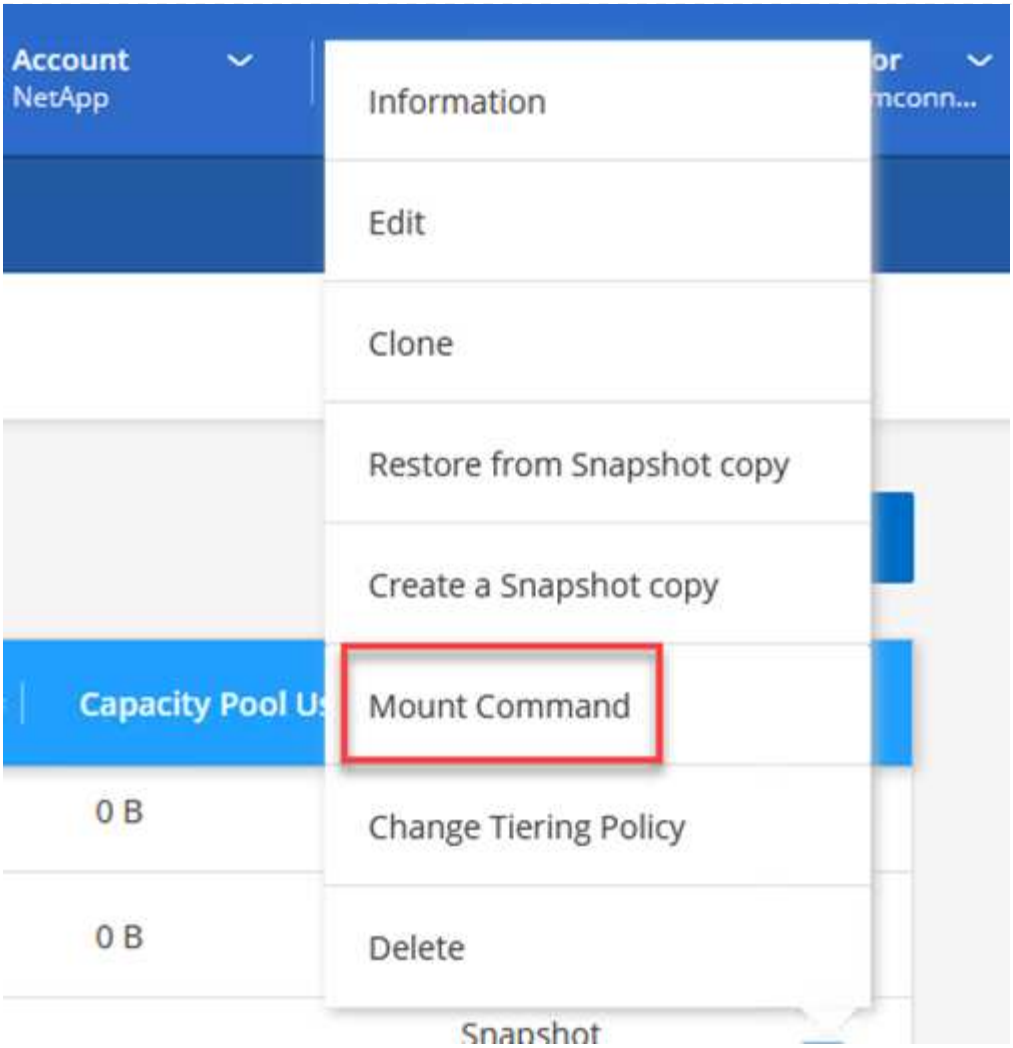
Montar volúmenes NFS en Oracle Server

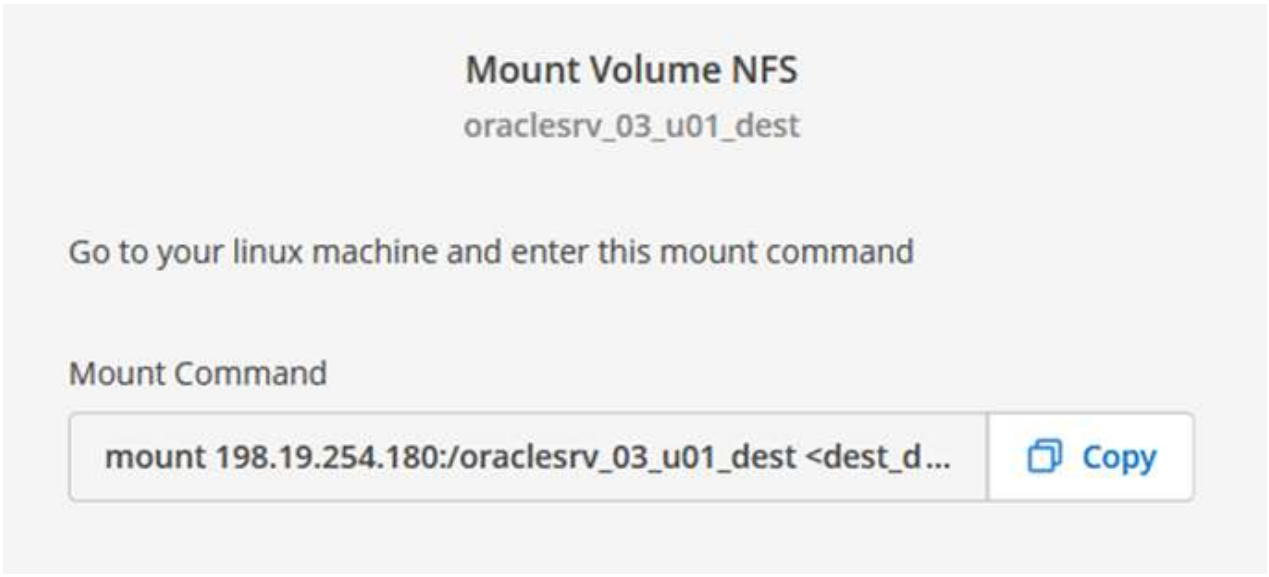
En Cloud Manager, puede obtener el comando de montaje con la dirección IP LIF de NFS correcta para montar los volúmenes NFS que contienen los archivos y registros de la base de datos de Oracle.

1. En Cloud Manager, acceda a la lista de volúmenes de su clúster FSx.



2. Desde el menú de acciones, seleccione Comando de montaje para ver y copiar el comando de montaje que se utilizará en nuestro servidor Oracle Linux.





3. Monte el sistema de archivos NFS en el servidor Oracle Linux. Los directorios para montar el recurso compartido NFS ya existen en el host de 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 para cada volumen asociado con las bases de datos de Oracle.

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

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

Recuperación por recuperación

Una vez completado con éxito el proceso de conmutación por error descrito en esta solución, SnapCenter y Veeam reanudan sus funciones de respaldo ejecutándose en AWS, y FSx ONTAP ahora está designado como almacenamiento principal sin relaciones SnapMirror existentes con el centro de datos local original. Una vez que se haya reanudado el funcionamiento normal en las instalaciones, puede utilizar un proceso idéntico al que se describe en esta documentación para reflejar los datos en el sistema de almacenamiento ONTAP local.

Como también se describe en esta documentación, puede configurar SnapCenter para reflejar los volúmenes de datos de la aplicación de FSx ONTAP a un sistema de almacenamiento ONTAP que resida en las instalaciones. De manera similar, puede configurar Veeam para replicar copias de respaldo en Amazon S3 mediante un repositorio de respaldo escalable para que dichas copias de respaldo sean accesibles para un servidor de respaldo de Veeam que resida en el centro de datos local.

La recuperación está fuera del alcance de esta documentación, pero difiere poco del proceso detallado que se describe aquí.

Conclusión

El caso de uso presentado en esta documentación se centra en tecnologías de recuperación ante desastres probadas que resaltan la integración entre NetApp y VMware. Los sistemas de almacenamiento NetApp ONTAP brindan tecnologías de duplicación de datos comprobadas que permiten a las organizaciones diseñar soluciones de recuperación ante desastres que abarcan tecnologías locales y ONTAP que residen con los principales proveedores de nube.

FSx ONTAP en AWS es una de esas soluciones que permite una integración perfecta con SnapCenter y SyncMirror para replicar datos de aplicaciones en la nube. Veeam Backup & Replication es otra tecnología conocida que se integra bien con los sistemas de almacenamiento NetApp ONTAP y puede proporcionar conmutación por error al almacenamiento nativo de vSphere.

Esta solución presentó una solución de recuperación ante desastres utilizando almacenamiento conectado a un sistema ONTAP que aloja datos de aplicaciones de SQL Server y Oracle. SnapCenter con SnapMirror proporciona una solución fácil de administrar para proteger los volúmenes de aplicaciones en sistemas ONTAP y replicarlos en FSx o CVO que residen en la nube. SnapCenter es una solución habilitada para recuperación ante desastres para conmutar por error todos los datos de aplicaciones a VMware Cloud en AWS.

Información de copyright

Información de la marca comercial